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

In the Matter of	)	
	)	**WC Docket No. 05-196**
E911 Requirements for IP-Enabled Service Providers	)	

COMMENTS OF TELECOMMUNICATION SYSTEMS, INC.

H. Russell Frisby, Jr.
Marc S. Martin
KIRKPATRICK & LOCKHART NICHOLSON GRAHAM
1800 Massachusetts Avenue, NW
Suite 200
Washington, DC 20036-1221
(202) 778-9000

Counsel for TeleCommunication Systems, Inc.

August 15, 2005

TABLE OF CONTENTS

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

In the Matter of	)	
	)	
	)	**WC Docket No. 05-196**
E911 Requirements for IP-Enabled Service Providers	)	

COMMENTS OF TELECOMMUNICATION SYSTEMS, INC.

TeleCommunication Systems, Inc. ("TCS"), by its attorneys, respectfully submits its comments in the above-referenced proceeding.

INTRODUCTION AND SUMMARY

Founded in 1987 in Annapolis, Maryland, TCS is a leading provider of mission critical wireless communications to wireline and wireless carriers and the public safety community. TCS-designed systems include location and messaging products deployed in wireless carrier networks, logistics and proof of delivery applications in enterprise networks, and highly secure communication systems used by government and military customers. TCS's TL-9000-certified network operations centers host messaging and location-based services, including wireless enhanced 911 ("E911") and direct wireless applications.

TCS has significant experience with the deployment of E911 service. The company has contracted to deploy wireless E911 services to over 80 million subscribers on behalf of over 35 carriers and has deployed wireless E911 in 42 states to over 4,600 public safety answering points ("PSAPs"). TCS processes almost half of the wireless E911 calls made in the United States.

TCS has been very much involved in the debate regarding the provision of E911 service for Voice over Internet Protocol ("VoIP")-based technologies and serves as the editor of the Emergency Context Resolution with Internet Technologies (ECRIT) committee of the Internet

Engineering Task Force (IETF). TCS is also an active participant in various efforts associated with public safety, including memberships in APCO, NENA, E911 Institute, and ComCare. It is a charter member of the NENA Next Generation task force and serves on the latest National Reliability and Interoperability Council (NRIC) created at the direction of the FCC.

TCS applauds the Commission's decision to require Interconnected VoIP Service Providers to supply E911 capabilities to their customers.[1] The Commission's action has accelerated the efforts of all parties involved and has encouraged a higher level of collaboration and cooperation. TCS believes that in serving this public interest goal, the Commission should encourage the open and flexible development of innovative E911 technology. VoIP E911 technology fuels a nascent industry that, in the proper regulatory environment, could continue to evolve to better serve the public, particularly in the case of VoIP-based location identification and data transmission applications. The Commission can promote this innovation by providing performance metrics and technical guidelines that avoid favoring one type of network access or interconnection technology over another used to provide VoIP E911 technology. TCS believes that the Commission's decision should be guided by a fundamental principle of network neutrality. Consistent with such principle, the Commission should ensure that:

1. its VoIP E911 rules are generally applicable to all VoIP services used to terminate calls on the PSTN,
2. required interconnections to the PSTN network are technically neutral, and

[1] *IP-Enabled Services*, WC Docket No. 04-36, *E-911 Requirements for IP-Enabled Service Providers*, WC Docket No. 05-196, First Report and Order (Order) and Notice of Proposed Rulemaking, FCC 05-116 (rel June 3, 2005) (*NPRM*).

3. proper guidance is given through the adoption of appropriate performance metrics and technical guidelines.

It should be noted that throughout the remainder of these comments we define the term "Interconnected VoIP Service Providers" ("IVSPs") as VoIP Service Providers that terminate calls to the PSTN (*i.e.,* it is the ability to terminate calls that defines interconnection rather than the combined ability to terminate and originate calls from the PSTN).

ARGUMENT

In the NPRM, the Commission solicited comments as to how it could support the development of VoIP E911 technology to ensure that IVSPs provide ubiquitous and reliable E911 service.[2] TCS believes that the Commission's new rules should broadly apply to all IVSPs, ensure the network neutrality that will be required to properly service a wide variety of IVSPs , and provide direction for IVSP and vendor efforts through the issuance of performance metrics and technical guidelines.

I. THE COMMISSION'S RULES SHOULD APPLY TO ALL IVSP PROVIDERS

The Commission's rules should generally apply to all IVSPs using any technology that permits its end users to terminate calls on the PSTN. If an end user routinely uses or expects to be able to use a VoIP service to terminate calls on the PSTN, then common sense dictates that this pattern of use would extend to a reasonable reliance upon the same method for contacting emergency services. This is a very simple test and a more parsed definition might cause consumer confusion. This is a view supported by the testimony of individuals at the

[2] *NPRM* at page 32.

Commission's open meeting, where it was repeatedly noted that if an IVSP service functions like standard telephone service for the consumer, then the average consumer's common sense expects the service to provide E911. Application of this rule should not be clouded by concerns over the future applicability of Title I regulation[3] or the payment of USF charges. These are questions that can be dealt with later, and as the Supreme Court stated in its *Brand X* decision, the Commission retains the power to impose some "regulatory duties" even under Title I.[4]

This principle of general applicability should also apply to softphones.[5] The Commission must design its VoIP E911 rules not only for today, but also for the future. In the future, softphones, just like wireless telephones today, will likely become the primary telecommunications device for a number of subscribers and will be used to terminate a significant number of the over 20 million VoIP E911 calls that TCS expects will occur on an annual basis by 2009. In an emergency, a user should not have to question whether a device, which is routinely used to terminate calls on the PSTN, is the appropriate device to use.

II. THE FUNDAMENTAL PRINCIPLE OF NETWORK NEUTRALITY SHOULD GOVERN THE COMMISSION'S NEW RULES

The network should be neutral with regard to interconnection and the type of technology used to provide VoIP E911. IVSPs and CLECs must be able to access the ILEC infrastructure

---

[3] 47 U.S.C. § 151.

[4] *National Cable & Telecommunications Association v. Brand X Internet Services*, No. 04-277 and *FCC v. Brand X Internet Services,* No. 04-281, slip op. at 25 (2005) (*Brand X*).

[5] In computing, a softphone is software that simulates a real phone and runs on a general purpose computer, rather than a dedicated device. It is usually used with a headset connected to the sound card of the PC or USB phone. Source: Wikipedia.

that supports PSAPs in a manner that permits the free selection of VoIP E911 technical solutions. As innovations in the VoIP industry continue, it is important that great latitude must be granted to efforts to meet the Commission's Order. Chairman Martin noted, in his statement regarding the Order, that "[b]y not dictating the technical means by which providers must come into compliance, we do not impose undue regulation on these services." We believe that this is recognition that what may work for one provider may not work for another, and that the regulations become onerous only when rigid specifications prevent innovation and competition.

For this reason, it is important that the Commission encourage access to **all** elements required to interconnect to the PSAPs, including but not limited to: trunks to selective routers, data population of selective routers, interconnection to and provision of Automatic Line Identification (ALI) databases, and assignment of pseudo-ANIs (pANIs) which are used to retrieve location data from the IVSP or its third party affiliates. Also, in order to facilitate the neutrality that will allow a rapid response to the Order, industry cooperation should be encouraged or mandated by the Commission.

VoIP E911 technology is still evolving. To succeed, the market needs time to innovate. Network neutrality will encourage innovation by permitting the provision of new VoIP E911 technology by multiple vendors. Network neutrality is also critical because, as the Commission noted in the *NPRM*,[6] unless interconnected VoIP is determined to be a telecommunications service or the IVSP is a certificated telecommunications carrier, then an IVSP is not entitled to receive access to 911 infrastructure and the E911 services provided are not guaranteed to be at parity with those received by an ILEC. Under such circumstances, and without a guarantee of

[6] *NPRM* at pages 23-24, n.128.

network neutrality, the end user may not receive a quality emergency service response. Furthermore, restricting E911 infrastructure access will limit the innovation of new E911 applications. Since the very companies that are classified as information service providers could be denied equal access to E911 infrastructure, an entire segment of the information industry that has demonstrated experience in providing innovative information sharing services would be barred from applying its expertise to new E911 applications.

Network neutrality is also important because a "one-size-fits-all" solution for 6,000 different PSAPs with different levels of technological sophistication will not work. If the networks are not kept open to various E911 technical solutions, then PSAPs will be forced to accept technology that may be inappropriate for them. In such a case, the full potential of VoIP E911 technology may never be realized. The various engineering solutions that may make VoIP E911 technology more efficient may also help to provide support for additional beneficial applications, which could provide more extensive location data, text messaging, pictures from an accident, data from an accident (such as car speed and the presence of passengers), medication allergies of the caller, and other information. Regulatory flexibility and neutrality are the *sine qua non* of innovation.

In order to facilitate the innovation that is so critical for the further development of VoIP E911, the Commission should provide guidance to the industry through the adoption of performance metrics and technical guidelines. In so doing, the Commission's focus should be on solutions and not technology and should be on the needs of public safety rather than the current limitations of the telecommunications infrastructure.

The industry does, however, need guidance. The Commission can provide this by adopting performance metrics and technical guidelines, as well as guidelines for industry cooperation and collaboration.

III. THE COMMISSION SHOULD FACILITATE THE DEVELOPMENT OF IMPROVED AUTOMATIC LOCATION IDENTIFICATION TECHNOLOGY AND PROCEDURES

In the *NPRM*, the Commission requested comment on how it should ensure secure, reliable and automatic location information from portable (sometimes called "nomadic") users.[7] As a first step, the Commission should require that all IVSPs implement improved location determination technology within a reasonable period after it becomes available. Such a requirement will create a ready market for potential developers of this technology.

The Commission should temper this requirement, however, with the parallel adoption of performance metrics that would define the actual availability of this technology. The Commission's metrics should be based on threshold criteria that would evaluate the speed and accuracy of location recognition processes.

IV. ANY VOIP PROVIDER OFFERING SERVICE THAT ALLOWS A USER TO TERMINATE A CALL ON THE PSTN SHOULD BE GOVERNED BY THE COMMISSION'S NEW RULES

In the *NPRM*, the Commission asks, *inter alia*, whether the Commission's rules should apply only to IVSPs.[8] TCS believes that the rules should apply to all VoIP services that enable users to terminate calls to the PSTN. The series of hypothetical examples that the Commission raises in the *NPRM* support the need for the simple test proposed by TCS. End users in a crisis

---

[7] *Id.* at page 33.

[8] *Id.* at page 32.

situation will typically use the device from which they normally place calls to the PSTN. Precious time may be lost if the user is forced to call 9-1-1 from a different device because the IVSP has circumvented the Commission's Order on the basis of a technicality. Note that this simple test would indicate that "softphones" must also provide E911 capabilities per the Commission's Order if that softphone provides termination capabilities to the PSTN. TCS believes that softphones, in particular, will increasingly be used as primary replacement lines. Exempting softphones could leave increasingly substantial numbers of end users without effective E911 capabilities.

V. THE COMMISSION SHOULD ADOPT CERTAIN ADDITIONAL REGULATIONS THAT WILL ASSIST IN THE PROVISION OF EMERGENCY SERVICES

In order to ensure that customers of IVSPs obtain the best possible emergency service, the Commission should adopt additional regulations regarding the usage of uniform nationwide street addresses and wireless broadband location technology.

One step in this direction would be the Commission's issuance of guidance regarding the need for a nationwide Master Street Address Guide ("MSAG"). VoIP offers callers the freedom to make calls wherever they can acquire a broadband connection. Current technology places upon the user the responsibility to provide accurate location information. Most PSAPs require that the address information presented to them match an address in an MSAG that the PSAP maintains. Unfortunately, the MSAG-valid address is often an abbreviated version of the civic street address known by the average person. The combination of portability, cryptic abbreviations, and users who may not be able to provide accurate address information can create situations in which the user's reported location may not coincide with an MSAG-valid street

address. The user's provided address, however, may be sufficiently valid to determine proper routing and/or the dispatch of responders. Although most IVSPs offer some level of MSAG validation, the ability to provide 100% MSAG-valid addresses is contingent upon the ability of the IVSP to access up-to-date MSAGs. As yet, no nationwide mechanism exists by which an IVSP may acquire this data. Some PSAPs make this data available, some make it available at a price, and others refuse to provide it at all. The FCC has properly refused to require MSAG validity of the ALI data provided by the IVSPs to the PSAPs. TCS recommends that the FCC continue to show this restraint and encourage the industry as a whole to allow the use of civic addresses, which are more easily understood by the end user and more readily available on a nationwide basis.

Additionally, the Commission should reexamine how the use of such wireless broadband connections may implicate the Commission's VoIP E911 rules. Although the Commission has explicitly addressed nomadic VoIP services in the latest IP Order and has required the IVSP to obtain a location of the 9-1-1 caller, typically through self-registration techniques, such self-registration methods will not work as IVSPs introduce mobile versions of VoIP that rely upon wireless broadband connections such as Wi-Fi or WiMax. The combination of wireless and IP technology creates at least two situations requiring further examination.

In particular, the Commission should require that location information automatically be provided in scenarios involving wireless broadband connections. Currently, wireless carriers provide the MSAG-valid cell site address. WiFi or WiMax carriers should likewise provide an MSAG-valid hot-spot address. The problem is that cellular towers are owned and operated by the wireless service providers, whereas a hot-spot may typically be operated by any number of vendors unknown to the VoIP provider or even the individual subscriber. The Commission

could choose to adopt a phased approach, similar to requirements affecting CMRS providers. For WiFi, it is likely that a hot-spot address will provide sufficient accuracy. However, WiMax scenarios will much more closely resemble cell towers in the CMRS environment and would need to have stronger location requirements than simply the address of the tower. Thus, the most open approach would be for the Commission to apply accuracy requirements without addressing the technology differences – this would encourage innovative approaches to the problem without dictating specific solutions. As with wireless, however, this requirement should be phased in commensurate with the available technology. WiFi and WiMax could be required to meet the same accuracy standards as those imposed upon wireless: 50 meters/150 meters for GPS units and 150/300 meters for network units.

Additionally, TCS recommends that the Commission work toward requirements for both CDMA and VoIP technologies that are consistent (*e.g.,* a CDMA operator that meets the GPS requirements should meet similar E911 requirements when a customer roams into a WiFi hotspot). Even now, technologies are being tested that integrate wireless broadband and CMRS technologies. This innovation will lead to some difficult challenges for E911. For example, a customer with a CMRS handset may be in a location better served by a Wi-Fi hotspot. In such a circumstance, it is imperative that the customer be oblivious to the change in technology. It is unreasonable to expect a customer, in a crisis situation, to realize that Public Safety might not be able to automatically get and transmit a location fix to the PSAP simply because the call happens to be handled by a WiFi hotspot instead of a CMRS tower. The average consumer is not aware of the differences in technology; the operator, and the underlying vendors and third parties that support that operator, must make such situations transparent to the user.

VI. ADDITIONAL REPORTING REQUIREMENTS SHOULD BE ADOPTED IN ORDER TO MEASURE IMPLEMENTATION EFFORTS

TCS anticipates that a number of IVSPs will apply for waivers asking the Commission for more time to complete the requested tasks. In order to assist the Commission in determining what weight to give such requests, TCS recommends that VoIP service providers should be obligated to report compliance statistics that detail the level of success or failure of their efforts to complete E911 deployments. These statistics should include a status list, PSAP by PSAP, of deployment milestones. IVSPs should be required to report as follows:

First, IVSPs should report when a PSAP was contacted to request permission to deploy E911 service. PSAPs should be protected from IVSPs that would propose to deploy E911 service without the PSAP's permission. Efforts by IVSPs to act without coordinating with the PSAPs would only serve to undermine the efforts of responsible IVSPs.

Second, IVSPs should report the date on which PSAP permission was granted. The FCC should not assume that all PSAPs want or will accept VoIP E911 service. The Commission has already noted that more than one solution exists to support its current VoIP E911 requirements and has properly refused to endorse a specific solution. Reminiscent of wireless E911 "Call Associated Signaling (CAS) vs. Non-Call Associated Signaling (NCAS)" debates, disagreements have already arisen regarding whether a provider has the authority to impose its solution on the PSAP. Conversely, there also exists disagreement as to whether the PSAP can require one solution or another from the IVSP. TCS proposes that IVSPs be allowed to suspend E911 deployments to a PSAP that refuses to allow its chosen method of VoIP E911 support, provided that the IVSP can demonstrate that it has completed in good faith all of the necessary tasks required for deployment. All efforts should be made to encourage resolution of these issues since failing to deploy existing VoIP E911 capability would undermine the intent of the FCC

Order. Recognizing that the FCC may not have jurisdiction to force locally run PSAPs to work with solutions provided by the IVSP, the Commission nonetheless has the ability to influence and work with Public Safety authorities at the national level and can encourage cooperation through NRIC and other methods.

Third, IVSPs should report when a PSAP completes its deployment activities. Based upon the deployment experience of wireless E911, TCS anticipates that many PSAPs will agree to accept VoIP E911 service, but will fail to complete the actions required of them in a timely manner. These actions may include the creation of MSAG records and the approval of ESQKs and trunk orders. Situations such as these make the deployment of VoIP E911 difficult, if not impossible, and provide solid reasons to grant an IVSP relief or waiver from the Commission's VoIP Order.

Fourth, IVSPs should report when the local exchange carrier interconnect to the selective router is complete. Based upon the wireless experience, TCS anticipates delays in the establishment of voice trunks between the IVSP and the selective router. The IVSPs may have no control over this effort, since the IVSP may rely on third party vendors and no other options may be available to access certain PSAPs.

Fifth, IVSPs should report on when the VPC ALI interconnectivity is completed. If the ILECs are permitted to require parallel ALI data circuits in addition to existing ALI circuits, the ILECs may delay the installation of these circuits as they did during wireless E911 deployments. Even if existing ALI circuits are used, the LECs may delay implementation while they upgrade their ALI databases and schedule additional testing. For this reason, TCS recommends that the VSPs report the status of ALI integration with the IVSP's VPC.

Sixth, IVSPs should report on "ready to test." In the rush to deploy, a provider may be prepared to commence testing, but the PSAP, overwhelmed by a multitude of IVSPs who want to test, may have a limited capacity for scheduling the required testing. An IVSP should not be penalized for delays related to the ability of a PSAP to support required testing.

CONCLUSION

For the foregoing reasons, TCS urges the Commission to adopt the proposals described in its comments.

Respectfully submitted,

Kirkpatrick & Lockhart Nicholson Graham, LLP
1800 Massachusetts Avenue, NW
Washington, DC 20036
202-778-9000

Dated: August 15, 2005

By: _____

H. Russell Frisby, Jr.
Marc S. Martin
Attorneys for Telecommunication Systems, Inc.