**WRITTEN STATEMENT OF:**

**SUSAN R. BAILEY, Ph.D.**
**VICE PRESIDENT – GLOBAL NETWORK OPERATIONS PLANNING**
**AT&T INC.**

**UNITED STATES HOUSE OF REPRESENTATIVES**
**COMMITTEE ON HOMELAND SECURITY**

**May 6, 2008**

My name is Dr. Susan R. Bailey. I am AT&T's Vice President, Global Network Operations Planning, located in Bedminster, New Jersey. I appreciate the opportunity to share ideas with Members of Congress and other industry participants to enhance America's homeland security capabilities.

I have over 20 years of experience in developing, deploying and operating advanced communications technologies and support systems, and have held numerous positions in planning, network operations, and product research and development. In my current role, I develop the network operations model spanning all services and technologies for the entire company, including global and long distance services, regional access, wireless mobility, and video applications. I am, therefore, intimately familiar with AT&T's principles and methods for building and maintaining a robust communications infrastructure.

As the nation's largest communications company, AT&T is a critical link in keeping our society connected – especially during disasters. Among other things, we provide lifeline and emergency communications to millions of consumers and businesses; mission-critical support for government agencies and institutions; and robust communications networks and support for the full range of business enterprises, including in the healthcare, electric power and banking sectors. We know that, in many ways, peoples' lives and safety, as well as the function of our government and economy, depend on the services we provide. For these reasons, ensuring that our component of the nation's infrastructure is sound and resilient is one of our top priorities.

The following outlines AT&T's approach to protecting its network and responding to disasters, and includes some examples of that approach in action.

## AT&T's Network Reach

AT&T operates one of the most extensive communications networks on the planet. We have deployed and maintain more than 500,000 miles of fiber in the U.S., under the oceans, and around the world. Every day our network carries more than 16 petabytes of data – the equivalent of moving the entire written contents of the Library of Congress every 35 seconds. In the U.S., we are the leading provider of broadband Internet access services; the leading wireless provider – able to offer 3G wireless broadband in 265 major metropolitan areas; and the leading provider of telephone service in rural areas. We have equipment deployed to serve 143 countries. All told,

over 1 billion devices are connected to AT&T's network, and we make data services available to 97% of the world economy.

The breadth of AT&T's network allows us to provide unmatched quality across an unmatched range of services, but it also necessarily means that our capabilities are subject to a wide range of threats. These threats include power outages, hurricanes, typhoons, earthquakes, terrorist attacks, and even an otherwise innocuous fiber-seeking backhoe that accidentally strikes an underground cable. Moreover, we see indications of nearly 39 million potential cyber-attacks every month; while these do not result in physical damage, they can wreak havoc on the logic of a network that is not adequately defended. And, of course, health pandemics, transit disruptions, or work stoppages can affect our workforce, which in turn can directly impact our networks. We worry about and plan for all these incidents – and more.

**AT&T's Approach to Business Continuity and Network Resiliency**

AT&T is in the business of connecting people anywhere and any time. In order to connect people, continuity of operations is critical. The hallmark of our business continuity program is a common, structured approach to infrastructure design, management, and execution.

Our enterprise business continuity paradigm focuses on protecting three types of assets:

1) The network itself, i.e., the computers, switches, routers and fibers that carry our customers' data.

2) Work centers and the people who work in them, in particular those that perform mission-critical help-desk and network operations functions. We plan for the safe evacuation of our people through emergency communications and evacuation plans. And we plan for the recovery of mission-critical work functions, such as customer help desk and network operations, in alternate locations or arrangements.

3) Network management tools, such as network and customer databases, ticketing systems, provisioning and alarm management systems, and business process automation platforms.

More specifically, AT&T focuses on service or functional resiliency. At its core, this means the continued operation of a function *despite* the loss of certain assets and controlling the impact once a threat arises. This compares to a strategy that unduly emphasizes the elimination of all possible threats. We cannot prevent a tornado or earthquake – or a terrorist attack – from destroying one of our buildings. But we can protect the functions performed in that location, such as by maintaining an alternate site geographically distanced from the primary site. To be clear, we certainly do our fair share of asset protection, such as securing the physical environment along our fiber routes or employing building security. But no amount of protection can possibly guarantee that any asset can completely be protected.

**AT&T's Philosophy in Action**

Consistent with our general philosophy, we leverage technology to protect functions and the services despite failure and disasters. For example, the telecommunications infrastructure depends heavily on commercial power. We therefore build resiliency into our major offices by connecting them to *two different and diverse* electrical substations. In addition, we equip them with battery backup and auto-start generators for continuous operation in the absence of commercial power. This fundamental design has sustained us through even widespread power outages, such as the widespread power outage of 2003.[1]

In addition to diversity of power, we employ diversity of fiber and other equipment. For example, most of our fiber routes have a physically diverse, geographically separated alternate route. This physical fiber diversity extends all the way to building entrances. In addition, the fiber connections to our major central offices have two separate entrances at different places within the building. Likewise, customer applications or data storage solutions can be hosted in any of AT&T's 38 worldwide internet data centers, with backup and failover capacity to provide uninterrupted capability even in the face of the loss of an entire data center. Servers and databases for a given application can be deployed, for instance, in a data center on the west coast and another on the east coast, perhaps configured to share the load between them under normal operating conditions. If, for whatever reason, one of the centers fails, the other could pick up the load and continue with uninterrupted service.

One of our most powerful assets to handle disasters of almost any kind is our fleet of more than 500 trailers equipped with all the gear we need to run our network – routers, switches, multiplexers and the like; these are mobile central offices. AT&T has been building and expanding this fleet for more than 15 years and so far has invested over $500 million in these disaster recovery assets. On a normal day, the trailers are stored in warehouses around the world. But they are not just collecting dust: they are right now connected to our network, monitored and managed, upgraded and repaired, just like any other element of our network. If we need any of the equipment, we can literally unplug a trailer, hook it up to a truck, and drive it to wherever we need it. And, we have software support that enables us to download all of the configurations that we use throughout our system almost instantly, which reduces the actual turn-up time at a site down to our objective of 72 hours. We test our disaster response capability four times per year so that we are ready to respond. In fact, at the same time as this hearing, AT&T will be conducting a simulated disaster scenario in Chicago.

Perhaps the most storied use of our mobile network facilities was in connection with the horrific events of 9/11. Because our mobile equipment is capable of operating in the stead of even the largest of our major central offices, we were able to use them to recover our transport

[1] In order to provide continuous service in the face of a power outage, AT&T and other service providers require access to the impacted area to refuel generators and perform other tasks. Especially in connection with disaster situations, providers often need the help of the government to gain access to areas and obtain needed fuel and supplies. It would be worthwhile, therefore, to develop methods and systems, which should include necessary pre-approvals or certifications, to ensure that gaining access to critical infrastructure is a priority in any disaster scenario.

hub that was in the 6th sub-basement of the World Trade Center South Tower, which was totally destroyed, as well as support three switches in nearby buildings that were heavily damaged. We dispatched trailers to New York, and by noon that day they were setting up in a parking lot across the river in Jersey City. Within 48 hours, these trailers were completely installed, configured, and ready to accept traffic.

Another dimension of the 9/11 disaster was the unprecedented traffic volume, all concentrated in and out of lower Manhattan, precisely where we had lost a major portion of our network capacity due to damage. Four hundred thirty-one million call attempts were made on our network on 9/11, which far outpaced our previous record day of 330 million call attempts. Through our Global Network Operations Center, we rerouted all traffic not directly destined for lower Manhattan, and prioritized traffic to maximize our ability to deliver outbound calls from lower Manhattan. As a result, AT&T successfully delivered 96% of Government Emergency Telecommunications Service (GETS) calls on 9/11.

Much of our effectiveness in disaster response and recovery results from our emphasis on training and practice. We run exercises of our work-center, network, and systems disaster recovery plans multiple times a year to ensure that we maintain a state of readiness. We learn from each one, and we keep our staff fresh on exactly what they need to do. This enables us to implement our plan quickly and efficiently when an unexpected event hits.

**A Note on Cyber-security**

We treat cyber security as an integral part of our network operations model, and have invested significant resources to become the industry leader in securing our network and our customers from the full gamut of cyber threats. The diversity of our network and the services we provide has given us deep insight into the most effective means to combat cyber-crime and other threats. The raw quantity of data traversing our network allows us to identify and discern traffic patterns across a 24-hour day and a 7-day week. This gives us a unique ability to detect abnormalities that can suggest cyber crimes in the making. We have learned that worms and viruses rarely hit without any preceding indicators. We see the hackers testing and probing, looking for openings and vulnerabilities, and sometimes even rolling out their code on a limited basis to see how it works, days and weeks in advance of the full scale launch. Now that we understand these anomalies and how they can serve as important leading indicators, we use this information (and take advantage of the lead time it provides us) to take the action on our network and with our customers to load the filters and patches necessary to combat the hack or virus.

In this regard, AT&T is pleased to offer our new network-based security services, which help our customers migrate away from a totally perimeter-based approach. Because placing security intelligence at the edge of the network or into individual applications is costly to scale and difficult to manage, a network-based approach is often superior, as it is more nimble and efficiently distributed. One example is our offering to protect customers from Distributed Denial of Service (DDOS) attacks. A DDOS attack involves large numbers of "attackers" (mostly infected PCs whose owners do not realize anything is wrong), sending large quantities of data, all destined for the "victim" machine, ultimately overwhelming it. For customers who purchase our DDOS protection capability, we can, from inside the backbone of our network, detect

emerging DDOS attacks, redirect attack traffic to scrubbers inside our network that separate the good from the bad traffic, and in turn redirect the good traffic back to a customer's IP address so that the customer can sustain operation without even feeling the effects of an ongoing attack.

I trust that the foregoing aids in your consideration of proper homeland security methods. AT&T looks forward to an ongoing discussion of these issues with the Committee.

# # #