

TESTIMONY TO THE COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, CHAIRMAN

U.S. HOUSE OF REPRESENTATIVES

August 3, 2004

BOB COLLET

VICE-PRESIDENT FOR ENGINEERING

AT&T GOVERNMENT SOLUTIONS

AT&T CORP.

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me here today to discuss AT&T's views on the need to share critical network infrastructure information. At AT&T, we take our responsibility to protect against infrastructure vulnerability very seriously, and we are constantly updating network security in response to ever-transforming threats.

As the nation's largest Internet backbone provider, interexchange carrier and provider of network services to businesses, we are routinely challenged to engineer and operate a network of unparalleled scale. Like our colleagues in the industry, the National Communications System has tasked us since the peak of the Cold War to provide a variety of National Security/Emergency Preparedness (NS/EP) services built to meet very unique requirements. We regularly exercise these capabilities and our proprietary disaster recovery strategies are unique and unparalleled in the industry. We exercise our Disaster Recovery Program under a simulated, and, unfortunately, sometimes a real incident environment, as evidenced by our response to the terrorist attacks of 9/11. We have an overarching interest in preserving and promoting a safe, secure and robust infrastructure that will be a key enabler of economic growth and prosperity of the United States. We therefore very much appreciate the opportunity to offer these comments today.

Following the tragic events of September 11, 2001, we have redoubled our efforts. For the recent Democratic National Convention, for example, we developed a location specific network recovery strategy in case of terrorist action, and stationed a response team in the area ready to implement that plan if necessary. The same will be

done for the upcoming Republican Convention, and for similar important, high-profile events.

As you know, most of the country's critical infrastructures are owned and operated by the private sector, thus the private sector must play a key role in safeguarding those infrastructures. Much has been said about the need for an effective "public-private partnership" to share security-related information and to address security-related threats and vulnerabilities. These are laudable goals, and in fact, AT&T and other telecommunications companies have been working together to identify and address security risks, and to develop security-related best practices in partnership with government, for many years. Two of the most significant partnerships are noteworthy.

The NCC Telecom-ISAC

The good news for telecommunications is that this sector has been a leader in forging a public – private partnership to address infrastructure security. Telecommunications carriers have shared information informally with the National Communications System (NCS) since 1984. In 1991, the National Security Information Exchange (NSIE) was established as a forum in which government and industry could share information in a confidential, trusted environment. Since March of 2000, the NCS's National Coordinating Center (NCC) has served as the Information Sharing and Analysis Center, or "ISAC" for Telecommunications. NCC Telecom-ISAC participants, including industry and government representatives, gather and share information on threats, vulnerabilities and intrusion attempts. Information is analyzed to help avert or minimize disruptions to the telecommunications infrastructure. The results are aggregated and disseminated as provided by agreement among the ISAC members. In

addition, the NCS hosts the NCC and is the lead agency for the telecommunications support functions under the Federal Emergency Response Plan. In that capacity, the NCC is specifically charged with assisting in the coordination of telecommunications restoration and provisioning during national disasters through government and industry cooperation on a 24-hour basis. NCS and the telecommunications carriers also collaborated on the development of the “Government Emergency Telecommunications Service” or “GETS”, which provides government and industry personnel with key national security or emergency preparedness responsibilities with the ability to gain priority access to the public switched telecom network in times of significant network congestion.

Much of the benefit attributed to a partnership between government and industry involves the need to encourage robust, timely, two-way information sharing about threats, vulnerabilities, intrusions and anomalies. New protections provided in the Homeland Security Act significantly reduce the possibility that sensitive information shared voluntarily for these purposes might be disclosed publicly. Nevertheless, companies will only engage in sustained and meaningful information sharing when there is a compelling business case for doing so, and only in a trusted environment

There are three related reasons why we believe that the NCC Telecom-ISAC has been particularly successful. First, the NCC Telecom-ISAC is the only joint government – industry ISAC and is funded largely by government appropriations, so the core infrastructure and round-the-clock staffing is not borne exclusively by the private sector, as is the case with some of the other ISACs. Government “partners” provide value back to the industry participants. The information-sharing goes two ways. The government

routinely provides specific threat and alert information to industry representatives. Second, the NCC Telecom ISAC has demonstrated its ability to handle corporate proprietary and government classified information in a secure manner. Third, in times of real crises, the government NCC representatives quickly engage as ombudsmen on behalf of industry, helping industry gain access to impaired locations for purposes of restoration and recovery. They represent the needs and concerns of the industry in terms of coordinating successful rapid response. On September 11, 2001, the NCC helped network providers gain access to Ground Zero to restore communications, including arranging for military air transport for some of our key disaster recovery personnel who were stranded in California when commercial aircraft were grounded. The ability of government to deliver this kind of assistance, proven repeatedly in crises of differing degrees over the years, has led to an atmosphere of trust and cooperation in which we in industry have felt comfortable sharing sensitive information with the government and with our competitors in times of crisis.

This level of trust is essential because in order for information about security concerns and incident response activities to be useful to companies and to the government, it must be shared quickly. This need for expediency may result in reports that are initially incomplete and potentially inaccurate, and there can be unintended consequences if the information is not treated with the appropriate care. This trusted environment has also allowed industry and government partners to engage in periodic “exercises” to test the potential impact of different threat scenarios based on accurate network data assessment from multiple carriers.

The National Reliability and Interoperability Council (NRIC)

Another example of the partnership that has worked and should be the model for any government and industry problem solving is the Network Reliability and Interoperability Council (NRIC). First organized by the Federal Communications Commission (FCC) in 1992, the NRIC was established following several telecom outages to study the causes of the outages and to make recommendations to reduce their number and effects on consumers. Since then, some 50 telecom carriers, equipment manufacturers, state regulators and consumers have participated. This has been a standing committee for over 10 years, and is a forum where industry and government come together for the good of the industry to work specific issues. Y2K was one such issue. NRIC VI was focused on Homeland Security with teams addressing both physical and cyber security and NRIC VII is further advancing this work. The product is a extensive set of best practices (proven processes used in the industry) for service providers, network operators, and equipment/software vendors to use to mitigate risk of attacks, as appropriate, based on internal analysis.

Another feature of NRIC is the monitoring and analysis of the performance of the public switched network based on reliability data collected during the last 10 years. The Network Reliability Steering Committee (NRSC), a voluntary industry committee, reviews each outage report submitted to the FCC, looks for trends, publishes the results quarterly and annually, and looks for ways to improve the collective performance of the network. A new phase of this work, currently underway in the NRSC, is collecting similar outage data on wireless, cable and ISP networks in order to conduct data analysis, enable performance improvement, and develop new best practices. In order for this effort

to be successful, it must be: 1) voluntary; 2) developed by industry experts; and 3) adaptable by different network providers to reflect differing architectures and approaches.

Safeguarding sensitive proprietary information:

As a private sector operator of a major part of one of America's most important critical infrastructures, we carefully safeguard all information about the physical locations, capabilities and components of our world-wide infrastructure. An ongoing major concern of the industry remains the public dissemination and availability of critical infrastructure information (communications that have been identified as part of the national critical infrastructure) to someone who has a desire to do harm to the national communications network.

Despite these concerns, we are increasingly solicited by various governmental entities for very specific, extremely sensitive, proprietary information about our capabilities and maps of our network facilities and routes.

States are attempting to compile lists of the critical assets of AT&T and other carriers for purposes of critical infrastructure protection. New York, for example, is seeking to establish a state-wide database that would reflect the location of all telecommunications infrastructure in the state and the number of customers that would be impacted if each location failed. New York has also approved a recommendation to ask local telecommunications carriers to offer certain "critical" customers access to information on where their circuits are routed. This would effectively provide a partial map of AT&T's overall infrastructure assets, and would potentially be aggregated with infrastructure assets of other service providers as well. In the wrong hands, this compilation of critical infrastructure assets only increases the vulnerability of the critical

telecommunications infrastructure. In Michigan and Maine, carriers are required to provide detailed infrastructure information, including routing maps. Other states have also imposed similar requirements. The FCC, too, has sought to require telecommunications carriers to file periodic reports with the Commission that include extensive information on problems and vulnerabilities identified in the telecommunications network. The FCC's proposed network outage reporting requirements, for example, would require telecommunications carriers to identify the location of every network outage and document the magnitude of its impact.

While well-intended, such requirements would greatly hinder our security efforts. As a practical matter, we must be able to react and respond immediately to new information, rather than first comply with a government mandated process. In this very important area, we need to be able to modify our designs and plans with a continued primary focus on reliability and security, not regulatory compliance.

More importantly, extremely sensitive network information is best kept closely guarded by the individual provider. In the past, as a result of such information gathering efforts, maps have actually been published in newspapers, in an attempt to inform citizens where an attack might be most likely to occur and what impact could be expected. In one prominent New York City newspaper, for example, a map was published showing the location of every chemical plant in the area along with the number of citizens that would be harmed if that facility were attacked.

If our critical infrastructure maps and information were filed and amassed with similar information from other providers, it would create a significantly enhanced security risk. Unlike other parts of the nation's critical infrastructure, such as dams and

power facilities, there is currently no ready way for terrorists to identify and develop a comprehensive list of communications networks and infrastructure locations. Such locations are numerous, often out of sight, and in the control of different providers. The lack of centralized information provides a degree of security for these facilities that should not be disrupted.

Filing such information with numerous government agencies and constituencies would greatly raise the risk of its release. While various agencies have the full intention to keep such information confidential, the fact is that persons less familiar with the network are not always able to identify that data which is most sensitive, and could unintentionally expose information that makes our network vulnerable to attack. Agencies outside the “security triangle” do not always have specific procedures for housing and handling information critical to national security.

In order to ensure that all information provided, which contains critical infrastructure information, is protected from public disclosure, it should be routed through one federal governmental agency. That agency should be the Department of Homeland Security. By initially providing voluntary reporting to the DHS, in the event of a terrorist attack or act of nature that affects all major utilities, including the communications infrastructure, one agency would maintain responsibility for leadership of all coordinating restoration efforts. The coordination of a unified response would result in greater efficiency in the restoration and recovery process. Further, the DHS process for administering the protection of critical infrastructure information should be refined to limit access to those entities on a need-to-know basis.

AT&T is concerned about the breadth, open-endedness, lack of specificity, potential cost, and ability to safeguard and keep confidential any information that is provided. Neither states nor the federal Government should expect to receive this information directly from the network operators. First, security-related information that is provided to government entities outside the federal Department of Homeland Security may not be adequately protected from federal and state Freedom of Information laws. Even more importantly, it is not clear that information collected on a wholesale or generalized basis advances homeland security in any way, and may inadvertently create greater risks to homeland security. In fact, proper analysis of any potential vulnerability requires a detailed assessment of the specific facilities of concern, the services they support, and the impact mitigation strategies applicable to those services. Instead of making arbitrary requests for massive downloads of extremely sensitive information, states should work with the Department of Homeland Security (DHS) and directly with critical infrastructure providers to determine what specific information is really needed and to establish coordinated processes and procedures. The DHS should be the appropriate focal point for the coordination across the regions, states, and municipalities, as well as across key industry sectors, to ensure that the information is useful, responsive, and properly managed.

In this time of elevated terror threat levels, we must all take every step necessary to protect America's citizens. At AT&T, we are living up to that responsibility in the fullest manner every day. But in some cases, a "need to know" better protects America than a "need to share." We ask that you carefully consider the security ramifications of wider information sharing as you proceed in your deliberations.

AT&T would like to particularly thank Chairman Davis and the Members of this Committee for holding a hearing on this important issue. I offer AT&T's assistance to the Committee as well as my own, and I would be glad to answer any questions you may have.