Testimony of
Roberta A. Bienfait

Hearing on
"Cyber Security: Recovery and Reconstitution of Critical Networks"

Before the

Subcommittee on Federal Financial Management, Government Information, and International Security

July 28, 2006

Good Morning, Chairman Coburn, and members of the Committee.

My name is Robin Bienfait and I am the Senior Vice President of AT&T's Global Network Operations that includes the local, data and voice networks worldwide. In addition, I lead the teams that manage our 30+Internet Data Centers, business continuity, network security, and disaster recovery for our global network.

I am responsible for the implementation of network design, development, engineering, operations, reliability, and restorability of AT&T's global network, and the deployment of new services, tools, and capabilities for next-generation Internet Protocol (IP) networks. On an average business day, AT&T carries more than 5.41petabytes of data [peta = quadrillion]. That is equivalent to the printed contents of the Library of Congress in Washington, D.C. passing through our network every 4.6 minutes. AT&T also carries over 400 million long-distance, local and international voice calls on an average business day and we provide network services to 127 countries.

I joined AT&T in 1985 and have held a variety of technical and leadership positions of increasing responsibility over the years. I have led AT&T's international and domestic core network operations and technical support division and I have led the organization responsible for providing all domestic services for customers of AT&T Business, the company's largest operating unit. In the past, I also led an AT&T Labs organization as vice president for service assurance, electronic maintenance and IP/data systems. I also led an organization responsible for the fundamental development of critical underlying networking capabilities across all global services. I currently have 11 patents pending.

I want to thank you for calling this important hearing and for allowing me the opportunity to share with you what we have done and are doing generally to ensure the reliability and restorability of AT&T network services.

There are 3 keys to success in terms of network security and disaster recovery – and I will examine them today in the context of our experience with Katrina recovery and outreach and in the context of the black out of 2003.

Those 3 keys are: Preparation, Execution and Evaluation/Improvement

I will examine these three elements in the following ways:

- looking at the strength of the public/private partnership
- looking at lessons learned especially from Katrina and the power outage
- proposing a series of policy recommendations that we believe will move us all forward toward improving our national ability in all three areas

We believe that strong infrastructure protection and cybersecurity practices are good business and they are our highest priority.

The commerce of our country is supported by a cyber and physical infrastructure that is in effect a very closely coupled partnership between all of the providers and users of this infrastructure. In a very simple example a consumer internet banking service has infrastructure that includes servers provided by the financial institution, telecommunications facilities provided by AT&T, and the consumer's home PC & network. Federal, state and local government also have a role in this infrastructure partnership. All of the elements of this simple example have hardware, software, and other components that must be functioning correctly to provide the end service. Each partner has a responsibility to keep their part of the infrastructure up and working. They also each have a responsibility to be able to recover or restore their component of the infrastructure.

None of the partners should ignore their responsibility or they risk disrupting this closely linked partnership or more likely they risk becoming isolated from the other partners. One example of this type of isolation is related to consumer voice communication. More and more consumers are

relying on the very convenient and portable cordless phones or cellular phones as their only means of voice telecommunications. During the widespread blackouts on August 14, 2003 many of these consumers did not have a working phone due to the lack of power to charge the batteries required for their handsets. The lack of a functioning phone in the home could be inconvenient or it could be catastrophic to an individual if they needed to reach 911 emergency services. The voice communications network in the United States was functioning during the blackout but that really didn't matter to this subset of consumers. Mandating stricter recovery or resiliency requirements for the other members of the partnership would not have helped these consumers. There is a very important component of individual or enterprise responsibility to ensure the recovery of critical processes or functions. There are similar circumstances where large enterprises have the responsibility to protect their critical services and infrastructure that should not be abdicated to the other partners including the Government. AT&T recognizes the critical importance of reliable electrical power to our infrastructure operations. To protect our network and customers from interruption we maintain several layers of emergency power backup. We do not assume that the electrical utilities will always be able to provide us the electrical power we need to operate our infrastructure.

For the fifth consecutive year, AT&T has polled chief information officers and other senior IT executives at companies throughout the United States with more than $10 million in annual revenue for their views on disaster planning/business continuity trends. Despite the devastating effects of Hurricanes Katrina and Rita last year, nearly half of the 1,000 companies polled by AT&T also said that they do not take specific protective actions even when state or federal governments issue warnings for an impending disaster, such as severe weather. It's evident that for some companies, the various events of the past year have been a real wake-up call. That's the good news. But it's surprising how many companies are still putting their businesses and future at risk by not adequately planning for the next hurricane, earthquake or cyber-security hit.

AT&T takes our responsibility for operating secure and reliable networks very seriously. Our network design goal is to have a network where failures are prevented, or predicted and pro-actively corrected, before they impact a customer's service. This goal is the foundation for the preventive, predictive, and proactive efforts that we take to first protect our physical and virtual infrastructure and second to be able to restore this infrastructure under any circumstances.

I. PROTECTING CRITICAL COMMUNICATIONS INFRASTRUCTURE

A. Preparation

As a preliminary matter, there are three overarching steps that AT&T has taken – and that are essential to protecting vital communications infrastructures. The first begins long before any disaster occurs. It entails *preparation* to ensure that the network and its components are as reliable as possible through proper design, hardening, redundancy, and performance at levels that far exceed routine needs. At AT&T, for example, we engineer our network to “five nines” of reliability – 99.999% reliability – that requires a diversity of communications links and equipment. This measurement relates to the number of defects in relation to opportunity. For every million opportunities 10 defects equal 99.999% availability/defect free or "Five Nines". For example, if you have 400 million calls during a given day, 4,000 blocked calls is equivalent to 99.999% were completed. Another example would be if 10 million packets were sent, if 100 were dropped, this is equivalent to 99.999% were successful or "Five Nines" performance.

When links and associated systems fail, there must be instantaneous and seamless rollover to backup facilities. This capability must be periodically tested, and given the frequency of cable dig-ups throughout the country, let alone emergencies of unprecedented scale such as Katrina, this testing must occur frequently.

Proper preparation, however, also contemplates that even the best facilities could fail. Proper preparation therefore requires rigorous planning for service restoration, including advance placement and availability of service restoration equipment where it can quickly meet identified needs, and ongoing training to ensure the availability of the skilled workforce needed to restore service. We make restoration our first priority and then move on to make repairs.

- Such a commitment to preparation, excellent service in the face of disaster, and responsiveness to threats to our networks and customers, does not come cheaply. At AT&T, we have invested over $300 million since 1991 in our mobile Network Disaster Recovery (“NDR”) infrastructure and capabilities. We also invested $200 million in an AT&T Labs-developed system called I-

GEMS that proactively monitors and manages the networks of some of our largest customers. We bring our Emergency Communications Vehicles ("ECVs") wherever needed to provide communications services in an emergency, and we have more than 500 various vehicles stored in locations around the country and loaded with generators, fiber and other supplies, repair and restoration facilities, circuit and packet switching, HVAC capabilities, lights, batteries, chillers, pumps, food, first-aid and whatever else may be necessary to make our response effective. We have the basic building blocks of our network infrastructure hardware and software installed in 150 technology trailers including the same electronics and optics that are installed in our telecommunications hubs. This equipment is installed and ready to roll at a moments notice. Our NDR can be seen as an active extension of our network that stays powered up and in synch with the 'live' network. We have extensively drilled our teams in various scenarios on a quarterly basis to ensure that readiness remains at peak levels.

Our Business Continuity/Network Disaster Recovery disaster planning and Continuity of Operations Plan ("COOP") gives us the ability to duplicate necessary capabilities quickly to meet or exceed our customers' business needs and continuity requirements, including those of our government customers. This has many components, including unparalleled security capabilities, logical systems, and physical capabilities. Network security is of particular importance given the prevalence of attacks through worms and viruses and the possibility of related threats. AT&T works diligently to provide network security for our infrastructure and to our customers. Network security requires great focus and attention, and will certainly remain a critical challenge.

AT&T also established a system level Certification and Assurance governance process whereby we measure our estimated likelihood of recovery in the event of an incident. We then drill down to the component level and assess the consequences of a potential failure and the impact to our business. We work to mitigate the risk of failure by either eliminating the threat and the vulnerability,

or by mitigating the exposure. This process informs our rigorous business case analysis and brings clarity to investment decisions. We regularly assess these components both for ourselves and on behalf of our customers.

An extremely important part of our preparation is focused on the virtual element of our infrastructure. Like every enterprise, AT&T faces multiple and growing threats to information security. Software viruses, Internet worms and denial of service attacks have become common. "Phishing" schemes aimed at extracting personal information from unsuspecting users appear every day. Much of what attempts to enter the corporate intranet is made up of unsolicited commercial messages, or spam. According to AT&T security experts, more than 75 percent of the e-mail messages aimed at the att.com portal daily are spam. Intelligent network security functions require infrastructure, analysts and expertise. We are the only provider that maintains an active research laboratory. The algorithms that we have running in our database are all proprietary, they're all based on sifting through daily traffic and trying to find anomalous conditions. By keeping a laboratory, by having infrastructure that we build up over a period of time, we can demonstrate the feasibility of these types of security techniques, methods and algorithms with our customers.

Like most large enterprises, AT&T was using a system of premises-based security firewalls distributed across the company's many locations. The company reviewed several options. As discussions continued, the most effective and efficient solution emerged: a solution based not solely on the company premises, but a layered approach with an emphasis on leveraging the network. In early 2004, AT&T security planners initiated a more comprehensive and systematic approach to security planning and implementation. How do we utilize the inherent strength of AT&T's network, they asked, to create security solutions that meet our internal needs and also meet the needs of our customers? Why not move many security defenses out of company offices and into one network that ties all those sites together? In addition to fending off attacks and providing more consistent software

patching, AT&T's security approach is designed to assure business continuity. Security infrastructure equipment is housed in hardened AT&T data centers, disaster-ready buildings equipped with robust backup systems, instead of being dispersed at potentially more vulnerable enterprise sites.

AT&T has a portfolio of security services that protects customer's vital data and secures their enterprise networking environment. AT&T delivers a suite of offers that assess vulnerabilities, protect customer's infrastructure, detect attacks and respond to suspicious activities and events. A leading innovation that came from the company's own learnings is AT&T's service called Internet Protect[SM] Service. This security alerting and notification service offers advanced information regarding potential real-time attacks including viruses, worms and DDOS attacks that are in the early formulation stages.

B. Execution

The second vital step to protect communications infrastructure requires *execution* during and immediately following a disaster. In many respects, execution is a function of proper preparation, particularly having a robust infrastructure, a well-trained and frequently-drilled workforce, and facilities and capabilities available for service restoration. Effective execution also requires a sophisticated command and control structure in emergencies to make every minute count, every deployment as effective and efficient as possible, and to enable our dedicated employees to work as safely as possible. We follow an incident command structure, which is led at every moment by an experienced Executive Duty Officer. Our incident command structure is a variation of the same National Incident Management System (NIMS) that is an important part of the National Response Plan under DHS. It is used by many other first responders in the public and private sectors. We do not wait for disasters or other emergencies to use our incident command system. As a foundation discipline we use it to manage changes in our network hardware & software and to manage other network incidents like fiber cable cuts. This allows our team to use the process on a regular basis so during a disaster it becomes a much more focused second nature.

In addition, execution requires close coordination with third parties, including federal, state, and local government authorities and first responders, others in the telecommunications industry, and others in the private sector trying to restore essential services and facilities, such as power, water, roadways, and the like. This communication and coordination effort is often the most difficult part of execution during and immediately after a disaster. In the communications field, the telecommunications industry response to disasters, other than that of a company responding to damage to its own facilities, is typically coordinated through the National Coordinating Center for Telecommunications ("NCC"). The NCC, as part of the Department of Homeland Security, has an important role in the telecommunications industry's ability to continue to operate our telecommunications infrastructure after a disaster by acting as a liaison between the industry and the government. They match telecommunications companies to those governmental entities with unmet emergency telecommunications needs. The NCC also provides a means for the telecommunications industry to request the assistance of the Federal Government. We have assisted the Federal Government and other carriers after receiving requests through the NCC including helping the Federal Marshals establish satellite communications in NYC after the WTC attacks. We have also received assistance from various Federal agencies after requesting it though the NCC including: fuel assistance after Tropical Storm Allison in 2001, flying a few of our NDR team members on a military transport from California to New York after the attacks on 9/11, and flight path requests for our helicopter support after Hurricane Katrina.

Finally, execution requires ingenuity and resourcefulness when the unforeseen happens. Each emergency situation presents its own unique set of challenges. Even the most thorough planning and training cannot take the place of highly skilled and resourceful emergency responders who can recognize and adapt to unplanned circumstances.

C. Evaluation and Improvement

Finally, the protection of the communications infrastructure requires a thorough and frank after-the-fact evaluation of performance, distillation of lessons learned, and implementation of *improvements*. In this regard, one outcome of Hurricane Katrina should be a critical reassessment of our performance as individual communications companies, as an industry, and as a nation, and implementation of the policy recommendations needed to improve performance in the future.

II. IMPACT OF KATRINA ON THE NETWORK AND ITS RESTORATION

Overall, AT&T's network remained overwhelmingly intact following the hurricane and flooding. At all times, we were able to carry at least 95% of the calls in the Gulf Coast area that came to our network. Of the 5% of our capacity in the area that was initially lost, FASTAR ®, our software and hardware system that redirects and reroutes traffic, restored half of that capacity within a couple of hours. Within 24 hours of the storm making landfall, another quarter of that capacity was restored via manual rerouting, and the final quarter was restored within 48 hours of the storm making landfall when AT&T workers physically installed two cables in the ground and rerouted certain traffic. This latter effort successfully worked around the loss of certain regenerators that boosted the strength of digital bits long distances over fiber. On a nationwide basis, on the day of Katrina and over the next few days, we successfully carried intercity traffic at levels that exceeded demand the week prior to Katrina by approximately 10%.

Nonetheless, because we interconnect with other carriers, including local exchange carriers and wireless carriers, we could not complete calls to other networks that suffered more severe disruptions. As a result, following Hurricane Katrina's landfall on the Gulf Coast, we needed to block millions of calls a day into the affected area due to outages in other telecommunications carrier's networks.

We built our only major switching station in the New Orleans area on high ground utilizing "submarine doors" and, therefore, it was not flooded. We had also invested money in the infrastructure of this major switching station based on past flooding threats in New Orleans including moving critical electrical equipment and emergency generators to upper floors in the facility. One of our most immediate concerns in the aftermath of Katrina regarding that facility, however, was looting

and security. Security concerns forced employees to evacuate our switching center late in the afternoon on August 31st as local law enforcement was unable to ensure the safety and security of the site. We requested the assistance of DHS and they dispatched heavily armed U.S. Marshals and FBI Special Agents to secure our critical switching center early that evening. Our employees returned to the building the following day, together with BellSouth employees who worked in the same building. They were escorted into the area by more U.S. Marshals and FBI Special Agents provided by DHS. At that time, our people delivered to the building fuel for the generators, water for the air conditioning chillers, food, and other supplies. Law enforcement authorities also set up operations in the lobby of the building in order to utilize the telephone connectivity available there. During the period that our employees were out of the building, the network infrastructure was put on automatic controls and monitored remotely by the AT&T Global Network Operations Center.

We had 162 offices loose commercial power during the storm event. We had ensured a sufficient backup generators and enough fuel for them. We were able to restore power by putting many of these sites on generators, and by making use of batteries or fuel cells in connection with a few. We replenished fuel supplies as necessary to avoid disruption, but our preparations included staged supplies of thousands of gallons of gas in portable containers, thousands of gallons of diesel fuel in portable cells, and thousands of gallons of water in portable tankers for cooling towers.

III. AT&T'S KATRINA RESPONSE AND OUTREACH

AT&T began moving equipment and teams from around the country toward the Gulf States in the days before the storm made landfall. We followed our prescribed approach. The first team restored AT&T's service to its prior levels, the next maintained and monitored AT&T's facilities so as to prevent new issues from arising, and the third came in to help others. AT&T worked around the clock to respond to this crisis and safeguard its network, support efforts to respond to the disaster, and address the needs of evacuees.

Because we fully restored and secured all of our network capabilities within the first 48 hours of the crisis, in a spirit of service and compassion, AT&T was able to direct its efforts to benefit its customers, other telecommunications competitors and their customers, first responders, and evacuees as needed. In this instance, we were largely able to use our in-place capabilities to meet not only our own needs, but also those of others. We put a variety of our facilities to work for other carriers and their customers, and continue to carry significant amounts of additional traffic for other carriers that cannot currently do so themselves. AT&T also helped to provide relief to those directly affected by the hurricane and flooding, and assistance to charitable relief activities.

Of course, the same is particularly true of our work with government customers like FEMA. In addition to immediately increasing FEMA call capacity and toll-free number availability, over the weekend of September 10th, AT&T was able to install an additional 3,360 voice circuits to boost call center capacity to support FEMA. AT&T worked directly with the IRS to execute in less than 24 hours an agreement to direct calls using IRS trunks which IRS provided to give FEMA necessary increased call capacity.

At the same time, we coordinated with the DHS NCC regarding the considerable resources that we could make available. First, we focused on the broader telecommunications network and the critical needs of first responders and ongoing rescue operations. In coordination with the NCC, we dispatched five Emergency Communications Vehicles ("ECVs") with satellite capabilities, and other forms of assistance, to assist in the relief efforts. Never before had we deployed so many of our satellite assets to a single area. During the first 13 days of the crisis, over 104,000 calls were made through AT&T ECVs. We assisted the Louisiana State Police, the Louisiana National Guard, Stennis International Airport, NASA and others, including civil emergency communications authorities in Mississippi and Louisiana. We also provided some of our portable diesel-powered generators to Louisiana State Police Troop L headquarters in Mandeville, LA on Saturday morning, September 3. They had lost their back-up power generator that morning. We offered an AT&T generator until its own could be repaired or commercial power restored.

The second part of our response was to provide relief to individuals, telecommunications services in support of charitable work, and to make our own charitable contributions.

- Working with Avaya, Cisco and SBC, we helped establish a communications network for evacuees at the Astrodome, including more than 1000 phone lines as well as data infrastructure.
- We established a phone bank to assist displaced college students to find alternative educational opportunities.
- We provided toll free calling and 10 call centers for a successful fundraiser: "Shelter from the Storm: A Concert for the Gulf Coast."

- The AT&T Foundation also pitched in to address the needs created by this disaster. It donated $1.5 million[1] and 148 laptops to the Red Cross for relief efforts. It issued 35,000 pre-paid calling cards for distribution to survivors and evacuees.

[1] This figure includes $500,000 in matching funds for donations from AT&T employees.

IV. IMPACT OF 2003 NORTHEAST BLACKOUT ON THE AT&T NETWORK

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. This outage affected an area with an estimated 50 million people in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time and power was not restored for 4 days in some parts of the United States. Estimates for the cost of the blackout range between $4 billion and $10 billion with the U.S. Department of Energy estimating $6 billion.

Internet traffic, data services, and voice calls flowed across our network without interruption. This was not due to luck but instead the reliability and redundancy that we designed and built into our network infrastructure including the multiple layers of emergency power provided by generators and battery back-up. It is also a tribute to the people of AT&T who worked around the clock to keep America's communications infrastructure up and running. We used our very disciplined incident command system to manage the event including refueling of some generators, moving portable generators to charge batteries at some of our smaller fiber cable regenerator stations, and respond to assistance requests from other carriers and some of our customers.

282 of our Network nodes were protected by our emergency backup power infrastructure for intervals ranging from several minutes up to 74 hours. AT&T did experience a significant spike in our long-distance phone traffic after the initial outage, which leveled off during the night. Our network performed superbly during this voice call surge and the call levels were back to normal by the next morning.

We did have a problem with one of our local voice switches in New York City on August 14th when the landlord at one our leased facilities refused to let us run a standby generator that we had for emergency backup due to exhaust fumes that were drifting back into the building. Late that evening the backup batteries for the site exhausted and we lost power at this location. By the time the batteries had exhausted and we lost power the business customers that were served by this voice switch had already left the city. We requested assistance through the New York City Mutual Assistance Restoration Consortium (MARC) to get a NYPD escort for a portable generator we brought in to provide power. The police escort was required to bring the generator though the gridlock caused by the blackout. NYC MARC has a very similar mission to the DHS NCC and acts as a two way liaison between the local authorities and private industry infrastructure operators including power, gas, and telecommunications.

IV. LESSONS LEARNED

Each emergency situation presents its own unique set of challenges, and even the most thorough planning cannot take the place of ingenuity and resourcefulness when the unforeseen happens. That said, much can be anticipated and we must plan and drill to address a variety of events on any scale. I am sure I join all of you in saluting our first responders and relief workers in their tireless efforts. But the importance of resourcefulness does not in any way obviate the need for very carefully thought out emergency planning led by seasoned professionals.

Our experiences have reinforced the following lessons which we all must incorporate in future planning:

- **Establish and Practice Disaster Recovery Processes in Anticipation of Emergencies: Communications, Command and Control.** Communications resources can be brought where needed very quickly, but it is essential that there be clear lines of command and control at all times in order to direct those resources effectively and to the area of greatest need. Moreover, if because of the scale or nature of the disaster, some aspect of the plan affecting the command structure is not workable, an alternative must also be part of the plan and ready for implementation. Finally, without practice and drilling, no team will be ready and no plan will be ready to implement.

- **Internalize the 3P Paradigm: Preventive Action, Proactive Focus, Predictive Models.** It is crucial to invest in facilities and plan and drill regularly and thoroughly for a wide variety of contingencies. Investment cannot be deferred and possible scenarios ignored. We cannot wait for a disaster to occur before we are prepared to move aggressively.

- **Make Risk Analysis Routine: Harden Critical Infrastructure Where Indicated.** It is imperative to know what part of your infrastructure is critical to continued operation of the network in times of crisis and how to harden it as much as possible and to replace or restore it to the extent it may be damaged. Such analysis must be part of any risk assessment, and the assessment must be followed promptly by action.

- **Establish Crisis Management Plan.** Every emergency situation is different, and even the best planning may not prevent things from going wrong. Thus, we need to prepare ourselves for that eventuality. Crisis management plans must recognize and allow for improvisation to adapt to the given circumstances.

- **Coordinate Restoration and Recovery Effort**. There should be no wasted effort in recovery operations. Everyone available should be participating, and there needs to be coordination so that efforts are not duplicated or in conflict with one another. The NCS NCC played a very positive role in matching available resources to pending needs. It is essential that logistical information such as what roads are closed and what medical precautions need to be taken be readily available. Moreover, a recommendation we made after 9/11 still has not been widely implemented. Companies who are crucial to the response to disasters such as AT&T should have special credentials designed for employees and accredited in advance in order to access disaster areas. In some cases AT&T employees only were able to respond and move mobile resources into the Gulf Coast area by virtue of their resourcefulness in talking their way into affected areas. Letters were provided during the disaster response but not all state and local law enforcement authorities recognized or honored them.

- Design Five 9's of Reliability. This storm again confirmed that telecommunications companies that design their networks to this standard – 99.999% reliability – have excellent disaster recovery and response capabilities, as well as reasonably hardened networks. That is the only way to maintain this standard. In times of crisis, this capability becomes a vital national asset.

- **Interoperability and Spectrum Availability.** A crisis on the scale we saw in the Gulf Coast, and smaller challenges as well, demand a well coordinated information and communications delivery system. We must resolve the spectrum needs highlighted by the 9/11 Commission, among others, to provide first responders and others with a better and more effective means of communicating quickly and easily in an emergency.

POLICY RECOMMENDATIONS

These lessons learned lead to the following specific policy recommendations:

- Focused and unified incident command is a very important function for coordinating any type of event but would be absolutely critical during a massive, nationwide disruption of our shared cyber infrastructure. The FCC, DHS Office of Cybersecurity & Telecommunications, National Cyber Response Coordination Group (NCRCG), and the NCC all appear to have roles in coordinating any reconstitution of the internet after a massive outage. A single agency must be identified, funded, and empowered to act as the National Cyber Incident Commander for any required cyber infrastructure recovery and reconstitution efforts.

- The agency that is designated as the National Cyber Incident Commander must also be the lead for the planning and exercising of coordinated response plans with all parties in the cyber infrastructure. The first items that must be addressed immediately by this agency are a coordinated advanced warning mechanism including an emergency communications plan. The coordinated advanced warning mechanism should be a way of identifying potential emergencies and agreed-upon protocols and thresholds that indicate an attack is under way or a disruption is imminent. Something along the lines of a blend between the Centers for Disease Control and Prevention (CDC) and the NOAA National Hurricane Center for our cyber infrastructure. An emergency communications plan must address the protocols and processes for responding to severe failures as well as the infrastructure used to communicate. This infrastructure could be a blend of the recently dissolved Alerting and Coordination Network (ACN) and the SHAred RESources (SHARES) High Frequency (HF) Radio Program administered by the NCC. This emergency communications infrastructure must not rely on the underlying cyber infrastructure. In the absolute worst case scenario of a complete cyber infrastructure shutdown the best communications means to coordinate the recovery and reconstitution may be a private line conference bridge arrangement or even HF radio.

- Drill frequently for emergencies under various scenarios and include the public and private sector. Do not be satisfied with a written plan. Put the plan in practice and continue to improve. A plan that is not tested and exercised regularly can actually be more harmful than not having a plan. A false sense of security is created with the untested plan and usually many resources have gone into producing something that may never work in trying circumstances.

An honest and thorough after exercise evaluation of performance, distillation of lessons learned, and implementation of improvements.

- Furnish standardized and approved emergency credentials to vital communications and other infrastructure providers in advance, so that AT&T and other specialized disaster staff can get into affected areas to restore vital capabilities without delay or interference. While our teams were given letters from state officials authorizing them to enter impacted areas, those were not necessarily recognized by security and other law enforcement personnel in the field. We have been participating in a trial of the DHS First Responder Authentication Card system that appears to meet this need. A national credentialing system must be established to allow us to more quickly restore critical communications after a disaster or other emergency.

- Predetermine security needs and formalize request process from telecommunications carriers for law enforcement deployment to protect critical infrastructure facilities immediately following a disaster.

- Increase the visibility of the resources that our Government has already created for emergency planning. www.ready.gov is an excellent resource provided by the DHS that includes emergency planning advice and resources for our citizens, businesses, and even our pets to help us all prepare for the unexpected. It should be promoted more widely to promote the message of individual and enterprise accountability for disaster and emergency planning.

- Consider subsidizing some emergency preparation by infrastructure companies since the government is likely to call such capabilities into use or would otherwise need to duplicate resources inefficiently.

- Minimize the amount of regulation and data reporting requirements during a disaster and maximize the amount of coordination and cooperation between the public and private sector. The priority must be on the safety of our employees and the recovery and reconstitution of this critical national resource. The limited Special Temporary Authority (STA) and waiver of the FCC's rules to engage in integrated disaster planning and response without observing the FCC's structural separation requirements that was granted by the FCC to AT&T, and several other carriers, is an excellent example of focusing on the recovery mission.

We can never anticipate every contingency in an emergency, nor can we assure a foolproof communications network all the time under all circumstances. Nonetheless, at AT&T, we have done much to ensure reliability and restorability of communications networks and together – as an industry and as a nation – we can do more. I thank you for holding this hearing to advance this important discussion.

* * *