

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

| | | |
|--|---|---------------------------------------|
| In re |) | |
| |) | |
| Public Safety, Homeland Security, and |) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Cybersecurity Elements of National Broadband |) | PS Docket Nos. 06-229, 07-100, 07-114 |
| Plan; National Broadband Plan Public |) | WT Docket No. 06-150 |
| Notice #8 |) | CC Docket No. 94-102 |
| |) | WC Docket No. 05-196 |
| _____ |) | |

COMMENTS OF AT&T INC. — NBP PUBLIC NOTICE # 8

Robert Vitanza
Gary Phillips
Paul Mancini

AT&T Inc.
1120 20th Street, NW
Suite 1000
Washington, DC 20036
(202) 457-3076 – phone
(202) 457-3073 – facsimile

Its Attorneys

November 12, 2009

TABLE OF CONTENTS

| | Page |
|--|-------------|
| I. INTRODUCTION AND SUMMARY | 1 |
| II. RESPONSES | 4 |
| 1. Public Safety Wireless Broadband Networks | 4 |
| 2. Next Generation 911 (NG911)..... | 24 |
| 3. Cybersecurity | 32 |
| 4. Alerting | 51 |
| III. CONCLUSION..... | 55 |
| AT&T Information & Network Security Customer Reference Guide | Appendix A |

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

| | | |
|--|---|---------------------------------------|
| In re |) | |
| |) | |
| Public Safety, Homeland Security, and |) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Cybersecurity Elements of National Broadband |) | PS Docket Nos. 06-229, 07-100, 07-114 |
| Plan; National Broadband Plan Public |) | WT Docket No. 06-150 |
| Notice #8 |) | CC Docket No. 94-102 |
| |) | WC Docket No. 05-196 |
| |) | |

COMMENTS OF AT&T INC. — NBP PUBLIC NOTICE # 8

AT&T Inc., on behalf of itself and its affiliates (“AT&T”), respectfully submits these comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) National Broadband Plan (“NBP”) Public Notice #8 (“*Public Notice*”), which seeks comments on the interplay between the NBP and various security concerns.¹

I. INTRODUCTION AND SUMMARY

To inform the NBP, the Commission seeks a better understanding of the impact of broadband communications on homeland security. Specifically, the *Public Notice* requests comments on four major communications initiatives that impact security: (1) deployment of a public safety wireless broadband network; (2) next generation 911 (“NG911”); (3) cybersecurity; and (4) emergency alerting. The instant comments address the Commission’s specific questions and detail how the communications industry’s broadband efforts – coupled with regulatory flexibility – will continue to boost the nation’s security. AT&T has been an active participant in

¹ *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice #8, GN Docket Nos. 09-47, 09-51, and 09-137, PS Docket Nos. 06-229, 07-100, and 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196, DA 09-2133 (rel. Sept. 28, 2009) (“*Public Notice*”).

efforts to advance the country's goals in all of these areas. AT&T hopes that the instant comments inform the Commission as to the significant role the company and other commercial broadband providers play – and should continue to play – in addressing these important topics.

With respect to the deployment of a national interoperable wireless broadband public safety network, AT&T reiterates that the Commission should adopt a “leveraged network” model.² First, Congress should repurpose the 10 MHz of 700 MHz D-Block commercial spectrum (758-763/788-793 MHz) for public safety broadband use. Coupled with the 10 MHz of 700 MHz broadband spectrum licensed to the Public Safety Spectrum Trust (“PSST”) (763-768/793-798 MHz), the D-Block spectrum would give public safety entities a full 20 MHz of broadband spectrum, the amount of spectrum necessary to support advanced applications at fourth generation (“4G”) data rates for multiple users. Second, the Commission should encourage public safety entities to use a standard Request for Proposal (“RFP”) process – perhaps with PSST consultation – to negotiate agreements with commercial operators on a regional basis and leverage existing and future commercial networks based on the unique needs of local and regional public safety agencies. Third, the Commission should establish technological standards and minimum system requirements for these public safety broadband systems and ensure that all networks adopt the LTE radio technology platform and infrastructure. Ultimately, nationwide interoperability would be achieved by linking the 700 MHz local and regional networks and establishing reciprocal roaming agreements and credentialing procedures between all public safety entities.

The instant comments also explore how broadband technologies will improve NG911 communications between the public and emergency responders. Although individuals will still

² For a detailed discussion of the “leveraged network” model, *see* Comments of AT&T, Inc., PS Docket 06-229, at 12-20 (filed Oct. 16, 2009) (“Comments of AT&T”).

be able to dial “911” on traditional wireline and wireless phones, NG911 capabilities will enable public safety answering points (“PSAPs”) to receive text messages, digital photos, streaming video, and other forms of data sent from future wireless, VoIP, or broadband enabled devices. The elimination of dated laws and regulations will be necessary at several levels of government to facilitate the new technologies and the network and data sharing essential to NG911 service.

The comments also explain the serious economic and national security threats cyberattacks continue to pose. However, both the communications industry and the Federal government are investing heavily to prevent cyberattacks and to mitigate the potential damages they can cause. The success of these cybersecurity efforts will continue to increase as the communications industry and the government coordinate efforts to most effectively leverage their unique resources and capabilities.

AT&T also addresses how public emergency alert and warning system effectiveness will significantly improve with the move towards broadband technologies and the adoption of the next generation Emergency Alert Systems (“EAS”), which includes the Common Alerting Protocol (“CAP”) and the next generation Commercial Mobile Alert System (“CMAS”). Broadband services like AT&T’s U-verse TV will enhance the utility of emergency alerts by quickly adopting the CAP and the next generation CMAS, which will likely: improve the text content of alerts by putting together more meaningful event information; support recorded and streaming audio for all alerts; enable alerts in multiple languages; and support enhanced message update and cancellation features for alerts as well as local Governments alerts with character free form text.

Ultimately, AT&T’s responses to the questions in the *Public Notice* show that the communications industry continues to make significant progress in deploying broadband

technologies and leveraging these technologies to enhance national security. Going forward, the communications industry will continue to require flexibility, not additional regulation, to better address these areas. Regulators at all levels of government should enhance this flexibility by removing regulatory roadblocks and pursuing effective voluntary partnerships between the government and industry.

II. RESPONSES

1. Public Safety Wireless Broadband Networks

a. How are public safety agencies making use of broadband networks today?

Comments: Today, public safety agencies use commercial broadband networks primarily for non-mission critical data applications, such as license plate identification, vehicle location information, computer aided dispatching, and incident report filing. Now and for the foreseeable future, the public safety community considers voice applications (*e.g.*, “one-to-many” dispatches and direct unit-to-unit communications conducted without accessing any fixed infrastructure) to be the most mission critical.³ These voice applications rely primarily on existing, privately operated and maintained Land Mobile Radio (“LMR”) systems rather than broadband networks. In the near future, the introduction of 4G LTE networks, coupled with the formation of public/private partnerships, will see the further development of integrated public safety applications conducted over commercial broadband networks and, in time, those applications will likely address mission critical voice requirements for public safety. However, for the foreseeable future, commercial broadband networks will augment existing LMR voice

³ Letter from Harlin McEwen, Chairman, PSST, to Jennifer A. Manner, Deputy Chief, Public Safety and Homeland Security Bureau, FCC, GN Docket No. 09-51 (filed Oct. 1, 2009) (“PSST Letter”), *available at* <http://fjallfoss.fcc.gov/ecfs2/document/view?id=7020040141>.

systems. Currently, approximately 1,500 government agencies use AT&T's data networks in this manner.

- b. **We seek specific details on both current and anticipated needs of the public safety community for mobile wireless broadband networks and applications. Specifically, we seek comment on:**
 - i. **The amount of anticipated peak, average, and cell edge broadband traffic and capacity requirements that public safety broadband use is generating and is expected to generate, and the number of current and anticipated public safety users.**

Comments: In a recent response to Commission questions directed to the PSST about the bandwidth requirements for public safety broadband applications, the PSST noted that predicting capacity and data rate requirements is difficult at this time because many public safety applications are still in early development.⁴ Also, because there are currently no broadband services available to public safety for wide-area use, the PSST implies that it is difficult to make assumptions about important factors that are needed to predict bandwidth requirements such as the number of simultaneous users in a given cell and the frequency of use of the application. AT&T agrees with the PSST's observations, but expects that public safety usage patterns will mimic the usage patterns experienced by commercial providers.

Commercial data use has exploded over the last several years. AT&T's wireless data traffic, for example, has increased by nearly *5,000 percent* in the past 12 quarters.⁵ Other carriers have reported similar dramatic increases.⁶ This trajectory is expected to continue.⁷

⁴ *Id.* at 2.

⁵ Kris Rinne, AT&T Senior Vice President, Architecture and Planning, *Tuesday Keynote*, 4G World, at 5 (Sept. 15, 2009); *see also* Kevin Fitchard, "4G World: AT&T Says HSPA+ Is Off the Table for Now," *TelephonyOnline* (Sept. 15, 2009), *available at* <http://telephonyonline.com/3g4g/news/Rinne-4gworld-keynote-091509> (last visited Nov. 10, 2009) ("data traffic on [AT&T's] 3G network has grown by almost 5000% in the last three years") ("*Fitchard*").

⁶ *See, e.g.*, Letter from Kathleen O'Brien Ham, Vice President, Federal Regulatory Affairs, T-Mobile, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 09-51, WT Docket No. 06-150, PS Docket No. 06-229, WT

Further, the deployment of broadband public safety networks will lead to the development of the advanced, bandwidth-intensive 4G applications that public safety needs and desires.

To ensure the efficient delivery of these applications to users and to accommodate the increased data traffic that the use of those applications will cause, public safety will require a full 20 MHz of contiguous spectrum (10 MHz uplink and 10 MHz downlink). Combining the 5 + 5 MHz block currently allocated for public safety broadband use with the adjacent 5 + 5 MHz D-Block creates two 10 MHz paired blocks, which are capable of supporting broadband and multi-media applications for a large number of simultaneous users during multi-agency response efforts in discrete geographic areas. If less than 20 MHz of broadband spectrum is available, the network congestion caused by advanced services and applications may foreclose some public safety users from accessing the network, thereby impacting interoperability and potentially stranding roaming first responders. As Bruce Gottlieb, aide to Chairman Genachowski, recently explained, “[d]emand for more capacity is exploding and increased spectral efficiency can only do so much.”⁸

ii. The type of traffic or users’ patterns and usages anticipated for broadband services associated with critical, medium and low demand theater operations.

Major incidents involving significant public safety response create congestion on commercial networks. This was true on September 11, 2001, when both consumer and public

Docket No. 05-265, WT Docket No. 00-193, WC Docket No. 05-25, at 9 (filed Aug. 6, 2009) (“T-Mobile G1 customers use 50 times the data of the average T-Mobile customer”).

⁷ See Declaration of Thomas Hazlett, ¶ 14, attachment to Comments of AT&T Inc., GN Docket No. 09-157 (filed Sept. 30, 2009) (“AT&T Sept. 30 Comments”); Gerald Faulhaber and David J. Farber, “Innovation In The Wireless Ecosystem: A Customer-Centric Framework,” at 9-10, attachment to AT&T Sept. 30 Comments; Michael L. Katz, “Public Policy Principles For Promotion Efficient Wireless Innovation And Investment,” ¶ 17, attachment to AT&T Sept. 30 Comments.

⁸ Howard Buskirk, “Google Voice Probe Shows Changes Overtaking Wireless Industry, Gottlieb Says,” Communications Daily (Sept. 16, 2009).

safety demand swamped commercial networks. It was also true in 2006 after the Amish school shooting incident in rural Pennsylvania. This more recent occurrence of congestion can be attributed more to public safety use, given the low population density of the surrounding area. Based on this history, AT&T anticipates that commercial networks will experience high-volume broadband traffic patterns from public safety users during critical and medium demand theater operations.

The most effective way to prevent congestion in the first place is to address bandwidth constraints upfront and dynamically engineer networks. For public safety, the best way to address bandwidth constraints – and thereby prevent congestion during emergencies – is to reallocate the 10 MHz of 700 MHz D-Block commercial spectrum to public safety for use in tandem with the existing 10 MHz of 700 MHz public safety broadband spectrum. This will create two 10 MHz blocks of contiguous spectrum that can be paired to support broadband and multimedia applications for a large number of users.

iii. Applications support requirements and associated data rates for both the down link and uplink operations and associated Quality of Service requirements.

Comments: The 4G LTE networks that AT&T and other 700 MHz carriers are preparing to deploy will be designed to achieve peak download speeds of 326 Mbps and peak upload speeds of 86 Mbps. These speeds will support a broad array of beneficial new applications, services, and devices – including important advances for public safety. These data rates are necessary to support the simultaneous offering of broadband applications and services within a cell site.

Specifically, the LTE standard will enable public safety to engage in real-time visual networking, transmit videos wirelessly from camcorders, and download full-motion videos of road conditions or other hazardous situations. Other examples of beneficial public safety

applications that AT&T expects to arise from LTE include: mobile voice, push-to-talk (“PTT”) voice, location services, database transactions, messaging, network operations data, dispatch data, generic traffic, telemetry, and virtual private networking.

iv. Current and anticipated public safety device and applications needs.

Comments: Public safety currently uses portions of its 700 MHz band spectrum allocation for narrowband, mission critical voice systems. State and local governments have spent millions of dollars to implement LMR public safety voice systems in this spectrum band, although deployment of such systems has been sporadic over the past decade due to the extension of the Digital Television transition and a lack of funding.⁹

AT&T anticipates that future public safety devices, including those that access the narrowband networks described above, will also be designed to operate over the 758-768 MHz and 788-798 MHz bands, which is the Upper 700 MHz D-Block spectrum and public safety broadband spectrum. This will allow public safety to utilize high bandwidth broadband applications such as video, location-based services, messaging, and virtual private networking. As public safety and 700 MHz commercial network operators pursue private/public partnerships, public safety devices may also incorporate other 700 MHz commercial spectrum bands to expand capacity and promote nationwide roaming opportunities. To that end, AT&T has approached its device vendors about adding the 700 MHz commercial and public safety spectrum bands into standard commercial devices. While AT&T is still evaluating the feedback from its vendors, early indications are that a device that works on all 700 MHz public safety

⁹ See Letter from Harlin McEwen, Chairman, Communications and Technology Committee of International Association of Chiefs of Police, to Julius Genachowski, Chairman, FCC, PS Docket No. 06-229 (Oct. 12, 2009) (“IACP Letter”), available at <http://fjallfoss.fcc.gov/ecfs2/document/view?id=7020141265> and <http://fjallfoss.fcc.gov/ecfs2/document/view?id=7020141266>.

broadband networks is feasible and can be available in a late 2011 or 2012 timeframe at near commercial prices.

- v. **The corresponding extent of broadband infrastructure and backhaul that would be required to support public safety applications, and what technologies and solutions do public safety use or anticipate using to meet these requirements.**

As noted above, the sharp spike in ordinary consumer use of wireless broadband foretells significant public safety interest in wireless broadband as well. AT&T expects that, with increased public safety demand, the need to utilize existing carrier infrastructure and commercial backhaul will also rise sharply. The “leveraged network” model for public safety broadband deployment addresses these needs and provides public safety with the fastest route to securing sufficient broadband infrastructure and backhaul capabilities.

Under the “leveraged network” model, as discussed more fully below, public safety entities would use a standard RFP process to negotiate agreements with commercial operators, system integrators, infrastructure vendors, and tower site vendors for network equipment and systems based on the public safety entity’s preferred network management model. Leveraging commercial networks would take advantage of the economies of scope and scale of commercial broadband infrastructure and technology to significantly reduce the cost and speed the deployment of public safety broadband networks. Indeed, the “leveraged network” model would reduce the time necessary for actual network deployment, as the vast majority of sites would be collocated with commercial operations.

For the same reasons, AT&T anticipates that the “leveraged network” model would speed public safety’s access to the backhaul needed for new bandwidth-heavy applications. Public safety additionally would benefit from the recent increase in commercial broadband traffic, which has prompted many commercial providers to develop innovative backhaul solutions. For

example, commercial carriers have defined a clear need to replace traditional T1s with fiber in urban areas, and virtually all wireless carriers are currently engaged in major projects to upgrade backhaul facilities to fiber.¹⁰ Cable companies are also investing in fiber and Ethernet connectivity to seize the opportunity to capture additional backhaul traffic. Use of microwave backhaul is additionally increasing.¹¹ Clearwire recently indicated that 90 percent of its wireless network is served by microwave backhaul (confirming what the rest of the industry knew for years – that microwave backhaul is economically viable and extremely efficient).¹² And participants in the Commission’s broadband workshops uniformly have noted that microwave is rapidly becoming a commonly used option outside of major metropolitan areas.¹³ The “leveraged network” model will enable public safety to benefit from this investment and innovation.¹⁴

¹⁰ See Neville Ray, Senior Vice President, Engineering, T-Mobile USA, Jake MacLeod, Principal Vice President and Chief Technology Officer, Bechtel Telecommunications, and Stephen Bye, Vice President, Wireless, Cox Communications, Remarks at the Wireless Deployment Workshop, at 45-48 (Aug. 12, 2009), *transcript available at* http://www.broadband.gov/docs/ws_03_deploy_wireless_transcript.pdf (last visited Nov. 10, 2009).

¹¹ See, e.g., Ed Evans, Chairman and Chief Executive Officer, Stelera Wireless, Remarks at the Wireless Deployment Workshop, at 20 (Aug. 12, 2009), *transcript available at* http://www.broadband.gov/docs/ws_03_deploy_wireless_transcript.pdf (last visited Nov. 10, 2009); Tarun Gupta, Vice President, Strategic Development, FiberTower, Remarks at the Spectrum Workshop (Sept. 17, 2009), *webcast available at* http://www.broadband.gov/ws_spectrum.html (last visited Nov. 10, 2009).

¹² See John Saw, Ph.D, Senior Vice President and Chief Technology Officer, Clearwire, Remarks at the Spectrum Workshop (Sept. 17, 2009), *webcast available at* http://www.broadband.gov/ws_spectrum.html (last visited Nov. 10, 2009).

¹³ See generally Remarks at the Wireless Deployment Workshop, at 20 (Aug. 12, 2009), *transcript available at* http://www.broadband.gov/docs/ws_03_deploy_wireless_transcript.pdf (last visited Nov. 10, 2009); Remarks at the Spectrum Workshop (Sept. 17, 2009), *webcast available at* http://www.broadband.gov/ws_spectrum.html (last visited Nov. 10, 2009).

¹⁴ For public safety communities to fully leverage the innovation unleashed by the transition to 3G and 4G networks, the Commission must ensure that its policies encourage competing suppliers to build the high-capacity fiber and microwave backhaul needed to support these networks.

- vi. **Specific network features and anticipated architecture that will allow the broadband network to operate seamlessly with disaster recovery capabilities nationwide, and the kind of connectivity needed with legacy and other commercial networks.**

Comments: The public safety community will reap substantial benefits by adopting LTE technology. LTE will support public safety’s need for voice, video, and data communications with high bandwidth and low latency, which can significantly improve first-responder access to mission-critical high-bandwidth communications applications. Moreover, LTE will capitalize on the research and development currently underway by commercial wireless providers that will be adopting LTE, including AT&T, Verizon Wireless, Cox Communications, Leap Wireless, MetroPCS, and US Cellular. Public safety will also benefit from the cost savings driven by using LTE, which has the advantage of global economies of scale derived from user pools exceeding two billion and compatibility with future networks.¹⁵

Public safety support for LTE as the broadband technology platform of choice is nearly unanimous. The Association of Public-Safety Communications Officials International (“APCO”) and the Executive Committee of the National Emergency Number Association (“NENA”) have both endorsed LTE as the network technology for public safety wireless broadband networks.¹⁶ So too has the PSST¹⁷ and the National Public Safety Telecommunications Council (“NPSTC”).¹⁸

¹⁵ 4G technology selection work is actively under way in the ITU-R (under the terminology IMT-Advanced) with full participation by global industry and governments. To date, this group has not sanctioned any technologies as 4G. However, the 4G requirements, evaluation criteria, and timelines have been defined by ITU-R, and the LTE enhancements meet/exceed these criteria. 3GPP will submit “LTE-Advanced,” which is planned as Release 10 of LTE, as the preeminent 4G candidate. Final industry-wide candidate technology submissions were made in October 2009 to ITU-R as entries in the defined ITU-R IMT-Advanced (4G) selection/confirmation process. See “IMT—Advanced Submission and Evaluation Process,” Int’l Telecommunications Union, <http://www.itu.int/ITU-R/index.asp?category=study-groups&mlink=rsg5-imt-advanced&lang=en> (last visited Nov. 10, 2009).

¹⁶ See “APCO & NENA Endorse LTE as Technology Standard for the Development of Nationwide Broadband Network,” APCO Press Release (June 9, 2009) available at <http://www.apco911.org/new/news/>

AT&T has also advocated that the Commission impose uniform criteria for local and regional public safety network builds in order to promote interoperability and roaming capabilities with other public safety networks.¹⁹ AT&T refers the Commission to the NPSTC Broadband Task Force Report (“BBTF Report”), which recently set the recommended minimum requirements for regional 700 MHz broadband networks to ensure future interoperability and compatibility with the proposed national public safety broadband network.²⁰ The BBTF Report, which NPSTC recently forwarded to the PSST, is the most complete and well thought-out list of conditions to advance the build-out of public safety networks.

vii. Definition and quantification of both mission critical voice and mission critical data.

Comments: Mission critical communications encompass any factor (*e.g.*, equipment, process, procedure, software) that is crucial to the successful completion and maintenance of voice calls or the successful and entire transmission of data. As stated earlier, public safety officials consider voice communications to be the most critical application that first responders require.

nena_endorse_lte.php (last visited Nov. 10, 2009).

¹⁷ “PSST Endorses LTE for Nationwide 700 MHz Band Network,” TR Daily (July 24, 2009).

¹⁸ “NPSTC Endorses LTE as Air Interface for Nationwide 700 MHz Band Network,” TR Daily (June 10, 2009). NPSTC’s governing board consists of fifteen voting and two non-voting organizations and, thus, represents a broad range of public safety interests. See “Who or What Is NPSTC?,” <http://www.npstc.org/npstcintro.jsp> (last visited Nov. 10, 2009).

¹⁹ Comments of AT&T at 9-12.

²⁰ “NPSTC 700 MHz Broadband Task Force Report and Recommendations,” NPSTC (Sept. 4, 2009), available at http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf (last visited Nov. 10, 2009) (“BBTF Report”).

viii. Specific requirements for hardening of cell sites and other network facilities, and for other requirements of network survivability and disaster recovery.

Comments: A successful network survivability and disaster recovery strategy for public safety should focus on the successful and prompt restoration of the network after an outage or disaster. Such a strategy should not attempt to provide full backup of every service, every circuit, and every server and system in the environment. This is both unnecessary and cost-prohibitive.

Rather, a successful network survivability and disaster recovery strategy should (1) minimize and/or avoid single points of failure in the system design; (2) ensure that service is restored as quickly as possible; and (3) ensure that services are easily accessible and widely available. Networks can minimize single points of failure by emphasizing redundancy in all mission critical network components, such as installing on-site backup power at all mission critical cell sites and redundancy of the backhaul connection between an antenna site and the core infrastructure. Ultimately, natural disasters and most outages cannot be prevented or, in many cases, even predicted. But with careful planning through effective public/private partnerships, the impact of a disaster can be substantially mitigated.²¹

For its part, AT&T already has invested over \$500 million in its network disaster recovery program. This program insures network reliability by harnessing the following assets, among others: specially-designed semi-tractor trailers strategically located around the U.S. for dispatch, as needed, to act as a virtual network office; mobile command centers that provide

²¹ Additionally, the Network Reliability and Interoperability Council (“NRIC”) has promulgated numerous best practices covering issues of disaster recovery and network hardening, which network operators may consult and implement as appropriate. *See, e.g.*, NRIC VII Recommendation 7-6-1007 (recommending that network operators consider establishing a geographically diverse back-up Emergency Operations Centers), *available at* <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-6-1007>; NRIC VII Recommendation 7-7-0546 (recommending that network operators minimize single points of failure in paths linking network elements deemed critical to the operations of a network), *available at* <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-7-0546>.

emergency response teams with fully equipped and controlled office space in the event of a disaster and that can be rapidly deployed and set up at a recovery site; self-contained mobile cell sites (*i.e.*, cells on wheels (“COWs”) and cells on light trucks (“COLTs”)) to replace a failed cell site or supplement cellular capacity during times of increased demand; emergency communications vehicles that use a satellite link to provide command communications during the initial phase of a recovery effort; emergency equipment located at designated locations, such as portable generators, chillers, pumps and fuel cells placed at network offices deemed at risk and permanent generators and battery backup at all wireless switches and many cell sites; and managers, engineers and technicians who are trained in network recovery and participate in periodic recovery exercises to ensure they are prepared when disasters occur.

ix. Any studies or other data demonstrating whether and how the requirements needed for urban, suburban, and rural environments currently differ and how they are expected to differ in the future.

AT&T does not believe that users in urban, suburban or rural environments will have differing data requirements. However, as a practical matter, public safety users in rural areas will typically operate with less than peak data rates more often than urban and suburban users. In mobile broadband systems, data rates are dependent on the distance between the mobile device and the fixed infrastructure transmitter or base station. As the distance between the two is increased, the data rate is reduced in order to maintain a robust transmission with low bit error rates. This is more likely to occur in rural areas where the density of cell sites will be less than in urban environments. On the other hand, rural users will typically have to contend with fewer broadband users in the same cell, which will improve their individual performance. Application providers need to consider these issues and ensure that functionality is maintained when data rates are reduced.

As demonstrated by the applications for waiver filed with the Commission to use the 700 MHz public safety spectrum, many larger markets will fund the build-out of their networks without assistance. In contrast, alternative funding will be needed for rural public safety networks.²² Federal funding is one option, through existing or future grant programs. Another option is for the PSST to bring in federal users to help with funding and utilization of the 20 MHz of spectrum, which is within the PSST's authority. Rural areas can also pool resources to achieve economies of scale when building regional networks. For example, Ohio's Multi-Agency Radio Communications System ("MARCS"), a voice and data network that utilizes state-of-the-art technology to provide interoperability to first responders and public safety throughout Ohio and a 10-mile radius outside of Ohio, demonstrates how a private/public partnership can fund the ongoing operation of a network.²³ The State of Ohio contracted with a private sector company to build MARCS. Through this public/private partnership, the State negotiated substantial discounts to pass on to the individual agencies, which buy directly from the vendor.²⁴ MARCS supports over 23,000 voice units and over 1,700 mobile data units from over 500 local, state, and federal agencies statewide.²⁵

Commercial communications operators can also serve rural areas by augmenting coverage with satellite service. For example, AT&T has partnered with satellite service provider

²² Even if rural areas obtain the right to use D-Block spectrum under the leveraged network model discussed in response to Questions 1.a.v. and 1.e., AT&T does not believe that spectrum leasing is a viable alternative for public safety to fully fund the build-out of their networks due to the value of spectrum in these areas and the resulting market lease rates.

²³ See Ohio Office of Information Technology, MARCS, "MARCS Facts," available at <http://www.oit.ohio.gov/sdd/marcs/> (last visited Nov. 10, 2009).

²⁴ For voice services, the network charges an annual fee of \$240 per subscriber and for data services \$4,200 per subscriber. See Ohio Office of Information Technology, MARCS, "MARCS Frequently Asked Questions," available at <http://www.oit.ohio.gov/SDD/Marcs/FAQAnswers.aspx> (last visited Nov. 10, 2009).

²⁵ *Supra* n. 23.

TerreStar Networks to offer back-up satellite service where terrestrial wireless service is unavailable in an integrated mobile device. The future presents the potential to adapt satellite coverage to public safety solutions.²⁶

- c. **We also seek concrete, itemized data on costs and resources necessary to satisfy public safety broadband needs for mobile wireless services.**

Comments: Next generation public safety networks can most effectively be built through an RFP process that encourages the sharing of commercial infrastructure. Leveraging commercial networks takes advantage of the economies of scope and scale of commercial broadband infrastructure and technology to significantly reduce the cost and speed the deployment of public safety broadband networks. It has been estimated that a nationwide network deployed using a “leveraged network” model would have initial capital expenditure costs of \$13 billion, with a 10-year operational cost of \$35 billion.²⁷ For a standalone public safety network, capital and operational expenditures for that same 10-year period would reach \$61 billion.²⁸ Thus, over a ten year period, the “leveraged network” approach would reduce the total cost of building, operating, and maintaining the network from an estimated \$61 billion to \$35 billion – a 43 percent savings. AT&T estimates that the total federal commitment until 2013 for this system would be about \$17-18 billion – less than one-third the cost of a stand-alone network.

Some of the most expensive and time-consuming parts of building and operating a

²⁶ AT&T expects its Integrated Cellular-Satellite Solution to be available in the first quarter of 2010. More information on AT&T’s Integrated Cellular-Satellite Solution is available at <http://www.wireless.att.com/businesscenter/business-programs/government/solutions/integrated-cellular-satellite-solution.jsp> (last visited Nov. 10, 2009).

²⁷ See Letter from John T. Scott III, Verizon Wireless, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 06-229, Appx. 2 at 4 (filed Apr. 4, 2007), available at <http://fjallfoss.fcc.gov/ecfs2/document/view?id=6519107918>.

²⁸ *Id.*

wireless network involve the operational support systems (“OSS”), which dynamically allocate spectrum, provision service, maintain network inventory, configure network components, and manage faults. The “leveraged network” approach would allow public safety to reduce these costs and delays by using a commercial operator’s core network and OSS.²⁹ Additionally, most commercial operators offer custom device management tools and even customized billing, eliminating the need for public safety to build and operate duplicative systems. The scale and scope of the commercial industry also ensures substantial cost savings for public safety in the purchase of handsets and other end-user devices.

- d. **We seek information on experiences and lessons learned to date by current public safety use of mobile wireless broadband networks (whether such networks are commercial or public safety-only), including use of such networks at central locations (e.g., emergency operations centers) and by public safety personnel in the field.**

Comments: To date, public safety agencies have not widely utilized commercial mobile broadband networks for mission critical applications. Rather, agencies utilize commercial broadband networks for non-mission critical data uses such as license plate identification, vehicle location information, computer aided dispatching, and incident report filing. The introduction of 4G LTE networks, coupled with the formation of public/private partnerships, will likely see the further development of integrated public safety applications conducted over commercial networks. Further, if one extrapolates broadband consumer use patterns to public safety, one can expect that the broadband bandwidth requirements for such users will be considerable.

Real-world data reveals that this expectation is legitimate. The Florida Department of Highway Safety & Motor Vehicles (“Florida Highway Patrol”), which uses AT&T’s network to

²⁹ Provisioning portals also may be provided to public safety, so public safety can add, delete or change features without direct involvement by the commercial operator.

connect with its fleet, has averaged monthly data usage of over 340,000 MB over the last two years. Florida Highway Patrol vehicles are equipped with systems for automatic vehicle location (“AVL”), the transmission of reports, automatic software updates, streaming audio and video, digital photograph uploading and downloading, digital roadside fingerprinting, and VoIP communications for roadside support. The Florida Highway Patrol advises that these applications help it weather headcount reductions. Troopers, given the tools to perform most office tasks in the vehicle via broadband communications, can spend more time on patrol in their communities, as a deterrent to crime. In the future, the Florida Highway Patrol expects to deploy applications that will further augment the efficiency of troopers in the field. These applications will include functionalities that allow troopers to broadcast digital video from their vehicles back to dispatch and command, enable dispatchers to remotely control in-car cameras, and grant troopers access to video-conferencing and training sessions from their vehicles

The City of Mountain View, California, which utilizes AT&T’s broadband network to connect its police and fire vehicles, has experienced a greater than 500 percent increase in wireless data usage over the last three years. During the same time period, the introduction of new systems and applications in selective vehicles, such as automated field reporting, limited online access to officer resource information and state and regional booking photo information, license plate recognition systems, and regional fire/EMS mutual aid/healthcare systems, has driven an increase in average monthly data use per device from 11.2 MB to 60.1 MB. City vehicles with access to more applications averaged much greater data usage, as monthly usage averaged 200-300 MB per month for vehicles with public internet access and approximately 700 MB per month for vehicles with license plate recognition systems. The City has indicated that it expects usage to further increase with the introduction of additional systems and applications,

such as AVL and other location-based services, in-car video systems, in-field biometric identification devices, and electronic citation systems.

- e. **We seek comment on what particular mobile wireless broadband needs could be satisfied by commercial broadband service providers in the short term and over the long term. Are there any assessment studies or field trials that show areas in which next generation mobile networks (4G) meet or do not meet Public Safety requirements?**

Comments: The quickest and most cost effective path to meet the mobile wireless broadband needs of public safety is to leverage the existing core network infrastructure of commercial carriers to build a network of networks that will ultimately provide an interoperable nationwide broadband network. The ability of commercial broadband network providers to meet public safety's needs now and in the foreseeable future utilizing this "leveraged network" approach is discussed in detail in AT&T's Comments filed in PS Docket No. 06-229.³⁰

- f. **Specific to wireless broadband platforms, what is the expected bandwidth usage for anticipated public safety applications in the short- and long-term?**

Comments: In response to Commission questions following the Public Safety and Homeland Security Workshop, the PSST explained that uncertainty about the future makes it difficult to assess the expected bandwidth requirements for anticipated public safety applications.³¹ AT&T agrees with this conclusion and with PSST's general assessment that video applications and map downloads will require significant bandwidth.³²

Regardless of the bandwidth requirements of any specific application, it is generally accepted that the current 10 MHz of spectrum allocated to broadband communications for public

³⁰ See Comments of AT&T, at 12-20.

³¹ See PSST Letter, at 2.

³² See AT&T's response to Question 1.d. above for the data usage experiences of the Florida Highway Patrol and the City of Mountain View, California Fire and Police Departments.

safety is inadequate to support anticipated public safety needs. In the words of NPTSC’s broadband taskforce: “During the work of the BBTF, it was apparent ... that the current 5+5 MHz of spectrum available for public safety use for broadband data systems will not be sufficient to support disaster operations.”³³ To provide public safety with a system that satisfies their short- and long-term bandwidth requirements, paired 10 MHz radio channels of 700 MHz spectrum (*i.e.*, 20 MHz of 700 MHz spectrum) should be fully allocated to public safety. The current Upper 700 MHz band plan, however, allocates paired 5 MHz channels for commercial broadband in the D-Block (758-763 MHz and 788-793 MHz bands) and paired 5 MHz channels for public safety broadband (763-768 MHz and 793-798 MHz bands). While this may allow both commercial and public safety operators to launch service, it should be recognized that in the future these spectrum blocks would be sub-optimal for both sets of users.³⁴ This approach would limit each network to a single 5 MHz channel (*i.e.*, 10 MHz per network), which will limit performance as the networks continue to add users and new services. In contrast, the “leveraged network” approach creates 10 MHz channels – by combining the D-Block with the contiguous public safety broadband spectrum at 700 MHz – to maximize the value of the two allocations and enable public safety to limit device and network costs.³⁵

Specifically, providing public safety with two paired 10 MHz channels in the Upper 700 MHz spectrum has the following benefits:

³³ BBTF Report, at 6, 11-12.

³⁴ If not combined with other spectrum, the 10 MHz (*i.e.*, 2 x 5 MHz) of D-Block spectrum is sub-optimal for new commercial services, would not be cost effective, and thus should not be implemented in its current form.

³⁵ Moreover, the D-Block and the public safety broadband spectrum are the last available contiguous 20 MHz of spectrum under 2.5 GHz available for public safety.

- Using adjacent spectrum blocks will limit the number of separate frequency bands that must be supported, and this will limit the cost of devices.³⁶
- With two 5 MHz channels combined into a single 10 MHz channel, broadband and multi-media applications can be supported for a larger number of users.
- Complicated network sharing agreements can be avoided, and the need to build two separate networks (or rather two separate radio channels) can be eliminated.

In sum, only with paired 10 MHz channels will public safety be able to satisfy its long term spectrum needs.³⁷ AT&T refers the Commission to a more detailed discussion on this point in AT&T's Comments filed in PS Docket No. 06-229³⁸ and to the BBTF Report that NPTSC submitted to the PSST.³⁹

g. What actions must the Commission or other entities take to ensure interoperability among public safety broadband systems?

Comments: The Commission must take several steps to ensure interoperability among public safety broadband systems. As a threshold matter, the Commission should adopt the “leveraged network” model discussed in AT&T's response to Question 1.e. The Commission should also establish technological standards and minimum system requirements for these public safety systems.⁴⁰ Specifically, the Commission should ensure, whether through regulation or oversight, that all networks adopt the LTE radio technology platform and infrastructure. The

³⁶ LTE, as standardized by 3GPP, can be designed to operate over 1.4 MHz to 20 MHz channels. The base station hardware to support a 5 MHz channel (*i.e.*, one half of a 10 MHz spectrum assignment) will be similar to that for a 10 MHz channel (*i.e.*, one half of a 20 MHz spectrum assignment). Thus, the infrastructure costs associated with deploying a 20 MHz system are comparable to a 10 MHz system but would provide increased functionality and capacity.

³⁷ Not all spectrum is fungible and blocks of non-contiguous spectrum are not attractive for public safety for technical as well as financial reasons (*e.g.*, increased device costs to support another frequency band, limited radio channel bandwidth).

³⁸ *See* Comments of AT&T, at 12-20.

³⁹ *See* BBTF Report, *supra* n. 23.

⁴⁰ These standards also would minimize duplicative build-out efforts and ensure that regions that build-out early are not forced to spend significant resources to become compatible with later-developed networks.

Commission also should mandate that local and regional public safety networks interconnect their backbone networks with adjacent public safety broadband networks as the networks deploy. Ultimately, nationwide interoperability would be achieved by linking the local and regional networks and establishing reciprocal roaming agreements and credentialing procedures between all public safety entities operating over 700 MHz networks.⁴¹ Finally, the Commission should grant the petitions for waiver of the Commission rules filed by public safety entities seeking authority to deploy public safety broadband systems on a local or regional basis in the 10 MHz of 700 MHz public safety broadband spectrum currently licensed to the PSST (*i.e.*, 763-768/793-798 MHz), and, in some cases, the 700 MHz D-Block (*i.e.*, 758-763/788-793 MHz).⁴² Permitting municipalities to use their own financial resources to build public safety networks will increase the amount of funding available to other regions and localities.⁴³ Additionally, the construction of these networks pursuant to the waiver grants will build momentum towards a standardized nationwide network composed of smaller interoperable networks. Together, these

⁴¹ Nationwide interoperability would be achieved by linking regional networks. *See, e.g.*, City of New York Petition for Waiver, PS Docket No. 06-229, at 12 (filed June 8, 2009) (“Regional interoperability would be achieved by adapting the dominant emerging 4G wireless technology (which, as noted, we believe will be LTE), operating within the same spectrum band and interconnecting our backbone network with adjacent public safety broadband networks as they are deployed. In a similar fashion, nationwide interoperability could be achieved by linking regional networks, and establishing reciprocal roaming agreements with other public safety 700 MHz broadband networks, enabling users with the proper credentials to access any deployed 700 MHz Public Safety broadband network in the nation.”).

⁴² *See* City of Boston Amended Request for Waiver, PS Docket No. 06-229 (filed May 28, 2009), as amended by City of Boston Erratum (filed June 19, 2009); City and County of San Francisco, City of Oakland, City of San Jose Amended Request for Waiver, PS Docket No. 06-229 (filed May 27, 2009) ; State of New Jersey Petition, PS Docket No. 06-229 (filed Apr. 3, 2009); NYC Request; District of Columbia Request for Waiver, PS Docket No. 06-229 (filed June 26, 2009); New York State Request for Waiver, PS Docket No. 06-229 (filed July 1, 2009); City of Chesapeake, Virginia Request for Waiver, PS Docket No. 06-229 (filed July 9, 2009); City of San Antonio, Texas Petition for Expedited Waiver, PS Docket No. 06-229 (filed July 10, 2009); State of New Mexico Petition for Expedited Waiver, PS Docket No. 06-229 (filed July 10, 2009); North Dakota Waiver-Expedited Action Requested, PS Docket No. 06-229 (filed August 18, 2009); Petition for Waiver of the City of Charlotte, North Carolina, PS Docket No. 06-229 (filed Aug. 4, 2009); Iowa Petition for Expedited Waiver, PS Docket No. 06-229 (filed Oct. 15, 2009); New EA, Inc. d/b/a Flow Mobile Request for Waiver, PS Docket No. 06-229 (filed July 7, 2009).

⁴³ The FCC, Congress, and public safety should establish additional funding models for municipalities that do not have the resources to build their own networks.

steps provide the best chance for achieving national interoperability that supports bandwidth intensive, 4G applications, including optical recognition systems, streaming video, VoIP applications, and collaboration tools.

- h. We also seek comment on whether public safety users anticipate using a single network for mobile broadband data and voice services in the short or long term, on the obstacles to such convergence, and on how the Commission could help to address these problems or otherwise support efforts at convergence.**

Comments: The primary obstacles to building an interoperable public safety network that provides a single source for public safety’s wireless voice and data needs are: (1) insufficient spectrum; (2) the lack of a standard that provides full public safety interoperability; (3) constructing a nationwide network that satisfies differing local and regional needs; and (4) the lack of funding. The Commission, however, can overcome these hurdles by following the steps outlined in the “leveraged network” model discussed above.

Insufficient Spectrum. AT&T’s response to Question 1.f. addresses concerns about the lack of sufficient public safety spectrum. Specifically, to provide public safety with a system that satisfies short- and long-term bandwidth requirements, 20 MHz of 700 MHz spectrum should be fully allocated to public safety.

Lack of Interoperability. AT&T’s response to Question 1.g. explains that nationwide interoperability could be achieved through a “network of networks” approach that consists of: adopting LTE as a nationwide 700 MHz public safety broadband standard; mandating that local and regional public safety networks interconnect their backbone networks with adjacent public safety broadband networks; and establishing reciprocal roaming agreements and credentialing procedures between all public safety entities operating over 700 MHz networks.

Nationwide Network Forecloses Local Input. AT&T’s response to Question 1.e. explains that regional or local public safety entities would tailor the RFPs to account for their unique

needs and the characteristics of specific regions. This approach will ensure that development, deployment, and training are conducted in cooperation with and in response to the specific needs of local public safety groups (while also ensuring nationwide interoperability).

Insufficient Funding. As a threshold matter, the “leveraged network” model uses the economies of scope and scale of commercial broadband infrastructure and technology to significantly reduce the cost for public safety broadband networks. As explained in response to Question 1.c., the total capital and operational expenditures over a ten-year period are estimated at \$35 billion for the “leveraged network” versus \$61 billion for a stand-alone network. In conjunction with the “leveraged network” model, AT&T recommends in response to Question 1.e. that Congress permit public safety agencies to use new and existing grant programs to fund the purchase or lease of fully-dedicated network equipment and managed broadband services. Further, granting the pending waivers to permit municipalities to use their own financial resources to build public safety networks in their area will increase the amount of funding available to other regions and localities

Deploying, maintaining, and operating a nationwide wireless broadband public safety network will be tremendously difficult. AT&T firmly believes, however, that a “leveraged network” approach adeptly navigates the concerns above and provides a roadmap for bringing broadband to public safety as quickly and cost-effectively as possible.

2. Next Generation 911 (NG911)

a. What are the broadband infrastructure requirements necessary to support deployment of NG911 capability?

Comments: NG911 will enable users to transmit, and public safety to receive and respond to, information sent via a variety of technological means. For example, although individuals will still be able to dial “911” on traditional wireline and wireless phones, NG911

capabilities will enable PSAPs to receive text messages, digital photos, streaming video, or other forms of data sent from future wireless, VoIP, or broadband enabled devices. The broadband infrastructure requirements necessary to support deployment of NG911 capability vary at different points in the emergency assistance process. From the perspective of PSAPs, deployment of NG911 capabilities requires the implementation of an Internet Protocol (“IP”) based managed emergency services network infrastructure, such as the “i3” network architecture for NG911 being developed by the NENA.⁴⁴ Substantial bandwidth and network hardening will be required to support these critical facilities.⁴⁵ From the perspective of a user who wishes to take advantage of these new functionalities, broadband infrastructure must be accessible in the user’s location and the network must have sufficient capacity to promptly transmit the user’s location information.

- b. Have NG911 technical standards been completely defined? If not, what has been done and what remains outstanding? Where is the associated equipment in the development pipeline?**

Comments: NG911 represents a new system for providing emergency services. This system will be comprised of hardware, software, policies and practices that will enable the utilization of new kinds of inputs from wireline and wireless users, the distribution of new kinds of data to responders, and new levels of coordination between agencies and across jurisdictions. The centerpiece of NENA’s i3 architecture is the Emergency Services IP network (“ESInet”), an IP-based network of networks shared by the various emergency response agencies. The final i3 standards are currently anticipated to be completed in early 2010.

⁴⁴ See “NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3),” National Emergency Number Association, 08-002 (2007) (“NG 911 Standards”), available at <http://www.nena.org/sites/default/files/08-002%20V1%2020071218.pdf> (last visited Nov. 10, 2009).

⁴⁵ Industry experts differ on approaches to bandwidth sizing and network hardening techniques. They do generally agree, however, that these two issues are highly fact-specific and extremely important in designing a robust IP network for NG911 use.

NENA has already coordinated the documentation of ESInet technical requirements⁴⁶ and architecture design characteristics⁴⁷ – often referred to as the Stage 1 and 2 levels of development of a technical standard. The Stage 3 work of providing detailed technical specifications is currently underway in NENA, with complementary standards development efforts ongoing at organizations such as the Internet Engineering Task Force (“IETF”) and 3GPP/3GPP2.⁴⁸ NENA is aggressively pursuing finalization of the NG911 standards that will enable manufacturers and developers to produce devices and applications to meet the needs of this next generation system. Several standards documents are targeted for release in 2009, while others may not be finalized until the first or second quarter of 2010. Although some developers have already begun work on devices and services meant to support NG911, these products are not likely to be readily available until some time after final publication of the i3 standards.

NENA also has a working group developing requirements and use cases for next generation messaging to NG-911 systems. This work is ongoing and will specify the requirements for messaging from any device to NG-911 systems.

- c. **To what extent are NG911 and near-NG911 technologies and services being deployed today? What states/regions/municipalities have already deployed these technologies and services or are on a path to doing so in the near-term? What factors have encouraged these deployments?**

Comments: Although no state or community has yet deployed a system meeting the NENA i3 specifications, some communities have already or soon plan to put into place different

⁴⁶ See, e.g., “NENA i3 Technical Requirements Document,” National Emergency Number Association, 08-751 (2006), available at http://www.nena.org/sites/default/files/08-751_20060928.pdf (last visited Nov. 10, 2009).

⁴⁷ See NG911 Standards.

⁴⁸ 3GPP (3rd Generation Partnership Project) and 3GPP2 (3rd Generation Partnership Project 2) are collaborative organizations made of up telecommunications standards development organizations working on developing mobile phone systems specifications based on the GSM and CDMA standards, respectively.

varieties of IP-enabled PSAPs. The state of Vermont has a statewide, IP-based 911 system wherein all 911 calls are received at one of two data centers where they are converted into Voice over IP (“VoIP”) format and directed to the appropriate PSAP.⁴⁹ Other states have planned pilot tests or submitted RFPs for NG911 systems based upon NENA specifications.⁵⁰ For example, Lake County, Florida released a RFP this year seeking proposals and bids on an IP-based 911 system. The RFP required vendors to commit to compliance with i3 and include the ability to handle text and video when the protocols are standardized.⁵¹ Many other jurisdictions are expected to take similar steps shortly. The U.S. Department of Transportation (“DOT”) previously conducted NG911 pilot programs across the country as the Proof of Concept portion of its NG911 initiative.⁵² Requirements tested in the DOT program included the ability of PSAPs to receive voice, video, text and data, location identification for wireless and VoIP callers, transmission of telematics data directly to the PSAP, and IP networking.⁵³ The DOT reported that, during PSAP-based testing, 241 of the 273 functional requirements passed testing.⁵⁴ Although the DOT acknowledged that technological improvements will be required at

⁴⁹ See generally, “Report to the Governor and VT General Assembly,” Enhanced 911 Board (Jan. 15, 2009), available at http://e911.vermont.gov/sites/e911/files/pdf/E911-2009_Rpt_to_Gov.pdf (last visited Nov. 10, 2009).

⁵⁰ See, e.g., Stephanie Taylor, “Alabama Could Pioneer New 911 Technology,” Tuscaloosa News (Sept. 20, 2009), available at <http://www.tuscaloosaneews.com/article/20090920/NEWS/909199935> (last visited Nov. 10, 2009).

⁵¹ See “Request For Proposal (RFP): Lake County NG911 Upgrade,” Lake County, Florida, RFP Number 09-0608 (Feb. 23, 2009), available at http://www.lakecountyfl.gov/pdfs/Procurement_Services/09-0608_RequestforProposals.pdf.

⁵² See “Next Generation 9-1-1 (NG9-1-1) System Initiative: Proof of Concept Testing Report,” Intelligent Transportation Systems, U.S. Department of Transportation (2008), available at http://www.its.dot.gov/ng911/pdf/NG911_POCTesTReport091708.pdf (last visited Nov. 10, 2009). Department of Transportation pilot programs were conducted in Rochester, NY, Seattle, WA, St. Paul, MN, Helena, MT, and the State of Indiana. *Id.* at 3.

⁵³ *Id.* at 2-3.

⁵⁴ *Id.* at 6.

multiple levels to support NG911, the DOT team was pleased that the testing successfully validated a significant portion of the NG911 concepts and use cases tested.⁵⁵

The main impediment to accelerated deployment of NG911 systems is lack of funding. Although the cost of replacing legacy 911 systems will vary substantially depending upon the size of the jurisdiction, the age and quality of the existing network infrastructure, and the technologies chosen for the new system, upgrading to NG911 is certain to require a significant appropriation of money above the typical budget of a jurisdiction's 911 board.⁵⁶ It is expected that adoption rates will increase after finalization of the NENA standards, as jurisdictions assess the experiences of early adopters and gain confidence that the systems they deploy will be compliant and interoperable.

- d. **Are there regulatory roadblocks that may be restricting more vigorous NG911 deployment? Which of these are within the Commission's jurisdiction and what actions should the Commission take in this regard?**

Comments: Several regulatory impediments must be overcome to facilitate deployment of the new technologies and the levels of network and data sharing that are essential to NG911 service. Many existing 911 laws are written based on the assumption that the notification to the PSAP will be delivered through a voice call to "911." However, in a NG911 system, some requests for assistance may be sent by an individual without actually *calling* 911 (*i.e.*, in the case of a text message), while others may be originated without any human actor at all (*i.e.*, in the case of a vehicle telematics system that automatically contacts a PSAP after an automobile accident).

⁵⁵ *Id.* at 6-7.

⁵⁶ Alabama is reportedly seeking over \$14 million in funds for its NG911 upgrade. *See Taylor, supra* n. 50.

Indeed, the Commission's own rules will require some modification to adjust to this paradigm. For example, Section 20.18 of the Commission's rules requires wireless carriers to provide location information to PSAPs with all "911 calls."⁵⁷ Thus, the Commission must examine its relevant rules to ensure that they accurately reflect a world in which NG911 services may be requested in ways other than through dialing a phone number.

However, Commission action alone will be insufficient to address all of the regulatory roadblocks to NG911 deployment. State and local laws, regulations and tariffs that are outside of the Commission's jurisdiction will require modification. For example, some existing laws or tariffs explicitly limit the sharing of information contained in emergency databases to those situations where a "caller" has "dialed 911." There are also a number of other areas in which states should modify their laws and regulations to facilitate deployment of NG911. For example, states should take action to:

- Review laws/regulations concerning the eligible use of NG911 funds;
- Ensure that laws/regulations do not require specific technology components for E911 service delivery that are not compatible with NG911 service;
- Eliminate laws/regulations that may inhibit appropriate and efficient sharing of NG911 data with appropriate safeguards for privacy protection;
- Craft uniform requirements for all NG911 service providers that meet accepted industry standards; and
- Ensure that laws/regulations are functional and performance-based without reference to any specific proprietary technology, manufacturer or service provider.

⁵⁷ 47 C.F.R. § 20.18.

These reforms will likely take some time and, considering that NG911 standards are soon to be finalized, the Commission should encourage states to begin addressing these issues immediately.⁵⁸

- e. **What technologies are available or under development in the NG911 environment to facilitate automatic location identification? How can this data be made useful to Public Safety Answering Points (PSAPs)?**

Comments: NENA has published an architecture for interconnecting VoIP telephone subscribers with E911 services, commonly referred to as “i2.”⁵⁹ This document details an automated process for determining the location of a wireline VoIP caller who dials 911. One key element of this design is the Location Information Server (“LIS”), a repository for location information that is maintained by the entity providing the physical network access facilities for subscribers, identified by NENA as the Access Infrastructure Provider (*i.e.*, the DSL or Cable Modem service provider). The LIS features prominently in the i3 documentation as well, and it plays a crucial part in allowing NG911 to associate the IP endpoint of a device with a physical location for an individual requesting emergency assistance. As the industry transitions from E911 to NG911, the LIS will essentially replace the current Automatic Location Information (“ALI”) databases and will function as the source of location information for all requests for assistance (“RFAs”).

Currently, in the VoIP context, location information is provided manually by the VoIP Service Provider (“VSP”) or the subscriber. Some VoIP offerings, such as AT&T’s U-verse

⁵⁸ AT&T anticipates that some entities might take this opportunity to push an agenda favoring government-mandated and price-regulated interconnection under the guise of “leveling the playing field.” However, as AT&T has explained elsewhere, this sort of unwarranted cost-shifting undermines incentives for investment and innovation in NG911 facilities and ultimately increases the risk of service disruptions and threatens public safety. *See* Comments of AT&T, WC Docket Nos. 08-185, 08-33, at 6-12 (filed July 6, 2009).

⁵⁹ *See* “Interim VoIP Architecture for Enhanced 9-1-1 Services (i2),” National Emergency Number Association, 08-001 (2005), available at http://www.nena.org/sites/default/files/08-001_20051205.pdf (last visited Nov. 10, 2009).

Voice, require the VSP to enter location information into the ALI database at the time of service provisioning, making the data highly accurate and requiring no effort on the part of the subscriber. Other VoIP offerings require users to input location information, often through a web browser, which can lead to less reliable location information.

Although there are several products available that are marketed as LIS systems, access infrastructure providers have not yet developed the capabilities required to support an *automated* LIS. For example, no existing product allows disassociated databases to automatically interoperate to gather the information needed to associate a given request for assistance with a specific location, such as would occur if the att.net DSL customer records database(s) could “talk to” outside plant cable databases to associate an IP address with a DSLAM port and cross-reference the IP address to the physical address for that cable pair. Until the provision of location information is fully automated, location information solutions will not meet the functional description of an LIS, as defined by NENA in i2 standards.

- f. **What does the public safety community, including PSAPs, need to do to enable emerging Internet applications that reliably deliver voice, video and data information to PSAPs? What is the best architecture and means to accomplish this?**

Comments: NENA’s i3 network architecture represents a standards-based design for an interoperable IP-based 911 network. The NENA architecture, or a truly equivalent and interoperable alternative, should form the cornerstone of NG911 systems being contemplated by PSAPs and 911 authorities. These entities should pay close attention to the finalization of the NENA documentation and should adopt usage of i3 architecture as a requirement in their RFPs, product acquisitions, and strategic planning.

3. Cybersecurity

- a. **What types of computer-based attacks against government or commercial computer systems or networks (*i.e.*, cyber attacks) are occurring or are anticipated to occur? What are federal agencies, commercial, and other entities doing to prevent, detect and respond to cyber attacks.**

Types of Computer-Based Attacks: Computer-based attacks pose serious economic and national security challenges. As the White House recently recognized in its Cyberspace Policy Review, a “growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information.”⁶⁰ Consumer Reports recently estimated that cyberattacks have cost \$8 billion over the past two years and affected over 1.2 million users.⁶¹ As detailed below, the most common cyberattacks on government and commercial computer networks include: attempts to extract information; attempts to compromise network systems; and attempts to disrupt operations.⁶²

Attempts to Extract Information. Attempts to extract information are generally referred to as “phishing.” Phishing typically occurs when an attacker attempts to acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication with the consumer. Phishing is typically carried out by an e-mail or instant message that directs users to access and enter sensitive

⁶⁰ “Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure,” National Security Council, at 1 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (last visited Nov. 10, 2009).

⁶¹ “Boom Time for Cybercrime: The economy and online social networks are the latest fodder for scams,” Consumer Reports (June 2009), *available at* <http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/overview/state-of-the-net-ov.htm> (last visited Nov. 10, 2009).

⁶² Consumer Reports estimates that “close to 2 million households have suffered identity theft in the past year as a result of Internet-related activity, most often online shopping.” *Id.* Additionally, phishing – sending authentic-looking but fraudulent e-mail to steal personal information – has affected approximately seven million consumers. *Id.*

information at a fake website that replicates a legitimate website.⁶³ Phishing sites often use banners, logos, and even the legal disclaimers from actual sites to make them look genuine. Phishers commonly lure victims with communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators. Attacks that target a specific person – frequently an affluent or vulnerable individual – are known as “spear phishing” attacks. Prior to such attacks, the attackers compile personal information to assist in the fraudulent conduct.⁶⁴ The “spear phishers” then launch a custom campaign against the individual to get them to disclose additional information.

The damages from phishing are extensive. Recent studies estimate losses between \$61 million annually⁶⁵ and a half-billion dollars during the past two years.⁶⁶ It is also estimated that seven million consumers gave phishers personal information over the past two years.⁶⁷ And out of these seven million consumers, one million consumers lost money.⁶⁸

⁶³ Recently, similar phishing attempts have occurred using SMS text messages on wireless devices.

⁶⁴ Instead of casting out thousands of e-mails randomly hoping a few victims will bite, “spear phishers” target select groups of people with something in common – they work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website. Armed with this inside information about their targets, the attacker sends fraudulent e-mail messages to those targets offering urgent and legitimate-sounding explanations as to why the target must enter their sensitive information. The e-mail messages are ostensibly sent by organizations or individuals from which the potential victims would expect to get e-mail messages, making the message even more deceptive. The targets are then asked to click on a link embedded in the e-mail message, which takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc. See “Spear Phishers,” FBI (Apr. 2009), available at http://www.fbi.gov/page2/april09/spearphishing_040109.html (last visited Nov. 10, 2009).

⁶⁵ See Cormac Herley and Dinei Florencio, Microsoft Research, “A Profitless Endeavor: Phishing as Tragedy of the Commons,” at § 4.4 (2008).

⁶⁶ “Phishing Costs Millions,” Consumer Reports (June 2009), available at <http://www.consumerreports.org/cro/magazine-archive/june-2009/electronics-computers/state-of-the-net/phishing-costs-millions/state-of-the-net-phishing-costs-millions.htm> (last visited Nov. 10, 2009).

⁶⁷ *Id.*

⁶⁸ *Id.* Moreover, Consumer Reports explains that last fall more than 250 brand names were used each month in e-mail scams and other cybercrime. The most targeted industry was financial services. *Id.*

Attempts to Compromise a System. Attempts to compromise computer systems typically occur with Trojan horse malware,⁶⁹ which enables an attacker to gain remote access and full control of computer systems and the information stored on those systems. To the unsuspecting user, a Trojan horse appears to perform a desirable function but, in fact, it facilitates unauthorized access to the user's computer system.⁷⁰ Frequently, attackers gain access by tricking users into downloading software, opening attachments that install software, or following hyperlinks to sites that install software.⁷¹ Attackers also compromise networks by promulgating software bugs to attack computer systems that lack appropriate patches. Trojan horse attacks are widespread. A survey conducted from January 2009 to June 2009 found that "Trojan-type malware is on the rise, accounting for 83-percent of the global malware detected in the wild."⁷²

Attempts to Disrupt Operations. Attempts to disrupt legitimate operations of a communications network are generally called Distributed Denial of Service ("DDoS") attacks. Attackers typically rent computer processing power, bandwidth, and storage online, which they then use to send a traffic overload to an online destination. This results in the destination becoming unavailable for its intended use. DDoS attacks can be very disruptive, frequently disabling entire websites, and even threatening national security. For example, a wave of cyberattacks in July 2009 targeted at least 27 American and South Korean government agencies

⁶⁹ Malware is malicious software that infiltrates a computer without the owner's informed consent.

⁷⁰ With the network compromised, Trojan-horse attackers perform Distributed Denial-of-Service ("DDoS") attacks; steal data (*e.g.*, passwords, security codes, credit card information); delete files; modify files; log keystrokes; view the user's screen; and use up computer storage space.

⁷¹ Attackers often include keystroke loggers and sniffers with control software, which enable the attacker to collect information not physically stored on disk.

⁷² "BitDefender Malware and Spam Survey finds E-Threats Adapting to Online Behavioral Trends," BitDefender (Aug. 2009), *available at* <http://news.bitdefender.com/NW1094-en--BitDefender-Malware-and-Spam-Survey-finds-E-Threats-Adapting-to-Online-Behavioral-Trends.html> (last visited Nov. 10, 2009).

and commercial websites, temporarily jamming more than a third of them.⁷³ Additionally, in August 2009, DDoS attacks disrupted operations on several social networking sites, temporarily crippling Twitter and Livejournal, and hindering service on Facebook and certain Google websites.⁷⁴

Botnets. Botnets are emerging as one of the primary, and most insidious, means to both extract information and disrupt operations. A botnet – short for Robot Network – is a software program that infects an operating system, and runs autonomously and automatically on compromised computers (called “Zombie computers”) to enable the originator (the “Bot Master”) to remotely control the end-user computer or more typically, a group of computers. Botnets can be used for a variety of criminal or other nefarious purposes, such as to gather sensitive personal information, participate in a DDoS attack, or engage in a mass distribution of spam. A botnet typically operates without the knowledge of the individual users and covertly communicates with the Bot Master for command and control or delivery of information. Botnets are usually installed via worms, Trojan horses, or backdoors.

What Federal Agencies, Commercial Entities, and Others Are Doing: Government and industry continue to enhance their efforts to prevent cyberattacks and mitigate the potential damages they cause. The White House repeatedly has demonstrated its commitment to cybersecurity through its Comprehensive National Cybersecurity Initiative (“CNCI”) and its recent CyberSecurity Review, which outlines next steps to streamline and synchronize intergovernmental and public/private security efforts. For their part, communications providers

⁷³ See “Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,” NY Times (July 8, 2009), available at <http://www.nytimes.com/2009/07/09/technology/09cyber.html> (last visited Nov. 10, 2009).

⁷⁴ See Jenna Wortham, “Professor Main Target of Assault on Twitter,” NY Times (Aug. 7, 2009), available at http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html?_r=2&hpw (last visited Nov. 10, 2009).

also continue to improve cybersecurity by boosting the security functionalities in their networks and empowering communications users with tools and education to avoid cyberattacks.

Federal Government Activities. Federal government efforts to enhance cybersecurity have been widespread. In 2008, the White House created the CNCI. The CNCI attempts to “bridge” historically separate cybersecurity missions with law enforcement, intelligence, counterintelligence, and military capabilities to address current and emerging cyber threats, shore up telecommunications and cyber vulnerabilities, and combat entities attempting to steal or manipulate data on federal systems.⁷⁵ A multitude of programs support this government-wide initiative. Two of these programs are the Office of Management and Budget’s (“OMB”) Trusted Internet Connection (“TIC”) program and the General Services Administration’s (“GSA”) Managed Trusted Internet Protocol Services (“MTIPS”) effort.⁷⁶ These programs focus on optimizing individual external connections – including Internet points of presence – currently in use by the federal government and greatly reduce the number of federal external connections. These programs will improve the federal government’s incident response capability by reducing

⁷⁵ The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 – issued on January 2, 2008 – established the CNCI. The CNCI formalizes a series of continuous efforts to further safeguard the federal government systems from cyber threats and attacks. At the national level, the CNCI focuses on three key areas: establish a frontline defense to reduce current vulnerabilities and prevent intrusions; defend against the full spectrum of threats by using intelligence and strengthening supply chain security; and shape the future environment by enhancing our research, development and education as well as investing in leap-ahead technologies. See “Protecting Our Federal Networks Against Cyber Attacks,” U.S. Department of Homeland Security (June 4, 2009), available at http://www.dhs.gov/files/programs/gc_1234200709381.shtm (last visited Nov. 10, 2009).

⁷⁶ In November 2007, OMB announced the implementation of TIC in “Implementation of Trusted Internet Connections (TIC),” Memorandum M-08-05, available at <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf> (last visited Nov. 10, 2009). GSA developed MTIPS to allow agencies to physically and logically connect to the Internet in full compliance with OMB’s TIC. MTIPS is designed to significantly enhance the security of federal agency IP traffic, by facilitating the reduction of internet connections in government networks and providing standard security services to all government users. Functionalities inherent in MTIPS include: a Security Operations Center for agency protection; transport from the agency-wide area network to the TIC Portal; redundant internet access service Supply Chain Risk Management Requirements; and optional features to allow for agency unique requirements. Notably, GSA awarded its first highly anticipated MTIPS contract to AT&T. See “GSA Awards First Trusted Internet Connection (TIC) Contract to AT&T,” GSA (Dec. 15, 2008), available at http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentType=GSA_BASIC&contentId=25486 (last visited Nov. 10, 2009).

external connections and centralizing gateway monitoring to a select group of federal government TIC Access Providers.⁷⁷

Consistent with recent recommendations made in the President's Cybersecurity Review, the federal government also is crafting "a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to . . . significant cyber incident[s]."⁷⁸ The Department of Homeland Security ("DHS") leads this initiative, and is managing a working group of representatives from the private and governmental (federal, state, and local) sectors to develop a National Cyber Incident Response Plan ("NCIRP").⁷⁹ This plan will clearly delineate roles and responsibilities in case of a major cyber incident. Importantly, DHS launched this process with the private sector integrated from the very start to establish an actionable public/private response to cyberattacks.⁸⁰

Commercial Provider Efforts. Cybersecurity relies heavily on effective network-based security measures.⁸¹ These solutions mitigate attacks and malicious activity in the core network

⁷⁷ Via the GSA Networx contract, AT&T is introducing MTIPS to its government customer base, which represents a significant step forward in managed, network-based cyber security services.

⁷⁸ "Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure," National Security Council, at 23 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("Cyberspace Review") (last visited Nov. 10, 2009).

⁷⁹ Testimony of Philip Reiting, Deputy Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security, Before the United States Senate Committee on Homeland Security and Governmental Affairs (Sept. 14, 2009).

⁸⁰ *Id.*

⁸¹ Individual system administrators and users do not typically have the knowledge and experience to make their systems secure and keep them that way. Even a well-configured platform, protected by the best commercial off-the-shelf technology, and managed by a security-savvy administrator is vulnerable to covert access by a sophisticated attacker, unless detected and mitigated in the network. Further, Botnet-driven DDoS attacks must be detected and mitigated (scrubbed) in the network itself.

before problems arrive on a customer's doorstep.⁸² Indeed, network exploits, malware, botnets, flooding attacks, protocol anomalies, and other threats are generally visible on the Internet. Commercial communications operators, as part of their normal monitoring of data traffic, are often able to identify and mitigate them long before they impact security.⁸³

AT&T leads the industry in developing and implementing network-based security solutions.⁸⁴ AT&T's advanced network technology currently transports more than 17 petabytes a day of IP data traffic, and that load is expected to double every 18 months for the foreseeable future. AT&T's network technologies give the company the capability to analyze traffic flows to detect malicious cyber-activities and, in many cases, to get very early indicators of attacks before they have the opportunity to become major events.⁸⁵ These measures to detect, prevent, and mitigate cyberattacks benefits all AT&T customers, whether consumer, business, or government.

For those AT&T customers that demand more focused cybersecurity protections, AT&T offers a suite of Security and Business Continuity Services that assess vulnerabilities, secure data

⁸² Experience shows that sophisticated cyberattacks that penetrate networks to user servers and desktops invariably succeed.

⁸³ Specific advantages of network-based solutions include: security elements are deployed network-wide; broad-based network attacks are defended in the network; the network runs a centralized security policy; the network receives improved alerting and reporting; and the security elements are easy to scale, cost-effective, and holistic.

⁸⁴ AT&T is uniquely able to understand threats on the Internet because of: its position as the largest provider of Internet services; its global IP network footprint; its Internet data analysis platform that examines Internet threats, including botnets, network worms, DDoS attacks, network exploits, and other anomalous activity; its analysis team that operates 24/7 to assess significant Internet activities that could affect network services; its algorithm research team that continually investigates and test methods for automated detection of network threats; and its Labs and Chief Security Office researchers, who participate in the security and networking research communities.

⁸⁵ For example, AT&T possesses the capability to automatically detect and mitigate most DDoS attacks within the AT&T network infrastructure before they affect service to AT&T customers. Indeed, AT&T has grown from having one domestic scrubbing complex to having multiple locations across the United States, as well as nodes in Europe and Asia. This gives the company the ability to filter out attack traffic as close to the source of the threat as possible.

and infrastructure, detect attacks, respond to suspicious activities, and provide for non-stop operations, including the following:

- **AT&T Encryption Services** provide a comprehensive suite of encryption solutions to help protect data in motion by automating the management and use of digital credentials.
- **AT&T Firewall Security Services** protects the network perimeter from the external hazards posed by doing business on the Internet (includes network-based, premises-based and end-user options).
- **AT&T Internet Protect®** is a security analysis and notification service that offers advanced information regarding potential real-time attacks.
- **AT&T DDoS Defense** is an option of Internet Protect and provides DDoS identification and mitigation within AT&T's backbone.
- **AT&T Managed Intrusion Detection Service** protects a customer's networking infrastructure by detecting/responding to unauthorized attempts to access the network.
- **AT&T Intrusion Prevention Service** provides tools to implement internal network defense by detecting endpoints on the network that are propagating threats or violating the security policy and revoking their access to the network.
- **AT&T Token Authentication Service** provides secure access to networks and applications by requiring users to enter a user ID, PIN and token code.
- **AT&T Secure E-mail Gateway Service** provides network-based e-mail security, message management and encryption.
- **My Internet Protect** is a security knowledge mining, analysis, and notification service for identified threats that enter a customer's network.
- **Private Intranet Protect** is an analysis and notification tool designed to analyze traffic on the user's Virtual Private Network and help detect intrusions, cyber attacks and other potentially threatening identified anomalies.
- **Web Security** provides network-based capabilities to perform Web content filtering and screening for malware and spyware, and IM filtering for malware.
- **AT&T Remote VaultSM** is an automated service that backs up the data on servers, laptops and desktops using a broadband Internet connection.
- **AT&T Business Continuity Professional Services** focuses on all aspects of business continuity requirements – availability, reliability, scalability, recoverability, performance and security.

- **Enterprise Recovery Services** offer a choice for recovery utilizing center-based, mobile-based or subscriber location-based recovery options for information systems and employees, telecommunications capabilities and IT resources.
- **AT&T StorageConnectSM** is a fully-managed, multi-location storage transport service that supports virtually any bandwidth and storage protocol.

Individual customer empowerment and education also is critical for preventing and mitigating the damages of cyberattacks. To this end, AT&T and other communications providers offer services and education programs that empower consumers. For example, AT&T's free High Speed Internet Parental Controls and MEdia™ Net Parental Control services help parents control the online content their children access via AT&T wireline and wireless services.⁸⁶ And the AT&T Smart Limits™ website brings together this information on parental-control features for the full suite of AT&T services – wireless, wireline, high speed Internet access and video – into one online portal.⁸⁷ Additionally, AT&T provides its high speed Internet customers with the AT&T-Yahoo! Online Protection Suite and the Internet Security Suite.⁸⁸ These suites include anti-virus software, firewall software, and Spamguard Plus software, which provide customers with the power to defend against cyberattacks and unwanted communications. This software is continually updated to help safeguard users against emerging threats.

AT&T and other commercial providers work with a variety of external organizations to promote online safety education and awareness to both adults and children. For example, AT&T developed the AT&T Hometown Tours program, which visited more than 100 communities nationwide and worked with more than 20,000 students on Internet safety lessons, programs and

⁸⁶ “AT&T Smart Limits,” *available at* <http://www.att.com/gen/sites/smartlimits?pid=8950> (last visited Nov. 10, 2009).

⁸⁷ *Id.* The website provides information and directions on how to use parental controls for wireless, Internet, video and home phone services from AT&T.

⁸⁸ “Connecting Your World,” AT&T, *available at* http://www.att.com/Common/about_us/files/pdf/Safety/Protecting_Your_World.pdf (last visited Nov. 10, 2009).

workshops geared toward elementary- and middle-school-aged children. This program focused on key Internet safety skills, such as protecting computers against viruses, hackers and spam, as well as reviewing age-appropriate content and the potential dangers associated with social networking. AT&T also implemented an online safety program with its partner iKeepSafe, where Drug Abuse Resistance Education (“DARE”) officers in thousands of communities across the country teach children in grades K-5 how to keep safe online. Older children also receive special lessons on how to ward off cyber bullies. Yet another AT&T partner, Enough is Enough, has developed educational kits for parents, as well as a program that will help reach at-risk youth with important safety education. AT&T also recently endorsed National Cyber Security Awareness Month and is a member of the National Cyber Security Alliance (“NCSA”), a public/private partnership focused on increasing awareness of cyber security issues for consumers and small and medium business.

Working with partner organizations OASIS and SeniorNet, AT&T has helped the senior community learn to operate their wireless devices safely and efficiently through one-on-one coaching sessions. AT&T also launched a cyber safety educational program for mature adults, Safe Surfing, with the National Caucus and Center on Black Aged and provides the presentation at various fairs and seniors events throughout the country. In 2009, AT&T reached out to more than 4,000 senior consumers through its programs. As the Baby Boom generation ages, resulting in a greater percentage of elderly Americans, this education is becoming more essential.

Activities of Other Entities. To prevent and minimize cyberattacks, broad user education about potential cyberattacks is critical.⁸⁹ Federal agencies, businesses, and other entities must

⁸⁹ The President’s Cyberspace Policy Review recognized the importance of public awareness. The Report concluded that “[b]road public awareness of the risks of online activities and how to manage them will require an effective communications strategy. The Federal government, in partnership with educators and industry, should conduct a national cybersecurity public awareness and education. The President’s cybersecurity policy official

inform their employees about the best ways to defend against attempts to extract information, compromise systems, and disrupt operations. Fortunately, many organizations now recognize the value of employee education on security and have issued security policy documents.⁹⁰ These documents inform workers how to prevent cyberattacks and how to mitigate the damage of cyberattacks. Examples of guidance found in security policies include:

- Assets must be inventoried, asset owners must be identified, and assets must be scanned for vulnerabilities on a periodic basis;
- Systems must be updated in a timely manner when updates or patches become available;
- Controls must be in place to ensure that only authorized users have access to systems and information (unique logins, complex passwords, tokens, etc.); and
- Sensitive information should be encrypted at rest and in transit.

b. How are other federal agencies of the United States and other governments collaborating with the communications segment to prevent, detect, and respond to cyber attacks?

Comments: See AT&T's response to question 3.a regarding the NCIRP. AT&T actively engages in a wide variety of global security initiatives, including numerous government-sponsored cybersecurity activities and fora. These include:

- Computer Emergency Response Team/Coordination Center (CERT/CC) – a global initiative

should lead the development and direct the implementation of this public awareness strategy and should seek endorsement by Congress; State, local, and tribal governments; the private sector; and the civil liberties and privacy communities." *Cyberspace Review* at 13.

⁹⁰ See, e.g., 44 U.S.C. § 3522 (providing that the head of each agency shall be responsible for providing information security protections against the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of agency information or information systems); "Agency Network Security Policy," U.S. Environmental Protection Agency (Nov. 27, 2007), available at <http://www.epa.gov/irmpoli8/ciopolicy/2150-0.pdf> (last visited Nov. 10, 2009); Colo. Rev. Stat § 24-37.5-404 (2006) (requiring all state agencies in Colorado to develop an information security plan); "Information Security Policy," University of Illinois (June 14, 2004), available at http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html (last visited Nov. 10, 2009); Joel Weise & Charles R. Martin, Sun Microsystems, "Developing a Security Policy" (Dec. 2001), available at <http://www.sun.com/blueprints/1201/secpolicy.pdf> (last visited Nov. 10, 2009).

- Security activities within the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) – a global initiative
- Forum of Incident Response and Security Teams (FIRST) – a global initiative
- National Coordinating Center for Telecommunications (NCC)
- Network Reliability and Interoperability Council (NRIC)
- Communications - Information Sharing and Analysis Center (Communications-ISAC)
- Network Reliability Steering Committee (NRSC)
- National Telecommunications and Information Administration (NTIA)
- National Communications System (NCS)
- National Security Telecommunications Advisory Committee (NSTAC)
- Federal Bureau of Investigation’s InfraGard
- U.S. Secret Service (USSS) Cyber Crimes Task Force
- National Security Information Exchange (NSIE)
- Shared High Frequency Radio Resources (SHARES) Program
- Communications Sector Coordinating Council (SCC)
- Telecommunications Service Priority (TSP) Oversight Committee.

The sheer number of federal public/private programs reflects the government’s interest in addressing the security and economic concerns connected to cyberattacks. Currently, however, there is no single entity that coordinates this wide-ranging collection of inter-governmental efforts and public/private efforts. As the Congressional Research Service explained: “[E]ach entity involved pursues cybersecurity from a limited vantage point dictated by [its own] jurisdiction. Many different initiatives exist, but because of fragmentation of missions and responsibilities, ‘stovepiping,’ and a lack of mutual awareness between stakeholders, it is

difficult to ascertain where there may be programmatic overlap or gaps in cybersecurity policy.”⁹¹

The President’s Cybersecurity Review also recognized that “[r]esponsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.”⁹² Additionally, the Cybersecurity Review concluded that although “[p]ublic-private partnerships have fostered information sharing and served as a foundation for U.S. critical infrastructure protection and cybersecurity policy for over a decade[,]” the lack of effort by some parties has left “participants frustrated with unclear delineation of roles and responsibilities, uneven capabilities across various groups, and a proliferation of plans and recommendations.”⁹³ As a result, “government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts.”⁹⁴

AT&T agrees that the many decentralized cybersecurity-related policy and technology efforts currently in place across the government and the industry should be harmonized and streamlined to improve cybersecurity efforts. Interested parties should also work to simplify crisis management by establishing a cohesive and voluntary cybersecurity policy that government and commercial entities follow for cyber incident response. Federal network

⁹¹ *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*, Congressional Research Service (Sept. 30, 2009), available at <http://www.fas.org/sgp/crs/natsec/R40836.pdf> (last visited Nov. 10, 2009).

⁹² *Cyberspace Review* at i.

⁹³ *Id.* at 18.

⁹⁴ *Id.*

security experts should contribute to the process and, to the extent they are able, share information about the federal government's network experience. Additionally, parties involved in public/private partnerships should reengage with each other and explicitly define the nature of their relationships, the roles and responsibilities of various groups and their participants, the expectations of each party's contributions, and accountability mechanisms. And while AT&T supports public-private partnerships and information sharing to improve cybersecurity efforts, such programs must be designed in a manner that protects the privacy and civil liberties of consumers.

c. What market incentives exist for commercial communications providers, large and small, to invest in secure infrastructure? (i.e., how do we avoid externalities?)

Comments: Commercial success and effective cybersecurity go hand-in-hand. Commercial service providers are targets for every type of cyber attack, and a provider's network will not operate smoothly if an attack compromises the provider's ability to offer service. Among other things, successful cyberattacks may cause service outages, which could cause customers to switch service providers.⁹⁵ Cyberattacks may additionally result in disclosure of customer information, which also can cause concerned customers to switch providers. In addition to foregone revenue from lost customers, providers incur significant

⁹⁵ Bruce S. Schaeffer, Henfree Chan, Henry Chan and Susan Ogulnick, "Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others," Wolters Kluwer Law & Business, *available at* http://business.cch.com/franlaw/cybercrime_whitepaper.pdf (last visited Nov. 10, 2009) ("Cyber Crime White Paper"). *See also* "Data and Contacts Vanish From Sidekick Phones," Los Angeles Times (Oct. 12, 2009), *available at* <http://www.latimes.com/business/la-fi-sidekick13-2009oct13,0,3031857.story> (last visited Nov. 10, 2009) (describing a recent service disruption to T-Mobile's Sidekick phone that caused some subscribers to cancel contracts); Ina Fried, "Lawsuits Filed Over Sidekick Outage," CNET News (Oct. 14, 2009), *available at* http://news.cnet.com/8301-13860_3-10375240-56.html (last visited Nov. 10, 2009) (describing lawsuits filed against T-Mobile and Microsoft relating to data loss caused by a service outage to the Sidekick phone).

monetary costs to notify customers of an illicit disclosure.⁹⁶ Further, cyberattacks may lead to costly litigation, regulatory investigations, contract disputes, and reputation damage.⁹⁷ As a result, commercial communications providers have numerous and significant market incentives to invest in measures to secure their network infrastructure. Indeed, providers view cybersecurity as a top priority and spend significant financial and personnel resources to combat cyberattacks.

Because of the direct correlation between network security and commercial success, communications providers typically develop network-based cybersecurity solutions before security breaches ever occur. This effort requires upfront planning and integration of security measures into business models before a provider even begins network construction. This is particularly important now during the transition to costly and complex 3G and 4G IP-based networking models. This year alone AT&T is investing between \$18-\$19 billion to expand its network capabilities and enhance security and reliability. Network security needs, however, do not end mid-construction or once service begins. AT&T spends – and must continue to spend – significant financial and human capital throughout the entire life of its network to monitor and combat the latest cyberattacks. A rapid response to constantly evolving cyber threats is critical to network integrity and to the communications needs of customers.

Market forces – and the flexibility provided by regulators to date – have driven the communications industry’s successful cybersecurity efforts. Given this current success story, AT&T opposes any government cybersecurity mandates imposed on providers or requirements

⁹⁶ The cost to enterprise clients of notifying customers that their information has been compromised is estimated to be \$1-3 per file accessed and \$100-300 or more per file compromised. *See Cyber Crime White Paper* at 4.

⁹⁷ *Id.* at 3.

that otherwise limit the flexibility providers need to protect their networks and customers. Commercial networks all contain unique characteristics, and network owners are best positioned to determine how to secure their networks. Regulators also should avoid imposing obligations that require providers to retrofit their networks to satisfy generalized, industry-wide security specifications. Commercial providers have developed distinct security features and practices that match the unique characteristics of their networks. It would be costly – and potentially dangerous – to force communications providers to scrap their network-specific optimized security measures in favor of generic measures adopted by regulators.⁹⁸

Regulators additionally should not impose any requirements, particularly “net neutrality” obligations, that could hamper the ability of commercial network providers to respond to cyberattacks or that discourage providers from deploying intelligent network technology that would better enable them to respond to such attacks.⁹⁹ Even with limited exceptions to permit cybersecurity efforts, restrictive rules could discourage providers from aggressively combating cyberattacks due to ambiguities in the rules, such as uncertainty over the meaning of “reasonable network management.” Indeed, any interpretation of “reasonable” in the cybersecurity context must not confine providers to a “narrowly tailored” or similarly limited countermeasures, which would only serve to aid those responsible for the cyberattacks. Instead, providers must in all

⁹⁸ Forcing communications providers to make costly aftermarket changes to their networks would remove the incentive for network investment, by making communications providers fearful of additional retroactive regulation years down the line.

⁹⁹ See *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 14853, ¶ 19 (2005) (finding that nondiscrimination obligations “constrain technological advances and deter broadband infrastructure investment by creating disincentives to the deployment of facilities capable of providing innovative broadband Internet access services”).

cases be afforded *wide latitude* to use their best judgment in protecting their networks and customers from cybersecurity threats.¹⁰⁰

- d. **Do end-users have sufficient independent information to make good decisions between communications providers that may differ in the extent to which they implement cyber security measures?**

Comments: End-users have ample information to determine which communications providers offer effective cybersecurity measures. Although AT&T is not aware of any ratings system that consumers may use to directly compare the cybersecurity efforts of communications providers, there are a number of publicly available sources that will direct consumers to communications providers with solid cybersecurity measures. For example, independent publications that report on service quality provide consumers with insight into the network security efforts of different service providers. Poor practices in cyber security will likely result in poor service quality and reliability and thus lower customer satisfaction. Moreover, communications providers frequently provide potential and existing customers with company-specific cyber-security information.¹⁰¹ AT&T, for example, provides potential and existing business customers with the AT&T Information & Network Security Customer Reference Guide, which provides an extensive description of its cybersecurity practices and is attached hereto at Appendix A.

- e. **How widely are cyber security best practices implemented by communications providers and what are these best practices?**

Comments: AT&T's company-specific best practices are detailed in the AT&T Information & Network Security Customer Reference Guide, attached hereto as Appendix A. In

¹⁰⁰ Applying a strict liability standard if a mistake occurs in protecting the network would discourage engineers from making real time decisions to protect communications networks and subscribers from cyberattacks.

¹⁰¹ While communications providers try to provide customers with an accurate picture of security measures, providers appropriately keep certain security information out of the public sphere, and thus out of the hands of potential cyber criminals.

many respects, AT&T's comprehensive security standards stem from similar leading industry standards, including the Control Objectives for Information and Related Technology ("COBIT")¹⁰² and the ISO/IEC 27005:2008.¹⁰³ Given the dynamic cyberspace environment, the library of AT&T security standards is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, operating procedures, tools and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout the company. NRIC has also promulgated extensive best practices, including recommendations on preventing, mitigating, and recovering from cyber security threats.¹⁰⁴

f. What are the specific wireless network features and handset features and capabilities necessary to combat such attacks?

Comments: To protect its wireless network, AT&T maintains a security plan with multiple components including: (1) incident response; (2) awareness; (3) research and development; (4) strategy and architecture; (5) network security measures; and (6) device security measures. Although each of these is critical, the first four components support the network and device security components.

¹⁰² COBIT is a set of best practices for IT management created by the Information Systems Audit and Control Association ("ISACA") and the IT Governance Institute. See "COBIT," ISACA available at <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=31519> (last visited Nov. 10, 2009).

¹⁰³ The purpose of ISO/IEC 27005 is to provide guidelines for information security risk management. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan. The standard was published in June 2008.

¹⁰⁴ See, e.g., NRIC VII Recommendation 7-6-8090 (on restricting the use of dynamic port allocations protocols), available at <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-6-8090>; NRIC VII Recommendation 7-7-8561 (on recovering from a Denial of Service attack), available at <https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=7-7-8561>. See "ISO/IEC 27005:2008," International Organization for Standardization, available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107 (last visited Nov. 10, 2009).

With respect to network security, AT&T leverages the lessons learned and security measures proven effective in its wireline network. Wireless network cyberattacks generally resemble the attacks against fixed-line networks – extraction (*i.e.*, phishing), compromise (*i.e.*, Trojan horses), and disruption (*i.e.*, DDoS). Accordingly, AT&T uses the same security architecture fundamentals across its fixed-line and wireless networks. These include centralized threat management, transport encryption, session boarder controllers, intrusion prevention systems, intrusion detection systems, firewalls, authentication, and access control lists. In addition, AT&T maintains industry standards for GSM/UMTS wireless network security across the six wireless network domains, including Radio Access Network (“RAN”), Circuit Core, Packet Core, Messaging Core, and IP Multimedia Subsystem (“IMS”) Core.

As for device security, tactical and strategic security decisions are not the sole responsibility of AT&T but of a partnership between three parties – platform vendors, original equipment manufacturers (“OEMs”), and operators. Although AT&T maintains a key role in the security configuration of each device that makes its way into the marketplace, both platform vendors and OEMs also retain equal influence over security. To achieve a common synergy between all three parties, the partnership works with two overall objectives in mind: 1) protect customer privacy; and 2) protect the network. AT&T maintains the following guiding strategic principals for achieving these objectives:

- Customers must be informed when applications activate or access sensitive features;
- Security sensitive features can only be accessed by trusted mobile application developers;
- Mobile applications must be reviewed for security threats before they are introduced; and

- Devices must be centrally manageable (remote device updates, configuration changes, application installation and application revocation) by AT&T owned infrastructure.

In addition, AT&T maintains the Mobility Security Center of Excellence (“MSCOE”) to ensure the delivery of secure wireless applications and services within the network and on devices. The MSCOE provides leadership and support in the following domains:

- **MSCOE Network** provides security leadership and direction for the wireless infrastructure, including, but not limited to, RAN, Circuit Core, Packet Core, Messaging Core, and IMS Core.
- **MSCOE Device** provides security analysis and direction on device security issues, including device security controls, platform security models, application signing strategy, and Appstore security strategy.
- **MSCOE Product Development** (Target Architectures, Planning, Technology & Network Resource Planning) creates wireless security target architectures, supports the review of wireless impacting architectures and strategic services.
- **MSCOE Strategic Applications** supports the development of strategic application efforts impacting AT&T Mobility (*i.e.*, web services, cloud computing).
- **MSCOE Mobility Operations** provides direction to operations security teams for wireless infrastructure.
- **MSCOE R&D/Vulnerability Assessment** provides research and development support and strategic vulnerability support.
- **MSCOE Standards** provides leadership and direction for wireless standards initiatives.

These and other initiatives have been effective in thwarting or minimizing cyberattacks.

4. Alerting

- a. **To what extent are broadband technologies currently being used as part of public emergency alert and warning systems? Please provide specific descriptions of their use as part of these systems, including system capabilities and limitations and examples of jurisdictions where such systems are currently in use.**

Comments: AT&T understands the crucial need for the rapid distribution of public safety information during emergencies.¹⁰⁵ In keeping with its commitment to provide its customers with the highest quality service, AT&T receives and transmits National/Presidential, State, and local alerts over its U-verse advanced television service.¹⁰⁶ U-verse TV is a broadband Internet service that provides video in a digital, IP-packet format, using compression and specially developed advanced modem technology. Unlike broadcast, cable, and competing fiber optic-based television services, AT&T U-verse TV is a switched, two-way service, only providing the content to a subscriber that he or she requests, and providing the potential for interactivity.

The AT&T U-verse TV Emergency Alert System solution is based on the current broadcast system for EAS distribution and is fully compliant with the requirements of Part 11 of the Commission's rules,¹⁰⁷ receiving and transmitting all required National/Presidential Alerts. AT&T also voluntarily transmits State and local alerts, including National Weather Service alerts and Amber alerts, and remains in compliance with state emergency alert plans.

AT&T provides these emergency alerts on all content sources, including local broadcast channels, national channels, Public, Education and Government channels, and AT&T U-verse TV special features such as Video on Demand and Digital Video Recorder. AT&T U-verse TV retransmits National/Presidential alerts provided by local broadcast TV stations and national news channels, delivering these alerts to viewers watching other content sources by "force

¹⁰⁵ As the Commission is aware, AT&T has played a leadership role since 2006 in the development of the CMAS for wireless users. Progress continues towards CMAS deployment per the recommendations of the Commercial Mobile Service Alert Advisory Committee established by the Commission.

¹⁰⁶ As of the second quarter of 2009, U-verse TV was available in 105 markets (Metropolitan Statistical Areas) across 19 states and served over 1.5 million customers, with more expansion constantly occurring.

¹⁰⁷ See 47 C.F.R. Part 11.

tuning” them to a pre-selected national or local channel (*e.g.*, CNN or NBC) that will carry the alert. State/local EAS alerts are provided via a text scroll along with the EAS alert tone, repeating on regular intervals, and are delivered only in the affected counties through the use of Federal Information Processing System code targeting. AT&T U-verse TV customers have the ability to dismiss these alerts using the “EXIT” button. AT&T does not override the programming of local broadcast channels, opting instead to retransmit the alerts provided by these stations.

- b. **How can broadband technologies improve the effectiveness of emergency alerts for all Americans, including people with disabilities, people living in rural areas and people who do not speak English? Comments should include information on improvements to message content, geographic targeting, system security, and speed of message transmission from the alert initiating government agency to the public.**

Comments: Emergency alert effectiveness will be greatly improved upon the adoption of the next generation of EAS, which includes digital-based alerts utilizing the CAP. The CAP will provide a uniform format for use in disseminating alert messages simultaneously across a variety of warning systems. Broadband services like AT&T U-verse TV will be able to enhance the utility of emergency alerts by quickly adopting the CAP, which will likely support the following functionalities:

- Improvement in the text content of an alert by putting together more meaningful event information to be displayed to subscribers;
- Ability to support recorded and streaming audio for all alerts;
- Ability to support alerts in multiple languages;
- Ability to support enhanced message update and cancellation features for alert messages;
- Ability to support alerts issued by local Governments with character free form text on those alerts; and

- Continued support for geographic targeting via FIPS code.¹⁰⁸

Adoption of the CAP will allow for more complete and up-to-date emergency information to reach consumers and for a more accurate description of alerting information. It also will allow emergency management personnel to target many non-English speaking customers with alerts in their language and to aid persons with disabilities with more descriptive text and audio alerts than is currently possible. AT&T is monitoring the progression of the CAP and is developing the functionalities that will be required to support the new protocol. Part 11 of the Commission's rules requires that all broadcasters and multichannel video programming distributors support the CAP when it is adopted by the Federal Emergency Management Agency.¹⁰⁹

AT&T is also working in partnership with government players in the development of the CMAS for wireless networks and has filed its election to transmit emergency alerts to its subscribers through CMAS as provided by Commission's Rules.¹¹⁰ CMAS enables geo-targeted emergency alerts to be delivered to wireless devices. As mobile wireless broadband evolves, CMAS may also evolve to provide enhanced alerting capabilities on commercial mobile networks, including increased message size, free-form text capability, multi-language support, and multimedia alerts as specified in the recommendations of the Commercial Mobile Service Alert Advisory Committee.

¹⁰⁸ The Federal Information Processing Standards ("FIPS") code is a sequence of numbers that identifies specific U.S. counties. FIPS codes are used by the National Oceanic and Atmospheric Administration and others to ensure that pertinent emergency information is transmitted specifically to affected areas.

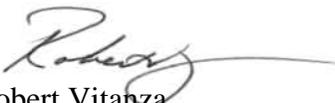
¹⁰⁹ 47 C.F.R. § 11.56.

¹¹⁰ AT&T's election letter is available at <http://fjallfoss.fcc.gov/ecfs2/document/view?id=6520066011>.

III. CONCLUSION

The instant comments detail how the communications industry's broadband efforts – coupled with regulatory flexibility and effective partnerships with government entities – have contributed significantly to the nation's security in the areas being reviewed by the NBP and the *Public Notice*. Going forward, the communications industry will continue to require significant flexibility to meet the evolving needs of law enforcement and the public as well as to defend against the ever-changing forms of cyberattacks. Accordingly, regulators at all levels of government should enhance this flexibility by removing regulatory roadblocks and pursuing effective voluntary partnerships between government and industry where appropriate.

Respectfully submitted,



Robert Vitanza
Gary L. Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036
(202) 457-3076 – phone
(202) 457-3073 – facsimile

Its Attorneys

November 12, 2009

Appendix A:

AT&T Information & Network Security

Customer Reference Guide



AT&T Information & Network Security Customer Reference Guide

November 2008
Version 4.0



TABLE OF CONTENTS

| | | |
|-----------|---|----------|
| 1 | To the Reader | 1 |
| 2 | Disclaimer | 1 |
| 3 | About AT&T | 2 |
| 4 | The AT&T Global Network | 2 |
| 5 | The New AT&T Laboratories | 2 |
| 6 | AT&T Chief Security Office | 2 |
| 7 | The Worldwide AT&T Security Organization | 3 |
| 8 | Security Organization Mandate | 3 |
| 9 | AT&T Security Responsibilities | 4 |
| 9.1 | Senior Executive | 4 |
| 9.2 | Management | 4 |
| 9.3 | Staff | 4 |
| 10 | AT&T Security Standards | 5 |
| 11 | AT&T Security Program | 5 |
| 11.1 | Confidentiality | 5 |
| 11.2 | Physical Access Control Measures | 6 |
| 11.3 | Logical Access Control Measures | 6 |
| 11.4 | Network Element Access Controls | 7 |
| 11.5 | Access Validation Process | 7 |
| 11.6 | Network Perimeter Protection | 7 |
| 11.7 | Intrusion Detection | 8 |
| 11.8 | Workstation Security Management | 8 |
| 11.9 | Payment Card Industry (PCI) Compliance | 8 |
| 11.10 | Security Status Checking and Vulnerability Testing | 9 |
| 11.10.1 | Security Status Checking | 9 |
| 11.10.2 | Vulnerability Testing and Analysis | 9 |
| 11.10.3 | Security Status Reporting | 10 |
| 11.11 | Risk Management | 10 |
| 11.12 | Security Advisory Process | 10 |
| 11.13 | Security Incident Reporting and Management | 11 |
| 11.14 | Security Compliance Reviews | 11 |
| 11.15 | Internal and External Reviews and Audits | 11 |
| 11.16 | Change Management | 12 |
| 11.17 | Business Continuity & Disaster Recovery | 13 |
| 11.18 | AT&T Corporate Management Engagement | 14 |
| 11.19 | Strategy of Continuous Improvement | 14 |
| 11.20 | Personnel Security | 14 |

© 2008 AT&T Intellectual Property, Inc.

All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies



AT&T Information & Network Security Customer
Reference Guide

| | | |
|-----------|--|-----------|
| 11.21 | Security Awareness and Education | 14 |
| 11.22 | AT&T Cyber Security Conference | 15 |
| 11.23 | Security Training and Certifications | 15 |
| 12 | AT&T Security Products and Services | 15 |
| 13 | AT&T Managed Services and Hosting | 17 |
| 14 | Customer Security Responsibilities | 18 |
| 15 | Summary | 19 |



1 To the Reader

This document is designed for the use of AT&T current and potential business customers. The document provides:

- An introduction to AT&T and its global security organization,
- An overview of AT&T's security policy and comprehensive programs that strive to ensure security is incorporated into every facet of AT&T's computing and networking environments. This overview focuses on the key elements and initiatives to safeguard AT&T's customers and their data while managed by AT&T or in transit on an AT&T network,
- A summary of the customers' security responsibilities to protect themselves.

For further information regarding AT&T, visit our website at <http://www.att.com> or contact your local AT&T account team.

2 Disclaimer

This document provides a summary overview of the AT&T security policy and program. In order to maximize security, AT&T does not divulge details regarding the management of security and the tools or processes utilized. AT&T operates a common infrastructure shared by its customers. Consequently, AT&T must safeguard all customers on the shared network platforms, including those with uniquely hosted environments and custom safeguards.

This document is provided as summary information only. It is not a contract, and no statement, representation, characterization within this document shall be construed as an implied or express commitment, obligation or warranty on the part of AT&T Inc. or any of its affiliates, or any other person.

All contractual obligations between AT&T and its customer are set out exclusively in a written agreement with the customer, and nothing in this document shall amend, modify, supplement or otherwise change the provisions or terms of that agreement.

AT&T will, at its sole discretion, alter the policies and procedures described in this document without notice to or consultation with any customer or other person. AT&T customers are responsible for maintaining security policies and programs appropriate to their enterprise.



3 About AT&T

AT&T Inc. is a premier communications holding company. Operating globally under the AT&T brand, AT&T is recognized as the leading worldwide provider of IP-based communications services to businesses and a leading U.S. provider of wireless, high speed broadband Internet access, local and long distance voice, as well as directory publishing and advertising services. AT&T operates one of the worlds most advanced and powerful global backbone networks, carrying more than 16.5 petabytes of data traffic on an average business day to nearly every continent and country, with up to 99.999 percent reliability.

4 The AT&T Global Network

AT&T provides worldwide, world-class network services to businesses in over 50 countries through the AT&T Global Network. Many AT&T customers are multinational corporations with locations in multiple global regions. AT&T is responsible for managing this worldwide data network with presence on six (6) continents. This document relates to security as it is applied to the AT&T global network which consists of multiple components converging into a common Multi-Protocol Label Switching (MPLS) network:

- A global Internet Protocol/MPLS backbone network
- A circuit switched network
- Frame Relay and ATM private networks
- Internal business and management networks
- Intelligent optical network.

5 The New AT&T Laboratories

The new AT&T Laboratories is the driving force behind groundbreaking communications innovations that transform the way people work, live and play. Formerly known separately as SBC Laboratories, BellSouth Laboratories and AT&T Laboratories, the combined AT&T Labs provides technology research and development to the subsidiaries of the new AT&T. Innovations include new technologies, applications and services that support our security portfolio which enhance and safeguard the customer experience.

6 AT&T Chief Security Office

The AT&T Chief Security Office organization establishes policy and requirements, as well as comprehensive programs, to ensure security is incorporated into every facet of AT&T's computing and networking environments. At the executive level, the Chief Security Officer chairs the AT&T Security Advisory Council, a program which key business and functional leaders meet on a regular basis to discuss corporate security strategy, vision, and concerns. This global AT&T security organization's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices.



7 The Worldwide AT&T Security Organization

AT&T maintains a comprehensive global security organization comprised of over 700 security professionals. This organization is dedicated to the physical and logical security of the AT&T global network and its service offerings. It supports a broad range of functions, from security policy management to customer-facing security solutions. The AT&T global security organization reviews and assesses the Corporation's security control posture to keep pace with industry security developments and to satisfy regulatory and business requirements. Recommendations are made to the Corporation on the technology solutions and critical skills that are to be developed or acquired in order to maintain the required security posture. AT&T actively participates in a number of global security organizations such as:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- Security activities within Internet Engineering Task Force (IETF) and the World Wide Web consortium (W3C)
- Forum of Incident Response and Security Teams (FIRST).

In addition, AT&T participates in the following government and government-sponsored organizations in the United States:

- National Coordinating Center for Telecommunications (NCC)
- U.S. Government Department of Homeland Security (DHS)
- Network Reliability and Interoperability Council (NRIC)
- Communications - Information Sharing and Analysis Center (Communications-ISAC)
- Network Reliability Steering Committee (NRSC)
- The National Telecommunications and Information Administration (NTIA)
- National Communications System (NCS)
- National Security Telecommunications Advisory Committee (NSTAC)
- FBI InfraGard
- U.S. Secret Service (USSS) Cyber Crimes Task Force
- National Security Information Exchange (NSIE)
- Shared High Frequency Radio Resources (SHARES) Program
- Communications Sector Coordinating Council (SCC)
- Telecommunications Service Priority (TSP) Oversight Committee.

8 Security Organization Mandate

AT&T considers network and information security to be a cornerstone of the services that it delivers worldwide. By the security policy mandate of AT&T's Chief Security Office, AT&T is committed to protecting its customers and its own information and resources from unauthorized access, disclosure, corruption or disruption of service. This security policy is designed to protect AT&T and AT&T managed assets, and is applicable to network elements, systems, applications and workstations owned or managed by AT&T. Execution of the policy is led by the AT&T Chief Security Office organization whose role is to:



AT&T Information & Network Security Customer Reference Guide

- Protect AT&T Managed assets and resources from security breaches by monitoring potential security threats, correlating network events, and facilitating compliance with legal and regulatory security requirements.
- Own and manage the AT&T security policies and standards for the Corporation and maintain ultimate responsibility for all aspects of network and information security within the Corporation.
- Ensure compliance to AT&T's security policies and network and information security program in a globally consistent manner on all networks, systems, and applications, and ensure senior executives are accountable for security compliance in their business unit or region.
- Provide a competitive advantage to AT&T and offer best-in-class security for our customers.

9 AT&T Security Responsibilities

9.1 Senior Executive

- Senior executives own the responsibility for network and information security within their organizations and are accountable to the AT&T Chief Security Officer.

9.2 Management

- Accountable for protecting assets under their ownership and control.
- Responsible to revoke logical and physical accesses owned by an employee on his/her job reassignment or termination from employment.
- Responsible for the compliance of their staff with the requirements of the AT&T security policies.
- Responsible for conducting logical and physical access revalidation at regular intervals.
- Responsible for developing skills of staff necessary to support the security function.
- Responsible for annual review and acceptance of AT&T Code of Business Conduct with staff.

9.3 Staff

- Comply with AT&T security policies.
- Maintain and execute security status checking processes, security profile/signature upgrades, etc., on systems under their control.
- Validate their personal logical and physical accesses on systems and facilities on a regular basis.
- Comply with confidentiality requirements, customer privacy agreements, government policies where applicable and necessary, and office "clean desk" programs for securing confidential information.
- Comply with the AT&T Code of Business Conduct.



10 AT&T Security Standards

AT&T has developed and maintains a comprehensive set of security standards based in part to similar leading industry standards (COBIT, ISO/IEC 27001:2005, etc.). Given the dynamic environment that AT&T supports, the library of AT&T security standards is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, operating procedures, tools and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout the Corporation.

AT&T's security policies and standards are proprietary to AT&T and are not generally disclosed to any organization or entity external to the AT&T corporate family. Maintaining the confidentiality of this information is, in itself, a facet of our security program that protects AT&T customers.

11 AT&T Security Program

11.1 Confidentiality

To ensure confidentiality, information is accessible only to those authorized. AT&T has implemented a three-tiered Information Classification framework for categorizing information based on sensitivity of the content and specific legal requirements. Document markings are specified for each data classification in order to identify the means and levels of protection required to safeguard information in each classification.

Sensitive customer information especially related to the provision and administration of AT&T services is accorded significant protections, including encryption (where permitted by law) when stored or transmitted on untrusted networks. Customer information managed by AT&T is further protected by requiring personnel to commit to a standard confidentiality agreement on commencement of their employment, and a code of business that assigns severe penalties to violations of these commitments.

AT&T employs information and data destruction and sanitization procedures to ensure that electronic and hard media containing proprietary data and information are physically destroyed or shredded, or properly erased or wiped according to commercially accepted practices when the media or hard copy leaves the control of the company or is no longer required for business purposes. Equipment containing storage media are checked to ensure that any proprietary data and licensed software has been removed or securely overwritten prior to disposal.

The AT&T Privacy organization maintains AT&T's corporate privacy policy. Protection of sensitive personal information or private customer information is addressed in the section "Internal and External Audits and Regulatory Compliance."



11.2 Physical Access Control Measures

AT&T operates in a highly secured environment where physical access to staff office space, switching centers, global network and service management centers and other network facilities is strictly monitored and controlled. AT&T employs many strategies to safeguard these assets by:

- Limiting and monitoring physical access to, and movement throughout, AT&T facilities through the use of physical monitoring and intrusion detection systems.
- Screening access through the use of trained security personnel and/or technical means such as automated card access systems and biometric screening systems.
- Conducting periodic in depth Physical Security surveys and audits of its facilities and locations.

11.3 Logical Access Control Measures

Logical access controls are based on the principle of "Least Privilege". A user who needs access to AT&T's and customers' systems must have a current business requirement, must be allocated a unique identifier (a User ID), and must verify that they are who they claim to be. The following control processes are used to manage logical access:

- Authentication is the process of proving a claimed identity to the satisfaction of an access permission-granting authority. All individual users must be positively and uniquely identified prior to granting access. Authentication of the user is achieved utilizing several methods such as: passwords, personal identification numbers (PIN) and tokens.
- UserIDs and accounts must be reviewed regularly by system and network administrators or access providers to verify that continued authorization and associated command and data access permissions are appropriate for the person's respective job responsibilities. If a valid business reason does not exist for the continuance of such privileges, the access must be removed.
- The "Least Privilege" principle ensures that all access to computer resources is restricted to only the commands, data and systems necessary to perform the authorized functions.
- Security administration of access control measures restricts access to sensitive information by authorized personnel and system network processors, and limits the ability to set, modify or disable system security functions. Privileged access to systems and network elements is tightly controlled.
- Audit logging provides a record for each successful and unsuccessful access attempt. Suspicious access attempts are recognized as security violations and reported. Repeated failed attempts result in the blocking of access.



- All passwords for user authentication (employee, contractor, business partner, etc.) must conform to established rules that specify minimum number and types of characters, uniqueness from previous user passwords, uniqueness from user name or dictionary words, avoidance of repeated characters, limitations on sharing or group use, etc. The passwords must also be changed at regular intervals.

11.4 Network Element Access Controls

Current industry tools are utilized for managing the authentication and approval of support personnel to access the large population of AT&T network routers in the worldwide network. Access is provided to AT&T technical support personnel only on an as-needed basis for individuals with responsibility for network element maintenance and support.

Access is controlled by an authenticating server that validates and verifies user access, ensuring that only personnel currently responsible for managing the customer networks have access. All access to the customer premises devices is logged and repeated failed login attempts are flagged and result in blocking of the offending accounts. Passwords for routers are changed at regular intervals and comply with AT&T internal password policies. Passwords on routers, or their management application, are also reviewed whenever an employee possessing such a password ceases to be employed or has been re-assigned. When strong authentication is required, two-factor token-based authentication is available for access to customer's managed elements.

11.5 Access Validation Process

Only those AT&T personnel with a current business need are authorized physical and logical access to facilities and systems. All managers are obligated to remove staff accesses, (physical and logical accesses) upon staff re-assignment or termination of employment. As a control measure, physical and logical accesses are revalidated regularly at defined time intervals. The owner or operator of the network elements or of the facility is obligated to conduct the revalidation of personnel accesses with their supervising manager to ensure that the staff continues to have a legitimate business requirement for the access.

11.6 Network Perimeter Protection

AT&T external network connections are protected by firewalls that screen incoming and outgoing traffic based on source and destination address, protocol and port, in accordance with the security policy. In particular, Internet connections and Extranets are protected by firewalls and demilitarized zones (DMZs) that block any direct network routing between the Internet and internal AT&T networks.

External customer and partner connections to AT&T networks are protected by access controls (such as access control lists or network based firewalls) that screen incoming and outgoing packets to ensure only authorized traffic is allowed.



11.7 Intrusion Detection

AT&T employs a combination of internally developed and commercial tools to detect attempts by unauthorized persons to penetrate AT&T Global Network. AT&T does not monitor individual customer connections for intrusions, except when part of a managed security service. For customers who have subscribed to this component of managed security service, AT&T will promptly notify the customer via the customer-care representative if it believes that a detected intrusion attempt may impact the customer's service.

11.8 Workstation Security Management

The workstation security policies protect AT&T and customer assets through a series of processes and technologies including verification of personnel workstation accesses, PC anti-virus protection, Operating System hardening and updates, full disk encryption where permitted by law to protect sensitive information on portable assets, along with a personal firewall intrinsic to remote access software implemented on workstations or portable PCs that remotely connect to the AT&T network.

Securing of the personal computer while in use is further managed by the requirements for power-on passwords, hard drive passwords where possible, and password-protected keyboard or screen-locks that are automatically triggered through inactivity. Management at AT&T is responsible for ensuring compliance with these policies.

AT&T workstations are required to have active, up-to-date "anti-virus" software. AT&T's antivirus software vendor regularly provides virus signature updates, which are propagated automatically to workstations across the Corporation. Furthermore, security advisories forwarded by the AT&T global security organization provide key AT&T personnel with details on virus warnings, new security patches and newly discovered vulnerabilities. The anti-virus vendor provides updates almost every business day as well as during virus outbreak emergencies; these updates are propagated automatically throughout the Corporation.

11.9 Payment Card Industry (PCI) Compliance

AT&T is committed to privacy and security compliance in its role as a Merchant of Mobility and other telecommunications services. AT&T's Payment Card Industry Compliance program is a collection of remediation and assessment initiatives addressing major components of security compliance as they relate to the evolving Payment Card Industry Data Security Standard (PCI DSS). This program includes but is not limited to:

- Privacy Masking sensitive data elements
- Encryption (data protection)
- Security Enhanced Software Development Life Cycle
- Secure Email
- Key Management
- Application Firewall rollout

© 2008 AT&T Intellectual Property, Inc.

All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies



AT&T Information & Network Security Customer Reference Guide

The Program also adheres to AT&T security standards as they pertain to security elements addressed during the projects and/or assessments.

AT&T also has a strong commitment to its customers' compliance obligations in its role as a Service Provider of services from its Managed Services portfolio. In 2008, AT&T became the first carrier listed with the Payment Card Industry to offer a portfolio of business network services evaluated against the PCI DSS. Information is available from your account team upon request.

11.10 Security Status Checking and Vulnerability Testing

AT&T conducts regular tests and evaluations to ensure that security controls are maintained and are functioning in accordance with policy. These initiatives include Security Status Checking and Vulnerability Testing. Results from these activities are reviewed and tracked to ensure timely remediation and follow-up actions.

11.10.1 Security Status Checking

- Status Checking is performed on a regular basis to review and verify system security settings, computer resource security settings and status, and users having security administrative authority or system authority.
- Status Checking also includes the testing of network elements to ensure the proper level of security patches, to ensure that only required system processes are active, to ensure the existence and retention of activity logs, and to verify support personnel accesses.
- Validation of server compliance to AT&T security policy is conducted on a regular basis on AT&T servers.

11.10.2 Vulnerability Testing and Analysis

Vulnerability Testing is performed by authorized personnel to verify whether controls can be bypassed to obtain any unauthorized access.

- Vulnerability tests to evaluate the level of safeguards on network components are performed on a varying frequency based on the risk of compromise, utilizing authorized leading-edge testing tools.
- Vulnerability scans are conducted on networks owned by AT&T at regular intervals as directed by AT&T's security policies.
- In addition to AT&T-developed tools, leading-edge scan tools from recognized commercial software providers are used by AT&T for network, computer host and application scans.



AT&T Information & Network Security Customer Reference Guide

Network or computer security analysis is commonly referred to as intrusion testing, sweeps, profiling, and vulnerability analysis. Performing security analysis of the AT&T networks or computers or applications is the responsibility of AT&T. Performance of security analysis by non-AT&T entities is expressly prohibited unless written approval has been obtained from AT&T global security organization management.

11.10.3 Security Status Reporting

Information regarding the security status of AT&T's infrastructure and services is managed and communicated on a need-to-know basis. Results of security health checking and vulnerability testing are tracked and reported by the security programs responsible for compliance management of those activities. Security status, as well as progress on security initiatives, is combined with threat intelligence gathered through trend analysis and reported to security organization executives.

Security program managers share security status information to ensure alignment of program objectives and prioritization of efforts. This disciplined sharing of security status information and reporting enables AT&T to achieve synergy and cooperation among security teams and appropriate management attention on our overall security posture.

11.11 Risk Management

AT&T's approach to identifying and mitigating network and application vulnerabilities is formalized in the Risk Management program. When vulnerabilities are identified, they are assessed as to severity, potential impact to AT&T and its customers, and likelihood of occurrence. Plans are developed, implemented and tracked to address vulnerabilities within prescribed timeframes according to security policy. When business needs preclude timely resolution, the risk level is documented and mitigating controls are put in place where practicable. Executives are expressly accountable for unmitigated vulnerabilities and accept responsibility for the potential risk.

11.12 Security Advisory Process

AT&T utilizes an internal global process to acquire and distribute security advisories, coupled with compliance and review processes as a follow-up to these advisories. The advisories originate from industry security organizations, equipment and systems suppliers. They predominately consist of newly identified flaws to established network software, systems and equipment which could potentially allow unauthorized users to bypass access controls and/or gain access to data.



AT&T Information & Network Security Customer Reference Guide

AT&T continually reviews security patch and vulnerability announcements from vendors and organizations such as CERT for all managed components. The security integrity and advisory process oversees that security patches are applied to network systems in a timely manner.

Each security advisory is categorized, assigned a severity rating and published by the AT&T global security organization, which in turn, dictates the timeframe within which the vulnerability must be resolved.

11.13 Security Incident Reporting and Management

AT&T uses a consistent, disciplined global process for the identification of security incidents and threats in a timely manner to minimize the loss or compromise of information assets belonging to both AT&T and its customers, and to facilitate incident resolution.

The AT&T global network operation centers maintain 24 x 7 real-time security monitoring of the AT&T network for investigation, action and response to network security events. AT&T's Threat Management platform and program provides real-time data correlation, situational awareness reporting, active incident investigation and case management, trending analysis, and predictive security alerting.

In the event of a security incident, AT&T identifies the level of the potential impact and notifies at-risk customers or designated customer contact via the customer's account representative.

Incidents are reported to AT&T's senior management to draw attention to the types of attacks reported by our incident response team as well as other noteworthy incident and vulnerability information.

11.14 Security Compliance Reviews

AT&T considers reviews of operations and applications functions for compliance to security requirements essential to evaluating the adherence to the established security procedures worldwide. Results of these reviews are reported to regional security managers and executive management. Results of internal reviews are not typically shared with customers.

Security reviews may be facilitated or conducted by the Chief Security Office; by a business area sponsor of a product, service, or supplier or partner relationship; or by an operations team responsible for life cycle service management. Business and operations areas are encouraged to perform self-reviews to verify compliance with published security requirements.

11.15 Internal and External Reviews and Audits

In addition to the security compliance reviews, AT&T conducts regular internal and external reviews to address compliance with regulatory requirements such as corporate governance,



AT&T Information & Network Security Customer Reference Guide

Sarbanes-Oxley and privacy requirements. The work-product, results and conclusions from these reviews are proprietary to AT&T and are not disclosed outside of the AT&T corporate family.

External audits and certifications are performed for specific services where business requirements merit third party attestations or compliance evaluation such as SAS 70, SysTrust, Payment Card Industry (PCI) Data Security Standard (DSS) or similar certifications or audits. This information is available from the account team upon request.

AT&T complies with legal and regulatory privacy controls relevant to network services. AT&T network services are available to support customer compliance with regulations in each applicable country such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and security standards as defined through governing bodies such as the European Union. However, most AT&T services do not process or access the customers' personal transactions or information. To the extent that AT&T personnel require access to information subject to privacy regulations, such information is used only for the agreed-upon purpose for which it is collected, unless the customer approves of a different use.

AT&T is willing to engage in general security discussions with a customer or with security organizations representing a customer to address customer questions or concerns. However, security audits and tests conducted by AT&T customers or their representatives are only permitted under specific terms and conditions. Generally, such audits are subject to restrictions and approvals, require contractual agreements on scope and frequency, and call for non-disclosure agreements. In particular, scans and vulnerability tests can only be conducted against systems and devices dedicated to the customer to ensure that such tests do not compromise the services or information of AT&T and its other customers.

11.16 Change Management

To ensure that the integrity of the security infrastructure is not degraded, AT&T uses change management processes to enter, approve, and report change requests. A new change request initiates approval processing and subsequent scheduling of maintenance activity for an 'approved' change request.

The scope of change management program includes but is not limited to:

- Installing or removing software
- Modifying configuration parameters including Operating System (OS) and application security logging and security parameters
- Upgrading to a new release level
- Installing patches or fixes
- Changes to application software
- Changes to hardware



11.17 Business Continuity & Disaster Recovery

AT&T Corporate Business Continuity Planning Services (CBCP) provides technical consultation and program management expertise to address the business continuity, disaster recovery and managed security needs of both AT&T and its customers. Business Continuity Planning Services focuses on all aspects of business continuity required to protect business operations: availability, reliability, scalability, recoverability, performance and security. Working closely with internal and external customers, Business Continuity Planning Services develops a thorough understanding of business needs, applying its knowledge, expertise, and proven methodologies to implement customized solutions.

An integral element of AT&T's business continuity and disaster recovery program is the mandatory process of certifying and assigning assurance levels to critical business operations. The goal of this process is to ensure, through certification, that no critical deficiencies exist.

AT&T networks and services are designed with a level of redundancy and recovery capabilities that enable AT&T to meet contracted Service Level Agreements. Custom solutions with an additional level of redundancy or route diversity can be provided for unique customer needs under specific contractual agreements.

Disasters create chaos, turmoil and heartbreak, but they do not diminish AT&T's commitment to our customers. AT&T recognizes that when a community, town, city, or region is struck by a catastrophic event, the rapid recovery of communications is critical.

AT&T's Network Disaster Recovery plan has three (3) primary goals:

1. Route non-involved communications traffic around an affected area.
2. Provide the affected area communications access to the rest of the world.
3. Recover the communications service to a normal condition as quickly as possible through restoration and repair.

For more information, please visit: <http://www.corp.att.com/ndr/> or contact your AT&T account representative.

AT&T conducts several major disaster recovery tests annually at different customer locations to review all aspects of emergency planning and response, and is leveraging investments in technology, equipment, and processes to support AT&T's Network Disaster Recovery capabilities throughout the world.



11.18 AT&T Corporate Management Engagement

AT&T management is engaged on a regular basis by various aspects of the security program and administration on a level and frequency commensurate with the criticality and impact of results of the programs or incidents as they occur. Following is a summary of some of the situations where management in the service lines is engaged:

- Security incidents as they occur
- Progress from security initiatives
- Threat intelligence gathered by trend analysis
- Results of internal and external audits and reviews

In addition, the management chain receives consolidated reports on a regular basis outlining the results of the security programs and the key issues for their area of responsibility. These reports are delivered to the senior executives as well as the line management.

The most senior executives are required to annually acknowledge their commitment to support corporate compliance. As a part of this requirement, senior executives attest that they and the areas of their responsibility are in compliance with the AT&T security requirements.

11.19 Strategy of Continuous Improvement

The world of networked computing and application security is fast moving and highly dynamic. As a result, AT&T is continually improving security through active security research and development programs, tracking of industry development, and evaluation of new security technologies and products. New tools are employed based on a cost/benefit analysis. The tools and systems selected are those which deliver effective security safeguards.

11.20 Personnel Security

The AT&T Human Resources and Vendor Management organizations have controls in place to ensure that employees, contractors, and subcontractors are properly screened, authorized to perform their job functions, properly trained, and aware of their responsibilities with regard to AT&T and customer assets.

11.21 Security Awareness and Education

The AT&T global security organization is charged with directing and coordinating security awareness and education across AT&T. The AT&T global security organization maintains an Internal security awareness website, a quarterly internal newsletter, all-employee bulletins, technology conferences, workshops and security courses to deliver general and targeted security awareness initiatives internally within AT&T. The program uses subject matter experts from the various security groups and disciplines for content development and partners



AT&T Information & Network Security Customer Reference Guide

with the AT&T education and training organization as well as other AT&T organizations for delivery channels. In addition, all AT&T personnel are required to annually acknowledge their responsibilities to adhere to AT&T's Code of Business Conduct and AT&T's security policy.

11.22 AT&T Cyber Security Conference

AT&T Chief Security Office hosts the annual AT&T Cyber Security Conference to enable open communications with our enterprise customer community on emerging threats and countermeasures within the security industry. The conference promotes awareness of AT&T's strategy and direction to further protect business customers utilizing AT&T network and systems. Contact your AT&T account team for more information.

11.23 Security Training and Certifications

AT&T encourages its employees to obtain security training, achieve accreditation and certifications. This training is conducted both within AT&T and through corporate training organizations such as:

- The International Information Systems Security Certification Consortium, Inc. (ISC)²
- Information Systems Security Association (ISSA)
- The SANS Institute
- Vendor and product-specific training and certification, such as, Cisco, Microsoft, Checkpoint and others.

Our large population of security professionals maintains certifications and credentials such as:

- Certified Information System Services Professionals (CISSP)
- Certified Information Systems Auditors (CISA)
- Certified Information Security Management (CISM)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)
- RSA Certified Security Professional (CSP)
- Microsoft Certified Professional (MCP)
- Cisco Qualified Professional.

12 AT&T Security Products and Services

AT&T offers managed security products and services to its customers, designed to assess and protect their vital network infrastructure. Although AT&T does offer some customized services, by the nature of the design of shared infrastructure, AT&T cannot customize common security settings shared by other customers to unique settings for a particular customer. Contact your Account Manager to discuss customizations and alternative AT&T services that can help meet your needs. AT&T Managed Security Products and Services include:



AT&T Information & Network Security Customer Reference Guide

AT&T Internet ProtectSM is a security alerting and notification service that offers advanced information regarding potential real-time attacks (viruses, worms and distributed denial of service or DDoS attacks) that are in the early formation stages. AT&T DDoS Defense option provides DDoS identification and mitigation within AT&T's backbone providing the customer with increased protection from malicious traffic before it reaches the customer's network. **My Internet Protect** provides customer specific event detection and alert notification. **Private Intranet Protect** provides statistics and reporting from customer's edge routers, including alert notification.

AT&T's Managed Intrusion Detection Service offers network-based and host-based Intrusion Detection Services.

AT&T Firewall Security Services including network-based, premises-based and personal firewall, Management Services designed for maximum performance and business continuity.

AT&T Endpoint Security Service helps customers overcome two critical Internet security challenges: deploying effective firewall policies and enforcing company security policies related to antivirus and application use.

AT&T Token Authentication Service provides enhanced security, called two-factor authentication, to protect the customers' network and applications from access by unauthorized users and malicious hackers.

AT&T Encryption Services provide information confidentiality. The capabilities of this service include data file content confidentiality and email confidentiality to help prevent unauthorized parties from accessing critical messages and attachments. Also included are authentication of the e-mail sender, as well as non-repudiation: a validation of the integrity of the e-mail message and its contents that ensures the recipient that the message was not modified.

AT&T's Secure Email Gateway Service incorporates spam filtering, virus blocking, content management, email policy enforcement, message archiving, and disaster recovery for both inbound and outbound messages, all delivered through a global network of redundant data centers.

AT&T Vulnerability Scanning Service (VSS) is used to continuously and reliably assess networks for vulnerabilities, and provide timely, automatic reporting to enable effective remediation of any vulnerability or emerging threat before any possible exploitation.

AT&T Consultative and Engineering Security Services provide customized security solutions for businesses through consultative and engineering security services which are available to external customers on a "for fee" basis.

AT&T VPN Tunneling Services (AVTS) offer fully managed solutions that allow customers remote access to their corporate LAN using encryption and client-initiated tunneling technology.

AT&T Network Based IP VPN Remote Access (ANIRA) provides business customers with a single solution for remote access from an end-user's personal computer, or Local Area Network (LAN) to corporate LANs, intranets, and extranet(s), as well as the public Internet.



AT&T Government sector services for government agencies and organizations. An example in the United States is the AT&T Access Certificates for Electronic Service (ACES) program which provides PKI and digital certificates to various Federal government (GSA) agencies in addition to managing the internal digital certificates for AT&T.

These products and services may not be available in all regions. For more information on these and other products and services, please visit; <http://www.business.att.com/> or contact your AT&T account team.

13 AT&T Managed Services and Hosting

AT&T Managed Services take advantage of the security of AT&T's global Internet Protocol/Multi Protocol Label Switching (IP/MPLS) network. MPLS technology enables the creation of feature-rich network-based services coupled with AT&T's management expertise, tools and automation. AT&T's network-based managed services include: AT&T Enhanced Virtual Private Network (EVPN) Service, AT&T Virtual Private Network (AVPN) Service and AT&T Managed Internet Service (MIS).

- **AT&T Enhanced Virtual Private Network (EVPN) Service** provides a fully meshed network that excludes having to configure numerous Permanent Virtual Circuits (PVCs). EVPN service bundles network transport with managed router and managed encryption capabilities. It interoperates with other AT&T security services such as managed firewall, managed authentication, anti-virus scanning, Internet ProtectSM, managed intrusion detection, and Private Intranet Protect to provide customers with a complete communications security solution.
- **AT&T Virtual Private Network (AVPN) Service** is a network-based IP VPN solution that provides a menu of transport capabilities. It combines the flexibility of IP access and inherent security with the reliability of frame relay and ATM. Customers can build an application-aware VPN to link global locations, enabling efficient transport of voice, data and video via a single connection. This solution supports customer managed routers and AT&T's managed firewall and intrusion detection services.
- **AT&T Managed Internet Service (MIS)** helps customers consolidate management of their Internet applications with high-speed dedicated access, optimized performance and security. This service provides proactive 24x7 network monitoring, enhanced network security features, and maintenance of the communications links between customer locations and the AT&T network. Customers can select a completely AT&T-managed solution or can choose to self-manage components of their Internet solution.

Hosting Services provide utility computing services that offer tailored or turnkey solutions. The mix-and-match tailored solutions offer IT infrastructure, hardware and/or software components, reliable & secure data center facilities, value-added services (i.e., security, backup and restore, professional services, monitoring, portal/reporting, utility, and disaster recovery), server virtualization, and integrated client networking. A fully managed turnkey solution provides capacity on demand, managed firewall and network Intrusion Detection System (IDS) functionality, proactive alerting and patching, dedicated virtual servers, and total isolation of each client's data in a data center environment.



14 Customer Security Responsibilities

AT&T customers are responsible for safeguarding the security of their enterprise, their data, and any connection to the AT&T Global Network from loss, disclosure, unauthorized access or service disruption. The customer is expected to promptly notify AT&T of any actual or suspected security incidents or vulnerabilities relating to AT&T services of which the customer becomes aware. Prompt notification is required if the customer believes that an unauthorized party has obtained access to the customer's user identifications and passwords, personal identification numbers or tokens.

The customer should have a security policy defined and a security program in place to support the policy. The program should address, at a minimum, physical and logical security, and confidentiality of data. The customer should designate a member of its management team to be the owner of its security policy and program. The customer's security obligations include, but are not limited to:

- Responsibility for protecting the customer's confidential information from disclosure.
- Responsibility for the management of customer data, content and transaction information stored on or transmitted over the AT&T Global Network, e.g., backup and restoration of data, erasing data from disk space that customer controls.
- Responsibility for the selection and use of appropriate services and security features and options to meet the customer's business and security requirements, such as encryption to protect privacy of personal information.
- Responsibility for developing and maintaining appropriate management and security procedures, such as, physical and logical access controls and processes, (e.g., application logon security, including unique user identifications and passwords/pins/tokens complying with prudent security policies) on any customer provisioned and managed networked devices and systems.
- For "Client Managed" customers who retain administrative control of their environment or portions thereof, sole responsibility for their own patch management, including the review, assessment, and application of patches. Under these circumstances, the customer assumes all risks due to vulnerability exploitation, including any additional usage charges due to such incidents. AT&T may disconnect a "Client Managed" customer from the network if AT&T finds them to be infected with a virus or other malicious code such that AT&T or its other customers could be placed at risk. If they choose, "Client Managed" customers may upgrade their service level to "AT&T Managed", in which case AT&T network and information security policies and procedures will then apply.
- Responsibility for the protection and physical security of devices and systems on the customer's premises, including preventing unauthorized sensors, sniffers and eavesdropping devices from being installed on the customer's premises.



AT&T Information & Network Security Customer Reference Guide

- Responsibility to ensure no security testing or scanning, etc sourced by the customer occurs on network or application components outside the responsibility and ownership of the customer.
- Responsibility to ensure that its end users comply with applicable law and also with the AT&T Acceptable Use Policy (found at <http://www.corp.att.com/aup/>) in using any service offered by AT&T that is provided over or includes access to the Internet.
- Responsibility for the acts and omissions of the customer's end users of any service obtained from AT&T.
- Responsibility to notify AT&T promptly of any security breaches detected by the customer related to the services provided by AT&T.

Many country laws (for example, in the United States) prohibit covertly accessing data transmitted over public network or commercial carrier (e.g., Internet) and unsecured transmission lines (e.g., cellular, radio or satellite). However, these open transmission services offer increased opportunity for unauthorized parties to discreetly obtain transmitted data. Consequently, all confidential traffic should be encrypted when transmitted across such networks or lines; ensuring that this protection is in place is the responsibility of the customer data owner.

15 Summary

AT&T Inc. is one of the world's largest communications companies and is recognized as the leading provider of IP-based communications services to businesses. AT&T views network and information security as a process, driven by management direction/directives and user awareness, and supported by expert skills and advanced technology. The security policies, programs and initiatives outlined throughout this document are administered by the AT&T Chief Security Office, worldwide.

This document provides an overview of AT&T's security policies and programs and how they are designed to safeguard AT&T's customers and their data while managed by AT&T or in transit on an AT&T network. This document also provides a summary of the customer's security responsibilities to protect their greatest assets, and heightens their awareness of why they should implement security measures.

For further information regarding AT&T, our security programs and services, please visit our website at <http://www.att.com> or contact your local AT&T account team.