



Alarm Industry Communications Committee

VIA ELECTRONIC DELIVERY

January 27, 2010

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Room TWA325
Washington, DC 20554

RE: Reply Comments Sought in Support of National Broadband Plan – NBP Public Notice 30
Reply to Comments of AT&T Inc. on the Transition from the Legacy Circuit-Switched
Network to Broadband – NBP Public Notice #25
GN Docket Nos. 09-47, 09-51, 09-137

Dear Ms. Dortch:

The Alarm Industry Communications Committee (“AICC”), on behalf of its members, hereby responds to the comments submitted by AT&T in the above-referenced docket, concerning the transition from the circuit-switched network to broadband and IP-based communications. Effective, reliable communications networks are a vital component of the services provided by the alarm industry. Accordingly, AICC supports a plan of orderly transition to broadband and IP-based communications that ensures communications to all Americans operate with a high degree of reliability and that ensures compatibility with existing services and equipment.

The AICC is comprised of representatives from all segments of the alarm industry, including central station alarm companies, alarm monitoring centers, alarm installation companies, alarm manufacturing companies and the associations representing the majority of such companies operating in the United States.¹ Alarm companies protect a wide range of

¹ The AICC’s members are comprised of the Central Station Alarm Association (“CSAA”), the Electronic Security Association (“ESA”) (formerly the National Burglar & Fire Alarm Association), the Security Industry Association (“SIA”), Bosch Security Systems, Digital Monitoring Products, Digital Security Control, Telular, Honeywell Security, Vector Security, Inc., ADT Security Services, Inc., AES-IntelliNet, GE Security, Alarm.com, Emizon LLC, Intertek Testing, Security Network of America, Numerex and Underwriters’ Laboratories. CSAA, ESA, and SIA are comprised of central station alarm companies, alarm monitoring

sensitive facilities, businesses and residences and the occupants of each from fire, burglary, sabotage, and other emergencies. For example, they protect government offices, power plants, hospitals, dam and water authorities, pharmaceutical plants, chemical plants, banks, and schools and universities. In addition, alarm companies protect approximately 20 million residences from burglary, duress, carbon monoxide and fire. They also provide medical alert services (e.g., obtaining ambulances) during medical emergencies. Approximately one-third of Americans today live in, work in and go to premises where security systems are utilized. Accordingly, many Americans would be impacted if the public switched telephone network (PSTN) is retired before there is a thorough understanding of how it is relied upon everyday in security applications to protect them from harm.

For example, monitored alarm systems must comply with various codes and it is important to ensure that the codes can be revised to accommodate new technologies. Residential and commercial fire alarm signaling systems must comply with NFPA 72, the National Fire Alarm Code. Until 2010, the code allowed the use of the PSTN for transmitting fire alarm signals. Since many consumers are given an insurance discount for using a monitored security system, consumers' migration to non-code, Voice over Internet Protocol (VoIP)-based telephony services put them at risk of being denied a claim since said digital voice services were not permitted by the national fire code. As of 2010, the NFPA code was modified to allow the use of digital phone services provided as part of a Managed Facilities Voice Network (MFVN.) (Examples of MFVN service include Verizon FiOS, AT&T U-Verse and Comcast digital voice.)

In addition, the legacy nature of the PSTN has resulted in a network that is believed to have an extremely high level of availability, often referred to as having "five 9's" or 99.999% up-time. Users of security and fire alarm systems installed over the last 30 years have depended on the PSTN to deliver with certainty, alarm signals to a centralized location where professional staff monitor the alarm signals and dispatch appropriate first responders as needed. This reliance on the PSTN for life safety applications is a direct result of the PSTN being engineered to assure a high probability of call completion. It should be assured that the networks that are proposed to replace the PSTN have the same Quality of Service that the PSTN offers. This assurance needs to take into account the service windows and associated downtimes that are part of the migration to network-based telephony systems. AICC notes that like the PSTN, alarm central monitoring stations have sufficient redundancy to remain operational when equipment and software are upgraded and believes that no less should be provided by proposed communications networks.

As the Katrina report highlighted, power back-up for communications networks is a concern. The power back-up requirements for newly proposed communications networks should be reviewed.

With respect to the request for a firm sunset date for the PSTN, AICC urges the Commission to ensure that any transition period provide sufficient time to ensure that broadband compatibility with existing life-safety services and equipment is achieved. The security industry has gained considerable experience in recent years as consumers have begun migrating to VoIP-

centers, alarm installation companies and alarm manufacturing companies. Their memberships represent the majority of such companies operating in the United States.

based telephony services as offered by cable television companies as well as by the legacy PSTN providers. The lessons learned to date are valuable, but are not necessarily valid when applied to the sheer scale of a possible PSTN sunset and the wholesale conversion to packet-based networks such a sunset would entail. As an example of one significant challenge, alarm systems use a feature known as line seizure. Line seizure allows an alarm panel to seize control of a phone line if alarm signals need to be transmitted to a monitoring center. Some providers of VoIP-based telephony do not take line seizure into account and bypass the line seizure device, rendering it inoperable.

Additionally, the protocols used by alarm panels were designed to operate within the “voice” range of the spectrum and, therefore, within the voice frequency range specification of the PSTN. Alarm companies have worked closely with broadband voice providers to assure compatibility between alarm protocols and the voice codecs (coder – decoder) deployed as part of the packet-switched voice network. However, as stated above, this is a matter of scale. The wholesale conversion of the PSTN to packet-based voice services provided by broadband providers must be “managed” so that compatibility can be maintained, thus assuring that life-safety systems are not rendered useless.

Despite the safeguards put in place, consumer conversions to VoIP-based digital telephony systems can cause problems if the correct practices are not followed. It is for this reason that the alarm company should be notified when an alarm customer switches to VoIP service.

The AICC sees great potential for the use of broadband and IP-based communications in connection with alarm services. For example, whereas the PSTN allows for simplistic forms of data transmission, broadband provides the ability to transmit more data at faster speeds from protected premises and to forward this data to an alarm monitoring central station. Broadband also provides the ability for services such as video from the premises and other techniques that will reduce false dispatches and help response times. In addition, broadband service will aid medical alarm systems (called PERS or Personal Emergency Response Systems) by making the transfer of medical vital signs and other medical data more feasible.

However, the ability of the alarm industry to rely on broadband and IP-based communications will be hindered if all aspects of the communications path are not reliable. Further, AICC supports a gradual transition to broadband and IP-based communications to ensure compatibility with existing services and equipment.

Respectfully submitted,

/s/ Louis T. Fiore

Louis T. Fiore

Chairman

Alarm Industry Communications Committee