

Written Testimony of Timothy R. Graham
Executive Vice President & General Counsel
Winstar Communications, Inc.
before the
United States Senate
Committee on Commerce, Science and Transportation
Subcommittee on Science, Technology and Space
9:00a.m. – December 5, 2001
Room 253 Senate Russell Office Building

- 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

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."

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.

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

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)

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 unforeseen, 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

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.

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* (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.”

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.

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 decision-making. It is an honor to have had the opportunity to provide this information to the official record for your consideration.

DOCUMENT INVENTORY: TESTIMONY OF TIMOTHY R. GRAHAM

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).