

**Before The
Federal Communications Commission
Washington, DC 20554**

In the Matters of)	
)	
911 Governance and Accountability)	PS Docket No. 14-193
)	
Improving 911 Reliability)	PS Docket No. 13-75

**INITIAL COMMENTS OF
TELECOMMUNICATION SYSTEMS, INC.
CONCERNING FCC PROMOTION OF A
NATIONAL GOVERNANCE STRUCTURE FOR 911**

**Timothy James Lorello
Senior Vice President
TeleCommunication Systems, Inc.
275 West Street – Suite 400
Annapolis, MD 21401**

**H. Russell Frisby, Jr.
Stinson Leonard Street
1775 Pennsylvania Ave. N.W.
Eighth Floor
Washington, DC 20006**

Table of Contents

Executive Summary	3
Initial Comments of TeleCommunication Systems, Inc.	6
I. The FCC Has Adopted Orders Addressing Multiple Forms of Communication	6
II. Existing FCC Oversight Can Continue as Terminating Networks Fragment	8
III. The Commission’s Ultimate Roles and Responsibilities Should Not Change.....	9
IV. Monitoring, Collaboration, and Resiliency Are Key Guidelines for Improvement	11
V. Monitoring Requires Best Practices and Information Sharing.....	12
VI. Error Events Would Benefit from Collaborative Problem Solving	13
VII. A Predetermined Resiliency Plan Is Critical During Times of Network Impairment	15
VIII. Quality Processes and Cybersecurity Evaluations Should Be Encouraged	16
IX. The Commission Must Address the Threat to 9-1-1 Reliability Resulting from Patent Lawsuits.....	17
Conclusion	20

Executive Summary

The Commission has undertaken an effort to improve the resiliency of the 9-1-1 public safety infrastructure by considering the enactment of rules that will expand the entities currently governed by FCC compliance. TCS submits that existing Commission governance is sufficient to address the changing 9-1-1 ecosystem and that the April 2014 Washington State outage does not support the notion of broader governance, but rather the opportunity to encourage best practices and appropriate collaboration between entities affected by harmful impacts to our 9-1-1 operations.

The Commission's oversight of originating service providers is clear and has been invoked on multiple occasions as new communications methods have become mainstream. All of these systems have traditionally terminated their 9-1-1 calls or texts to well-defined demarcations points – places where the originating service providers' responsibilities stop and where the state or local public safety entities' responsibilities begin. As these state and local entities upgrade the networks for which they provide governance, the FCC should use historical practices as the framework for any future rulemaking.

Where compliance exists, there is no need to expand such compliance to underlying vendors because they already have a contractual relationship with an entity over which the FCC exerts governance.

However, recent 9-1-1 outages, of which the April 2014 Washington State outage was the most severe, have created understandable urgency for analysis and improvement. Three clear areas of improvement are made manifest by actions that were taken during the April outage: network monitoring, problem solving and collaboration, and enhanced network resiliency.

Each of the interconnecting networks that make up our 9-1-1 infrastructure provides its own network monitoring capabilities. Sharing information that results from such monitoring can help identify an impairment before it becomes catastrophic. The Commission could encourage such information sharing or explore ways in which an overarching monitoring structure could be put in place to support the individual network entities.

When an impairment occurs, it is critical that the appropriate personnel and resources are brought to bear on the impairment given the dire impact to life and property that may occur if our 9-1-1 systems fail. Collaboration with stakeholders and experts can greatly mitigate the impact of an impairment or reduce the time to resolution, and the Commission should explore best practices and communication options to facilitate such collaboration.

Alternative routing methods or 9-1-1 service delivery methods need to be in place so they can be invoked if and when a failure in our 9-1-1 systems occurs. The Commission should leverage its resources, such as the Communications Security, Reliability, and Interoperability Council (CSRIC), to help the various communications stakeholders improve their operational resiliency, recognizing that good architectural design is more an art than a science and should not be artificially forced given the wealth of software and hardware design talent available to address these issues.

In addition to the three previously mentioned areas of improvement made manifest after actions taken during the April outage, there are two key foundational guidelines that the Commission should consider: the use of certified quality processes and the importance of strong cybersecurity vigilance.

TCS has long believed in establishing quality processes which use independent third-party quality certification. Having an independent certification process adds useful “outside the box” thinking and observations, and affords a perspective that is separate from underlying business considerations that sometimes lead to poor choices. The Commission could both educate and encourage the use of quality certification.

As we move to IP-based communications systems, the need for strong cybersecurity practices grows more urgent. The Commission’s efforts in CSRIC and other task forces can be instrumental in establishing guidelines for a strong cybersecurity posture in our nationwide 9-1-1 infrastructure.

Finally, we note that the Commission’s interest in expanded governance demonstrates its deep concern for the federally mandated 9-1-1 infrastructure that it oversees, and TCS respectfully asks for Commission action that can help protect this infrastructure from the deleterious effects of frivolous patent litigation.

**INITIAL COMMENTS OF
TELECOMMUNICATION SYSTEMS, INC.**

TeleCommunication Systems, Inc. (“TCS”) hereby submits its initial comments in response to the Notice of Proposed Rule Making (“Notice”) released by the Federal Communications Commission (“Commission” or “FCC”) dated November 21, 2014.¹ The Notice seeks comments on an FCC-initiated effort to promote a national 9-1-1 governance structure.

From a broad perspective, TCS supports the efforts of the FCC to promote a national governance structure for 9-1-1. Given the Commission’s primary purpose of “promoting safety of life and property through the use of wire and radio communications”² and the Commission’s subsequent institution of a 9-1-1 dialing plan³ to provide an easy-to-remember three-digit number to reach emergency responders, TCS believes that the Commission has promulgated the creation of a 9-1-1 infrastructure and believes it has a duty to oversee the resiliency and reliability of this infrastructure. The FCC has clearly exercised this oversight by instituting Orders which have addressed the ever-broadening methods by which the American public communicates.

I. The FCC Has Adopted Orders Addressing Multiple Forms of Communication

The public safety infrastructure initially addressed only one form of communication: wireline calls to 9-1-1.⁴ As telecommunications technology has progressed, the Commission has adopted Orders to address new forms of communication.

¹In the Matters of 911 Governance and Accountability, Improving 911 Reliability, PS Docket No. 14-193 (November 21, 2014) (“Notice”).

² 47 U.S.C. § 151

³ See e.g. Notice at ¶ 1.

⁴ See Task Force Report: Science and Technology, A Report to the President's Commission on Law Enforcement and Administration of Justice (June 3, 1967)

In 1996, the FCC adopted the Wireless 9-1-1 Order⁵ to provide rules and regulations that affect wireless service providers. In 2005, the FCC adopted the Voice-over-Internet Protocol (“VoIP”) Order⁶ to provide rules and regulations that affect interconnected VoIP service providers. In 2014, the FCC adopted the Text-to-911 Order⁷ to provide rules and regulations that affect text providers, whether they are wireless service providers using the FCC-licensed radio spectrum or Over-The-Top (“OTT”) service providers that provide interconnected text messaging using Internet Protocol (“IP”) communications in combination with the underlying wireless communications systems for data transport.

In all of these cases, the Commission addressed methods for new originating “9-1-1” communications methods to access a Public Safety Answering Point (“PSAP”) located nearest to the caller, ensuring appropriate delivery of emergency services to the originating party. Thus, the FCC oversees a broad array of originating communication systems and how they terminate to the public safety infrastructure that ultimately reaches the PSAP. In essence, the FCC has promulgated rules and regulations that ensure the interconnection of multiple originating service providers to the PSAP. Each of these services have a recognized demarcation point – the Selective Router (“SR”) – where the responsibility of the originating service provider (“OSP”) ends and the responsibility of the PSAP begins.

⁵ *Revision of the Commission’s Rules to Ensure Capability with Enhanced 911 Emergency Calling Sys.*, CC Docket No. 94-102, 11 FCC Rcd 18676 (1996).

⁶ *IP Enabled Services etc.* WC Docket Nos. 05-196 etc., First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245 (2005).

⁷ *In the Matter of Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Deployment. etc.* PS Dockets Nos. 11-153 and 10-255 (January 31, 2014).

II. Existing FCC Oversight Can Continue as Terminating Networks Fragment

The Commission has correctly noted that the methods of terminating calls to PSAPs – where the call crosses the originating network’s demarcation point and terminates at the PSAP – are fragmenting with the introduction of Next Generation 9-1-1 (“NG9-1-1”) services. A Local Exchange Carrier (“LEC”) has traditionally provided the communications network to terminate the call at the PSAP using an SR and has provided location delivery through an Automatic Location Identification (“ALI”) system. With the introduction of NG9-1-1 services, these systems are more frequently being provided by a state or local jurisdiction as an Emergency Service IP Network (“ESInet”).

It is important to note that the responsibility for handling the termination of a call to a PSAP has always been within the span of control, and ultimate ownership, of the PSAP. A PSAP might contract the service to a LEC, and the LEC might provide the call and location delivery services via SR and ALI systems, respectively, but the ultimate responsibility lies with the PSAP – an entity typically governed by state and local Public Utility Commission (“PUC”) oversight.

This is where TCS believes that the Commission should respect the authority of its state-managed counterparts. The state and local entities with ultimate authority over PSAPs in their jurisdictions have relied upon SR and ALI services to provide needed control, management, and resiliency of the PSAPs with regard to the termination of traffic to the actual telecommunicator workstations. This is a common responsibility in any enterprise call center that has multiple buildings to manage and multiple call-taker stations within those buildings.

State and larger local governments are now looking at creating ESInets, following well-established business practices promulgated by the Association of Public-Safety

Communications Officials (“APCO”) and industry communication standards initiated by the National Emergency Number Association (“NENA”). In particular, the work that NENA produced associated with the NENA “i3” architecture described a public safety–managed architecture that essentially replaces the SR/ALI architecture currently in place for legacy PSAP systems. In effect, the traditional SR/ALI demarcation points are going through an upgrade and transition to IP-based networks, and by doing so, the state and locally managed public safety infrastructure is living up to the very areas of improvement that have prompted the Commission to suggest intervention. It seems inappropriate to challenge the authority of the entities that are attempting to follow the same areas of improvement that the Commission has imparted.

TCS argues that the evolution of these legacy public safety networks to IP-based ESInets does not change the ultimate role and responsibilities of the Commission. For every 9-1-1 terminating message (whether voice, video, text, or data), the FCC has exercised a certain amount of oversight for both origination and termination networks. The precedents established for the existing origination and termination communications systems should serve as the foundation for future interactions. Where new challenges such as cyber threats and swatting/spoofing have emerged, the FCC can and should play a role, but that role should be informed by historic oversight.

III. The Commission’s Ultimate Roles and Responsibilities Should Not Change

The Commission has traditionally exercised direct oversight of originating service providers through specific rules and regulations concerning the provision of 9-1-1 and the requirements by which location information should be delivered to a PSAP. This is consistent with the creation of the 9-1-1 numbering plan and architecture.

OSPs have often looked to public safety vendors to provide some, many, or even all elements of the public safety infrastructure that meets their responsibilities to the FCC regarding the provision of 9-1-1 services. The FCC has held these OSPs accountable using various enforcement actions, and the OSPs have used their contractual relationships with their vendors to hold the vendors accountable as well.

TCS does not believe that the April 2014 Washington State outage (“Outage”) creates an obligation for the FCC to seek oversight of the OSPs’ vendors. Where a contractual vendor relationship exists with a regulated entity, the creation of a mandate on the vendor results in a duplication of oversight (since the contract already forms that oversight relationship) and the creation of a “second master” that adds limited, if any, value but creates the potential for confusion. In addition, direct intervention could place an undue burden on the vendor, which could receive enforcement action from the FCC and contractual action from its OSP customer or customers. This form of multiple and inflated punishment would be a severe disincentive to vendors, discouraging participation and innovation in public safety technologies because of an upside-down risk/reward scenario. This seems to be antithetical to the Commission’s stated goal to promote innovation.⁸

Similarly, the Outage does not create an excuse for the FCC to begin taking a larger oversight position over systems and facilities that extend beyond the traditional demarcation points currently managed by state and local governments. There is no evidence to imply that such an action would have prevented the Outage, for there was no evidence that either CenturyLink or Intrado were grossly negligent in their efforts to

⁸ See e.g. Notice at ¶¶ 35, 57.

provide a resilient 9-1-1 infrastructure. Though the software error ultimately responsible for the Outage was deemed detectable and preventable, it was the product of human error, and human error will occur with or without FCC oversight. Neither the FCC nor state/local PUCs perform code inspections or load testing – and based upon its years of software and system development experience, TCS believes that only such action could have detected and prevented the error that ultimately caused the Outage. The Outage was not the product of a lack of governance. However, it is both reasonable and expected that the Commission would wish to understand how it could provide appropriate governance to minimize risks and human errors as well as enhance the reliability and resilience of the 9-1-1 infrastructure whose creation it has instigated. TCS suggests looking at industry best practices and draws upon its own experiences during the Outage to suggest some general guidelines for broad improvements.

IV. Monitoring, Collaboration, and Resiliency Are Key Guidelines for Improvement

As the Commission noted in its general report on the Outage,⁹ there were some actions that TCS and its customers took during that Outage that mitigated the impacts on customers' 9-1-1 calls. TCS' Network Operations Center (NOC) personnel detected the Outage, collaborated with its customers to review the problem, and initiated secondary routing techniques that ultimately allowed 9-1-1 calls to flow successfully to the affected PSAPs. TCS respectfully submits that these three elements – monitoring, collaboration, and resiliency – can serve as the foundation for improved FCC oversight. TCS does not suggest that the FCC needs to take responsibility for conducting these efforts, but the

⁹ FCC Public Safety and Homeland Security Bureau *April 2014 Multistate 911 Outage: Cause and Impact*, P.S. Docket No. 14-72 (2014).

Commission can certainly encourage these activities through appropriate guidelines, best practices, and transparent information sharing.

V. Monitoring Requires Best Practices and Information Sharing

The Outage demonstrated that individual network monitoring can be effective in detecting problems in other parts of the network. The 9-1-1 system consists of multiple originating and terminating networks. Each of these networks can identify problems inside and at the borders of its networks, and the service providers of these networks monitor their systems today. However, monitoring is as much an art as it is a science. Knowing what data to collect, how to generate the appropriate alarms, how to appropriately correlate seemingly disparate alarms, and how to determine the appropriate corrective action is an ever-changing challenge.

Tools that afford 9-1-1 network service providers a view of the overall health of each system, along with a characterization of existing or anticipated impairment levels, are essential. Knowing whether a problem has already occurred or will likely occur within some reasonable amount of time can enable the service provider to reconfigure, restart, or redirect services based on a service impairment rating. Such predictive analytics are performed today, driven both by specific service level commitments provided by 9-1-1 service vendors as a Service Level Agreement (SLA) to the OSP or by existing market opportunities identified by vendors outside of specific contractual commitments.

The Commission can play two critical roles with regard to monitoring. First, via its various task forces and studies, including the continued activities of CSRIC¹⁰, the FCC can assist with the identification of monitoring best practices. Second, the FCC could either encourage or provide methods by which interconnected networks can alert each other to detected incidents. During the Outage, each OSP detected a variety of issues, but no mechanism existed to communicate those findings to other OSPs. In fact, because the OSPs and their vendors often are competitors, there are commercial disincentives to communicating problems. Addressing this issue would generate more rapid error detection and enhance problem resolution.

VI. Error Events Would Benefit from Collaborative Problem Solving

Error detection and information sharing are important, but collaboration is critical during a major event such as what happened during the Outage. Having worked in the public safety industry for almost two decades, TCS has had the benefit of interacting with a large number of brilliant technologists, data scientists, and operations managers. When a crisis occurs in which the public safety infrastructure is compromised, finding a way to efficiently and consistently engage these specialists in collaborative issue identification and remediation discussions would likely speed the ultimate resolution of the problem and would certainly improve the communication flow, eliminating speculation and confusion.

Because 9-1-1 emergency calling represents some of the most critically important services available to the public, it is imperative that any disruption to the 9-1-1 service,

¹⁰ FCC links: (current CSRIC IV info)
<http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv>
(CSRIC V announcement)
http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0212/DA-15-203A1.pdf

wherever it occurs, is resolved as quickly as possible. It is with this in mind that TCS has actively worked with other service providers, Public Safety entities, and associated third parties during times of service impairments or outages. TCS recommends a practiced and well-documented business continuity plan¹¹ be in place for a self-administered approach to solving these problems, including the establishment of multiprovider conference bridge administration and information exchange protocols such that all relevant stakeholders are equally abreast of and contributive to the resiliency and remediation of the end-to-end 9-1-1 system. Such a multiprovider communication protocol would facilitate transfer of information in real time and provide a venue for timely analysis, planning, and resolution. Such a protocol also would provide a basis for a clear and coalesced root cause analysis, post impairment, across all stakeholder entities.

Such collaboration exists within individual originating and terminating service providers, but no clear way has been established to communicate between service providers. Similar to the problems seen with sharing monitored information, collaboration between competitive entities is difficult. The Commission could consider the creation of a collaboration process, based on business continuity planning agreements, which would encourage vendors and service providers to communicate issues, suggest solutions, and ultimately reduce the time needed to resolve problems.

¹¹ http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
<https://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf>

VII. A Predetermined Resiliency Plan Is Critical During Times of Network Impairment

When network impairment occurs, a timely resolution can be elusive. During such events, it is important to have embedded network redundancy, alternate routing scenarios, backup plans, and disaster recovery processes already in place.

In order to achieve the level of resiliency required to meet service level commitments, every aspect of the overall ecosystem should be assessed, and a hierarchy of fault tolerance and potential impact should be established within each element of the public safety infrastructure. End-to-end architectures that make up what we know as Enhanced 9-1-1 (“E9-1-1”), VoIP 9-1-1, and Wireline 9-1-1 are composed of many different piece parts, each with its own level of resiliency. TCS recommends that system service providers develop a comprehensive business continuity plan to ensure resiliency, incorporating operational best practices and following design areas of improvement that promote the deployment and ongoing practices of maintaining highly available, fault-tolerant, self-healing, redundant, diverse, and active-active systems and networks.¹² TCS also recommends that, as an integral part of an individual business continuity plan, 9-1-1 system service providers develop disaster recovery processes using assured backup data, practice scenario planning exercises, and participate in continuous training.¹³

¹² TL 9000

7.1.C.2 Disaster Recovery – The organization shall establish and maintain documented plans for disaster recovery, infrastructure, and security restoration (see 6.3.C.1) to ensure the organization’s ability to recreate and service the product throughout its life cycle. Disaster recovery plans shall include, at a minimum, crisis management, business continuity, and information technology. Disaster recovery and infrastructure security restoration plans shall be periodically evaluated for effectiveness and reviewed with appropriate levels of management.

7.1.C.2-NOTE Types of recovery capabilities should include a series of action statements related to disaster recovery. Examples include who is notified, under what circumstances are they notified, who has authority to act, and who will coordinate the steps outlined in the plan.

¹³ ISO 27001

17.1.2 Implementing information security continuity

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

VIII. Quality Processes and Cybersecurity Evaluations Should Be Encouraged

In the development of its public safety systems, TCS has found two additional policies to be critical in provided resilient systems: certified quality processes and cybersecurity evaluations.

TCS has long supported the concept of independent, third-party quality certification of software development processes and network operational processes. Indeed, though TCS believes that the Outage would not have been prevented by stronger government oversight, strong adherence to quality processes may have uncovered the problem before it was deployed in the public domain. Independent quality certifications increase software quality and improve operational performance. As evidence of TCS' long-standing advocacy, the company became ISO 9001 certified in 2003 and recently celebrated its 12th consecutive year of TL 9000 certification. TCS offers the only TL 9000-certified company in support of E9-1-1 services including a Network Operations Center (NOC) for wireless and VoIP E9-1-1 services in the United States. These ISO and TL certification levels can establish a deeply structured and highly applicable foundation for interoperability across 9-1-1 providers as they collectively assess, coordinate, and respond to operational impacts on the 9-1-1 network. TCS is concerned that different or additional certification programs lacking the breadth, depth, and adaptability of ISO and TL would require untenable levels of administration and enforcement, both for the 9-1-1 service providers and the regulators at every level. TCS therefore encourages strong consideration of ISO and TL certifications as the baseline process certifications for 9-1-1 service providers, as they relate to network resiliency and improved operational methods.

TCS also believes that cybersecurity must be a foundational component of any enhanced 9-1-1 network resiliency plan. As with other aspects of E9-1-1 network

resiliency, TCS encourages the use of existing standards, procedures, and specifications. In particular, for public safety, the NENA Security for Next Generation 9-1-1 Standard (“NG-SEC”)¹⁴ provides a tenable and vetted approach to cybersecurity in the NG9-1-1 environment and can act as an important planning tool for legacy 9-1-1 networks as they consider transitions to NG9-1-1 platforms. In fact, TCS believes that the NG-SEC standard requirements should be part of all requests for proposals (“RFPs”) issued for new NG9-1-1 networks. With this type of forethought to safeguarding NG9-1-1 systems, public safety agencies can ensure that their levels of security and availability are commensurate with their duty to protect and serve their communities.

IX. The Commission Must Address the Threat to 9-1-1 Reliability Resulting from Patent Lawsuits

Unfortunately, while acknowledging the critical importance of 9-1-1 services, the Commission has overlooked the very real danger that the public may suffer disruption of current 9-1-1 and E9-1-1 services, and face a clear potential for delay or loss of NG9-1-1 services, due to the infringement lawsuits filed mostly by patent assertion entities (“PAEs”). These PAEs seek to enforce their claims by asserting that deployment of the capabilities (including technologies, systems, and methodologies) necessary to provide 9-1-1 and E9-1-1 services (and very soon NG9-1-1 services) in compliance with FCC orders, regulations, or standards is the proximate cause of alleged infringement.¹⁵

¹⁴ NG9-1-1 ESInet and PSAP relevant security documents available at: <http://www.nena.org/?page=Standards>
NENA 04-503 Network/System Access Security Information Document
NENA 75-001 Security for Next-Generation 9-1-1 Standard
NENA 75-502 Next Generation 9-1-1 Security Audit Checklist Information Document

¹⁵ See generally *Petition of TeleCommunication Systems, Inc. for Declaratory Ruling and/or Rulemaking*, GN Docket No. 11-117 etc. (July 24, 2012) (“Petition”).

Moreover, the problem will worsen as the industry moves toward the implementation of NG9-1-1 because of the large number of internet-based patents which PAEs will be able to draw upon in order to initiate frivolous patent enforcement action. Consequently, TCS believes that the Commission must address this threat.¹⁶

The FCC should grant TCS' request of the Commission to provide interpretive guidance as to the application of 28 U.S.C. § 1498 with regard to the Commission's E9-1-1 and proposed NG9-1-1 regulations. In particular, TCS has sought guidance (a) that based on § 9.7 and § 20.18 of the Rules and Commission precedent,¹⁷ the provision of 9-1-1/E9-1-1 and NG9-1-1 location-based services are in furtherance and fulfillment of a stated Government policy; (b) that the Commission is now aware that its stated policy may require application of a patent if a carrier, their vendor, an 9-1-1 Systems Service Provider (SSP), or a covered 9-1-1 service provider is to comply with FCC regulations; and (c) that 9-1-1/E9-1-1 and NG9-1-1 location-based services are used with the authorization or consent of the government.¹⁸ This issue has arisen and the Commission guidance sought by TCS is required because § 1498 provides a defense to patent infringement liability for those who are alleged to have infringed upon patents in the course of performing a function for the government, and companies operating in the E9-1-1 and NG9-1-1 space are attempting to fight back against infringement claims that

¹⁶ This issue falls within "the scope of this proceeding" because it includes "factors such as the design and manufacture of communications devices or operating systems where they are . . . part of a 911 service relationship between consumers and PSAPs." Notice at FN 10.

¹⁷ See e.g. Report and Order and Second Further Notice of Proposed Rulemaking, In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 18 FCC Rcd 25340, 25345-46 (2003) (E911 Scope Order); Report and Order and Further Notice of Proposed Rulemaking, In the Matter of Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, 11 FCC Rcd 18676 (1996) (E911 First Report and Order).

¹⁸ Petition p. 18-19.

are based largely, if not completely, on their mandatory compliance with 47 C.F.R. §§ 9.7 and 20.18.¹⁹

Commission guidance is both appropriate and necessary in this instance because the FCC has prescribed by regulation the 9-1-1 and E9-1-1 requirements upon which the infringement claims are based and has required that carriers, their vendors, SSPs, and covered 9-1-1 service providers adhere to them. Furthermore, guidance is in the public interest because it will better enable companies subject to the Commission's regulations to determine the risk associated with entering and/or remaining in the 9-1-1, E9-1-1, and NG9-1-1 markets, and perhaps more importantly, it will remove the threat of injunctions which could force these entities to stop providing the capabilities necessary for the continuing provision of 9-1-1 emergency services.

TCS believes that the very fact that the Commission is considering an expansive set of rules that would oversee companies involved in providing 9-1-1 infrastructure is an affirmative declaration that the 9-1-1 infrastructure is provided "by or for the benefit of the U.S. government"²⁰ and that the mandated entities are stewards of this federal responsibility. Should patents be invoked against a mandated entity, the alleged infringer would necessarily be required to continue operation. Or, as described earlier, the plaintiff

¹⁹ In cases filed between 2007 and 2012 where E9-1-1 was implicated (of which many of the 13 cases were multi-defendant litigations) ("E9-1-1 cases"), the affirmative defense of 28 U.S.C. § 1498 was asserted 36 times in answers and amended answers.

²⁰ A Defendant is immunized from liability for actions taken by or for the United States. 28 U.S.C. § 1498(a) (enacted in 1910, subsequently broadened in order to aid the government's procurement efforts during World War I (see, e.g., *Richmond Screw Anchor Co. v. United States*, 275 U.S. 331, 345 (1928)). An accused activity is "for the United States" if it is (1) taken "for the Government", which means "for the benefit of the government" (*Advanced Software Design Corp. v. Federal Reserve Bank of St. Louis*, 583 F.3d 1371, 1378 (Fed. Cir. 2009)); and (2) conducted "with the authorization or consent of the government" (see *TVI Energy Corp. v. United States*, 806 F.2d 1057, 1060 (1986) (authorization and consent can be either express or implied); see also *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976) ("Nor . . . is there any requirement that authorization or consent necessarily appear on the face of a particular contract. On the contrary, 'authorization or consent' on the part of the Government may be given in many ways other than by letter or other direct form of communication").

could request an injunction on such services, potentially disrupting 9-1-1 services for large portions of the U.S. population. These scenarios are key areas of improvement for which 28 U.S.C. § 1498 was created, and it is deeply concerning that the Commission would consider letting this vulnerability continue. As the Commission considers any oversight or governance action with the intent of better protecting the 9-1-1 infrastructure, TCS suggests that the Commission has a similar opportunity and responsibility to remove the 9-1-1 infrastructure's vulnerability to frivolous patent litigation.

Conclusion

TCS believes that current FCC oversight provides appropriate opportunity and authority to address the changing public safety ecosystem without the need to intervene between service provider/vendor contractual relationships or to take a governmental oversight position that has traditionally been performed by state and local governments. The Commission can use existing oversight to provide additional guidance in the areas of network monitoring, problem solving and collaboration, network resiliency, quality process certification, and cybersecurity evaluations; and the Commission can take proactive steps to protect mandated entities, and thereby the 9-1-1 infrastructure, from the damaging effects of frivolous patent litigation.

Respectfully submitted,



Timothy James Lorello
Senior Vice President
TeleCommunication Systems, Inc.
275 West Street – Suite 400
Annapolis, MD 21401

H. Russell Frisby, Jr.
Stinson Leonard Street
1775 Pennsylvania Ave., N.W.
Eighth Floor
Washington, DC 20006

March 23, 2015