

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

In the Matter of

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, 09-137  
PS Docket Nos. 06-229 07-100, 07-114  
WT Docket No. 06-150  
CC Docket No. 94-102  
WC Docket No. 05-196

**COMMENTS OF T-MOBILE USA, INC.**

---

Kathleen O'Brien Ham  
Harold Salters  
Jim Nixon  
Shellie Blakeney  
T-MOBILE USA, INC.  
401 Ninth Street, NW Suite 550  
Washington, DC 20005  
(202) 654-5900

Date: November 12, 2009

## TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY .....	1
II.	A NATIONAL INTEROPERABLE BROADBAND NETWORK FOR PUBLIC SAFETY CAN BE DEVELOPED AND FUNDED BY AUCTIONING THE D-BLOCK FOR COMMERCIAL PURPOSES.....	4
III.	NEXT GENERATION 911 CAN YIELD STRONG IMPROVEMENTS IN EMERGENCY ACCESS, BUT WILL REQUIRE A COMPLETE CHANGE IN THE 911 SYSTEM.....	6
IV.	COMPETITIVE MARKETS INCENT WIRELESS CARRIERS TO ADVANCE THE BEST AVAILABLE TECHNOLOGY TO PROTECT NETWORKS FROM CYBERSECURITY HARMS .....	11
V.	IMPLEMENTATION OF WIRELESS EMERGENCY ALERTS IS WELL UNDERWAY .....	14
VI.	CONCLUSION.....	18

---

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

In the Matter of

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, 09-137  
PS Docket Nos. 06-229 07-100, 07-114  
WT Docket No. 06-150  
CC Docket No. 94-102  
WC Docket No. 05-196

**COMMENTS OF T-MOBILE USA, INC.**

**I. INTRODUCTION AND SUMMARY**

T-Mobile USA, Inc. (“T-Mobile”) provides these comments in response to the Commission’s additional inquiries with respect to public safety, homeland security and cybersecurity and the National Broadband Plan.<sup>1</sup> The Commission can help improve public safety communications and our nation’s security by taking several steps to encourage the widespread deployment of broadband, including the deployment of underlying facilities. First, a public safety broadband network needs to be funded – which can best be done by auctioning the 700 MHz D Block for commercial use and dedicating the proceeds to public safety broadband deployments. Second, Next Generation 911 is an opportunity for a substantial advance in community access to public safety and in delivering better information to first responders, but it can be effectively accomplished only as a wholesale systems change across both industry and the

---

<sup>1</sup> See *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice #8, DA 09-2133 (rel. Sept. 28, 2009) (“NBP Public Notice #8”).

public safety community. Third, with respect to cybersecurity, carriers have strong incentives to protect their systems that affect the provision of wireless services, and have adequate mechanisms in place to help safeguard these assets. Rigid regulation could hinder those efforts. And, fourth, the Commission should facilitate the timely implementation of the Commercial Mobile Alert Service (CMAS) by ensuring that the current requirements and implementation plans are not altered.<sup>2</sup>

Over the years, T-Mobile has demonstrated its commitment to supporting important public safety and homeland security interests. A number of T-Mobile expert personnel have been intimately involved in a variety of industry and government fora aimed at, among other things, improving network security, interfacing with the public safety community, and developing industry technical standards. At the federal level, for example, T-Mobile is a charter member of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC),<sup>3</sup> and served on CSRIC's predecessor councils on network reliability and interoperability matters. In fact, our Senior Vice President for Engineering and Operations recently was selected to sit on the CSRIC,<sup>4</sup> providing the FCC with someone who has a high profile at our company and in industry and who has vast experience with network operations. T-

---

<sup>2</sup> The Warning, Alert and Response Network Act (WARN Act), Pub. L. No. 109-347, §§ 601-613. 120 Stat. 1936-1943 (2006), required the Commission to establish an advisory committee, the CMSAAC, tasked with recommending technical standards and other requirements enabling commercial wireless service providers voluntarily to transmit emergency alerts. *Id.* at § 603. The CMSAAC included experts representing public safety organizations, Federal and local governments, Tribal leaders, wireless carriers, broadcasters, rural carriers, public television stations, and disability and elder rights organizations. The Committee met between December 2006 and October 2007, when it submitted its recommendations to the Commission.

<sup>3</sup> See Federal Communications Commission, FCC Announces Membership Of The Communications Security, Reliability, and Interoperability Council (CSRIC), Public Notice, DA 09-2297 (Oct. 26, 2009) .

<sup>4</sup> *Id.*

Mobile also has been involved in efforts at both FEMA and the FCC concerning Emergency Support Function-2 (ESF-2) preparedness.<sup>5</sup> Company representatives hold key roles on the ATIS Network Reliability Steering Committee (NRSC), recently serving on the NRSC Best Practices team. The intensive work of the NRSC team resulted in the Pandemic Best Practices document, which was released on August 31, 2009. In addition, T-Mobile chairs the NRSC's Wireless Sub-team, which addresses FCC Network Outage Reporting Systems (NORS) concerns, as well as co-chairs the Outage Reporting Advisory Sub-team, which has regular liaison with the Commission. T-Mobile has been working closely with Commission staff on the Commission's Disaster Information Reporting System (DIRS) and commends the staff for their efforts in developing this important program.

T-Mobile similarly has played an active role in the development of the CMAS from its inception.<sup>6</sup> T-Mobile held a leading position on the FCC's CMSAAC and has filed its letter of intent to participate in this voluntary system. The Company is also engaged in the standards development process for CMAS, including the final, approved joint ATIS/TIA specification for

---

<sup>5</sup> ESF-2 is part of the Department of Homeland Security's National Response Function, which provides guiding principles for a coordinated national response to disasters and emergencies. The 15 ESFs provide the structure for coordinating Federal interagency support for disaster response. FEMA, *Emergency Support Function Annexes: Introduction* (Jan. 2008), <http://www.fema.gov/pdf/emergency/nrf/nrf-esf-02.pdf>. ESF-2 addresses communications support. Specifically, ESF-2 provides emergency communications support to Federal, state, tribal, and local governments and first responders during a non-wartime emergency, including cyberattacks. It also supports restoration of communications infrastructure, facilitates recovery of systems and applications, and coordinates Federal communications support to respond to such incidents. FEMA, *Emergency Support Function #2 – Communications Annex* (Jan. 2008), <http://www.fema.gov/pdf/emergency/nrf/nrf-esf-02.pdf>.

<sup>6</sup> See generally, Comments of T-Mobile on Notice of Proposed Rulemaking, PS Docket No. 07-287 (filed Feb. 4, 2008); Reply Comments of T-Mobile on Notice of Proposed Rulemaking, PS Docket No. 07-287 (filed Feb. 19, 2008).

the Federal Alert Gateway Interface, which is expected to be released soon, and has worked with the DHS Science and Technology Directorate on aspects of the initiative.<sup>7</sup>

T-Mobile is engaged in pandemic planning, addressing issues relating to health crises such as H1N1 flu or other potential pandemics, and participates in a number of public safety efforts such as the AMBER Alert program. Our desire to provide customers a first-rate wireless experience is a significant incentive for T-Mobile to invest in network continuity.<sup>8</sup>

## **II. A NATIONAL INTEROPERABLE BROADBAND NETWORK FOR PUBLIC SAFETY CAN BE DEVELOPED AND FUNDED BY AUCTIONING THE D-BLOCK FOR COMMERCIAL PURPOSES**

In its NBP Public Notice #8, the Commission recognizes some of the advantages of ensuring broadband access by public safety agencies and seeks further comment as to how best to meet public safety's needs for mobile wireless networks.<sup>9</sup> Specifically, with increased access to mobile wireless broadband service, the FCC envisions public safety organizations having enhanced tools necessary to carry out their responsibilities. For instance, the Commission offers examples of how firefighters and police officers would benefit from such advanced capabilities - *e.g.*, accessing a recent video of a fire or crime scene.<sup>10</sup> Likewise, the Commission notes such

---

<sup>7</sup> T-Mobile also participated in the DHS Request for Information process for establishing a CMAS research, development, testing, and evaluation program; *See* U.S. Department of Homeland Security, Science & Technology Directorate, *Request for Information No. HSHQDC-09-R-00105 Commercial Mobile Alert Service Research, Development, Testing & Evaluation* (rel. July 28, 2009), <https://www.fbo.gov/utills/view?id=0ace9232af169632261408e1c22180de>.

<sup>8</sup> T-Mobile recently achieved recertification through CTIA's Business Continuity Certification Program, reflecting its commitment to providing outstanding and uninterrupted service to its customers. *See* Letter from Steve Largent, President/CEO, CTIA-The Wireless Association®, to Kathleen O'Brien Ham, Vice President, Federal Regulatory Affairs, T-Mobile USA, Inc. (Oct. 14, 2009).

<sup>9</sup> *See NBP Public Notice #8.*

<sup>10</sup> *Id.*

networks would enhance public safety's ability to provide alerts and emergency information to the public.<sup>11</sup>

As the Commission examines how best to develop a national interoperable broadband network for public safety organizations, we urge it to consider carefully all proposals for meeting its objective. In T-Mobile's view, the 700 MHz D Block presents a unique opportunity for public safety, as well as commercial mobile service providers and, ultimately, consumers. Auctioning the D Block solely for commercial purposes, with the auction proceeds directed to fund the build out and maintenance of a nationwide, interoperable public safety broadband network, presents a solution that would best serve the needs of all stakeholders involved and, most importantly, the American public.<sup>12</sup>

Of the 24 MHz of spectrum at 700 MHz allocated for public safety use, the existing 10 MHz block of paired spectrum, currently designated for broadband services, is sufficient to support a public safety broadband network at this time – particularly if the network takes advantage of new, more efficient technologies.<sup>13</sup> Funding continues to be a key factor in – and a key obstacle to – enabling progress here. Given the current economic environment and resource constraints facing many, if not most, local and state governments, public safety agencies confront

---

<sup>11</sup> *Id.*

<sup>12</sup> See Letter from Thomas J. Sugrue, Vice President – Government Affairs, T-Mobile USA, Inc., to the Hon. Rick Boucher, Chairman, and the Hon. Cliff Stearns, Ranking Member, Subcommittee on Communications, Technology and the Internet, Committee on Energy and Commerce (Sept. 23, 2009) (“T-Mobile 700 MHz Letter”) (attached as appendix to *Ex Parte* Letter from Cheryl A. Tritt, Counsel to T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC (Sept. 24, 2009)).

<sup>13</sup> See *A National Interoperable Broadband Network for Public Safety: Recent Developments: Hearing Before the Subcomm. on Commc'ns, Tech. & Internet of the H. Comm. on Energy & Commerce* (Sept. 24, 2009) (written statement of Kostas Liopiros, Ph.D., The Sun Fire Group), [http://energycommerce.house.gov/Press\\_111/20090924/liopiros\\_testimony.pdf](http://energycommerce.house.gov/Press_111/20090924/liopiros_testimony.pdf) (“Liopiros Statement”); see also T-Mobile 700 MHz Letter at 4.

ever more acute funding challenges. Identifying a dedicated source of funds to help build and maintain a public safety broadband network therefore would be a major step forward.<sup>14</sup>

Auctioning the spectrum at 700 MHz to help meet current and anticipated consumer demand for advanced wireless services presents the best opportunity for getting necessary funding to develop an interoperable broadband network for public safety organizations, as well as facilitating competition in the wireless marketplace.<sup>15</sup>

### **III. NEXT GENERATION 911 CAN YIELD STRONG IMPROVEMENTS IN EMERGENCY ACCESS, BUT WILL REQUIRE A COMPLETE CHANGE IN THE 911 SYSTEM**

There is no question that moving the 911 system to a modern IP-based, integrated network would yield substantial benefits in terms of public communication with emergency response dispatchers and information for first responders. But it is also well-documented – most recently by the National E9-1-1 Implementation and Coordination Office’s report, *A National Plan for Migrating to IP-Enabled 9-1-1 Systems* – that implementation of next-generation 911 (NG911) systems requires substantial changes in what has heretofore been thought of as the PSAP’s side of the 911 system, including state or regional backbones, routing plans, software and customer premises equipment.<sup>16</sup> This represents not simply an upgrade of the existing 911 network, but a wholesale replacement, without which many significant changes in carriers’ capabilities would be unusable. T-Mobile has been an active participant in NG911 development efforts, and will continue to do its part in this transition. However, it is critical that a NG911

---

<sup>14</sup> *Liopiros Statement* at 2-3.

<sup>15</sup> *Id.*; T-Mobile 700 MHz Letter at 5 (“Although the auction proceeds alone would not be sufficient to fully fund and maintain a nationwide public safety broadband network, they would provide a valuable beginning and make the remaining funding challenges more manageable.”).

<sup>16</sup> The National E9-1-1 Implementation Coordination Office, *A National Plan for Migration to IP-Enabled 9-1-1 Systems* at 2-1- 2-2 (Sept. 2009), [http://www.e-911ico.gov/NationalNG911MigrationPlan\\_sept2009.pdf](http://www.e-911ico.gov/NationalNG911MigrationPlan_sept2009.pdf) (“NET 911 Act Report”).

transition address all parts of the system, and not just those controlled by carriers – as has often been the case in the past.

Most of the questions raised in the Public Notice are addressed by the National E9-1-1 Implementation and Coordination Office's *NET 911 Act Report*. For example, that report discusses the multiple efforts underway to develop NG911 standards, and also catalogs the various state and local trials and other IP-based 911 implementations.<sup>17</sup> The report also describes the location technologies that vendors are developing for potential use in 911 systems – although few of these technologies are currently in use in commercial networks.<sup>18</sup> T-Mobile thus limits its comments here to a few key points.

As recent reports have documented, the current 911 system is built on legacy analog communications technologies that substantially constrain the adaptability of the 911 network to new technologies, and that substantially limit the incorporation of new technologies into the 911 system.<sup>19</sup> The analog network technology embedded in the 911 system is a fundamental technological barrier to a next-generation 911 system: “[T]he 9-1-1 network remains a voice-centric environment in a data-centric world.”<sup>20</sup> Equally apparent, this is not just a limitation within the communications networks, but an overall systems problem. As Weiser, Hatfield and

---

<sup>17</sup> *NET 911 Act Report* at 1-10, 6-1 – 6-11.

<sup>18</sup> *See Id.* at Appendix B. With respect to location technologies, in order to be technically feasible, these technologies must not only work in the laboratory and field trials, but must also be standardized so that they can be incorporated into mass produced handsets and/or network elements without creating overall systemic reliability problems. Moreover, they must work within the specific handset's environment, including power consumption and not interfering with the handset's other radios.

<sup>19</sup> *See* Philip J. Weiser, Dale Hatfield & Brad Bernthal, *The Future of 9-1-1: New Technologies and the Need for Reform*, 6 J. Telecomm. & High Tech. L. 213, 225-43 (2008) (describing the evolution of current generation 911 systems and the technical limitation that current technology places on the 911 systems) (“*Future of 9-1-1*”); *NET 911 Act Report* at 2-2 - 2-3.

<sup>20</sup> *Future of 9-1-1* at 239.

Bernthal noted, “even with the adoption of a modern all-digital, broadband, IP-based packet switched network (i.e., one capable of conveying voice, text, data, image, and video traffic) for 9-1-1 traffic, PSAPs would still lack the capability to receive, process and display such information without upgrading their CPE.”<sup>21</sup>

The potential benefits and difficulties in NG911 implementation are illustrated in the example of text-to-911. It clearly would be helpful for consumers to have the ability to send text messages to 911, provided that this could be done reliably. Many consumers use text messaging, and, in disasters, some have tried to text to 911. Moreover, for hearing impaired individuals, text messaging would provide a better way to reach 911 than cumbersome TTY equipment.

The predominant mode of texting today, however, is a store-and-forward service, not a real-time service. As such, there is no guaranteed delivery, and messages do not necessarily arrive promptly or in sequence. This can result in substantial confusion, as well as danger to the public if, for example, messages intended, to be read “Evacuate the building” and “Cancel the evacuation” arrived in the opposite order: “Cancel the evacuation” and then, “Evacuate the building.”<sup>22</sup> SMS messages also lack a means of authentication, which means they can be forged. Most significantly, SMS systems are not tied in with location identification systems.<sup>23</sup>

---

Furthermore, SMS systems route messages to the home carrier’s network. For voice 911 calls, in contrast, the receiving CMRS carrier handles the call, even if from a non-subscriber or a

---

<sup>21</sup> *Future of 9-1-1* at 238. The authors paraphrased an E9-1-1 professional they interviewed as follows: “upgrading the network side of the system without upgrading the PSAP equipment itself will only move the bottleneck or chokepoint from the last few miles to the last few feet.” *Id.*

<sup>22</sup> See Patrick Traynor, *Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Systems* 17 (Sept. 2008) (“Traynor EAS Report”).

<sup>23</sup> *NET 911 Report* at 6-7.

roamer.<sup>24</sup> And SMS systems, unlike voice calls, do not provide “the call taker with an easy method of caller interrogation.”<sup>25</sup>

Substantial changes thus would be necessary even to begin developing a texting capability robust enough to support 911 access. GSM carriers, including T-Mobile, are addressing the incorporation of such a robust real-time texting capability for emergency access in the context of 4G (LTE) standards development. As of today, however, a useful text-to-911 system is not technically or operationally feasible.

Moreover, even if such a system were technically feasible in the carrier networks, the overall systems are not in place to utilize the data. In the first instance, PSAPs would have to have a way to receive SMS messages and display those messages on emergency screens at the PSAP. Today’s 911 infrastructure generally will not permit that, and PSAPs generally do not have CPE that accommodates this function. In addition, call takers would need to be trained to handle multiple, simultaneous SMS messages – which is contrary to the way that PSAPs generally operate today.<sup>26</sup> All these issues need to be resolved before a viable text-to-911 system can be established – and all parts of the problem must be addressed for any part of the solution to be useful.

---

The Public Notice asks about regulatory roadblocks to NG911 implementation. The *NET 911 Report*, Weiser, Hatfield, and Bernthal article, and NENA’s *A Policy Maker Blueprint for Transitioning to the Next Generation 9-1-1 System* all describe the many legal and regulatory barriers to implementation of NG911, the vast majority of which are a function of state and local

---

<sup>24</sup> For example, prototype text-to-911 systems today require the caller to enter his or her location as part of the text message.

<sup>25</sup> *NET 911 Report* at 6-7.

<sup>26</sup> *Id.*

organization, governance and funding with respect to PSAP operations. T-Mobile provides comment with respect to two specific regulatory roadblocks.

First, the FCC's E911 rules, as written, include provisions precluding NG911 deployment. In its VoIP E911 rules, for example, the Commission specifies that all 911 calls must be delivered "via the dedicated Wireline E911 Network," which is defined as including a Selective Router.<sup>27</sup> Similarly, in wireless E911, the selective router is the demarcation point between the wireless network and the PSAP's network.<sup>28</sup> A selective router, however, resides in an ILEC tandem office that is specific to current generation 911 deployments.<sup>29</sup> As NENA has observed, these rules do not "clearly include the routing of 9-1-1 calls via an IP-based NG9-1-1 system."<sup>30</sup> The Commission should clarify its rules so that all parties know they can implement NG911 architectures without further regulatory approvals or waivers.

Second, the welter of technology-specific provisions in various state and federal 911-related rules creates problems for 911-implementation with respect to new services. For example, the FCC's CMRS 911 rules require PSAPs to request wireless E911 (either Phase 1 or Phase 2), but require interconnected VoIP providers to deliver all calls with location information to any PSAP that can receive and process ANI or location information, irrespective of whether the PSAP makes a request. Similarly, 911 fees can vary, and be paid to different entities,

---

<sup>27</sup> 47 C.F.R. §9.5.

<sup>28</sup> *Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Request of King County, Washington*, Order on Reconsideration, CC Docket No. 94-102, 17 FCC Rcd. 14,789 (2002).

<sup>29</sup> *The Future of 9-1-1* at 228-30 (describing the selective router and its limitations).

<sup>30</sup> National Emergency Number Ass'n, Next Generation Partner Program, *Transitioning to the Next Generation 9-1-1 System; Issues and Recommendations for State and Federal Policy Makers to Enable NG9-1-1* at 11, [http://www.nena.org/sites/default/files/NG9-1-1PolicyMakerBlueprintTransitionGuide-Final\\_0.pdf](http://www.nena.org/sites/default/files/NG9-1-1PolicyMakerBlueprintTransitionGuide-Final_0.pdf).

depending upon whether a service is “wireline” (including at least some forms of interconnected VoIP) or wireless. In addition, the point of delivery for a call, and the information to be provided, can vary between “wireline” and “wireless” calls, raising a slew of questions as services begin to converge and can be delivered via multiple delivery modes. These inconsistencies create barriers to the successful implementation of a new NG911 system, and to the deployment of new services and technologies within the existing 911 system.

The implementation of a NG911 system unquestionably will be a major advance for access to public safety services and for PSAPs to gain valuable information to help first responders carry out their jobs. But, this is not just an incremental upgrade; the entire 911 infrastructure within a particular region will have to be changed in order to obtain these benefits. T-Mobile continues to work with NENA and other stakeholders on NG911 standards and procedures, some of which are specifically designed to allow NG911 PSAPs to communicate with legacy PSAPs (although in these situations the level of services available will vary according to the current state of each PSAP). Through the combined public safety, industry, and governmental efforts, consumers will, in the foreseeable future, be able to access the full benefits of a modern, integrated, and technologically advanced NG911 system.

---

#### **IV. COMPETITIVE MARKETS INCENT WIRELESS CARRIERS TO ADVANCE THE BEST AVAILABLE TECHNOLOGY TO PROTECT NETWORKS FROM CYBERSECURITY HARMS**

The Public Notice asks what market incentives exist for commercial communications providers to invest in secure infrastructure.<sup>31</sup> The answer is that the market provides substantial incentives to make these investments. The wireless market is highly competitive, meaning that a provider’s brand and image are vital to its continued success. Service reliability and consumer

---

<sup>31</sup> See NBP Public Notice #8 at ¶ 3c.

confidence in a carrier's service are critical to developing and maintaining a competitive edge in a maturing market. Spammers, hackers, botnets, and other attackers attempt to disrupt and damage networks and put subscriber data at risk. Furthermore, spam to both text and email is a significant customer nuisance – and potential cost to the carrier. Carriers, therefore, have every business incentive to manage their networks to ensure ample protections are in place for safeguarding network and consumer information, and to maintain service continuity even in the event of a cyberattack.

An important distinction should be made between network facilities that are critical to maintaining network service, and those customer-facing support facilities, such as websites and value added services, which do not affect network service. For its network, T-Mobile has physical and logical security in place to protect its network and physical assets. In addition, T-Mobile is aligned with the International Organization for Standardization (ISO) 27000-series, which provide best practice recommendations on information security managements and controls. Although these efforts are effective, cyberattacks constantly evolve.<sup>32</sup> Thus, cybersecurity practices must be dynamic and flexible. This approach will facilitate carrier efforts to effectively protect and, when necessary, respond to malicious acts targeted at any network.

---

Although industry-wide best practices in cybersecurity have yet to be established, the NRSC is looking to initiate a preliminary investigation into this issue. In addition, cybersecurity may be identified as a primary matter for consideration by the Commission's newly-formed CSRIC. T-Mobile recommends as a general principle that cybersecurity be addressed in the

---

<sup>32</sup> *National Broadband Plan Workshop: Cybersecurity, Federal Communications Commission* (Sept. 30, 2009) (comments of John Nagengast). As noted at the Commission's September 30, 2009 Cyber Security Workshop, "[t]he speed and the threat [are] rapidly advancing" and cybersecurity "is a continuing saga" ("*FCC Cybersecurity Workshop*") [http://broadband.gov/docs/ws\\_26\\_cyber\\_security.pdf](http://broadband.gov/docs/ws_26_cyber_security.pdf).

context of industry-government collaboration on best practices, rather than via government-imposed standards. Collaborative best practices driven by industry allow the flexibility to combine the public's concern with cybersecurity in critical infrastructure with the inherent dynamism and rapid evolution of wireless carrier networks. Further, best practices are the preferred design for providing carriers with the necessary flexibility to address their individual and rapidly evolving security needs. T-Mobile also has met with FEMA regarding emergency preparedness and has been involved with DHS's transition to a consolidated watch program, the National Cybersecurity and Communications Integration Center (NCCIC).<sup>33</sup> T-Mobile continues to work cooperatively with these organizations.

With respect to the customer-facing portion of their system, carriers need flexibility to respond immediately to evolving threats specific to their systems. Not all cyberattacks affect all carriers the same way. For example, T-Mobile has not yet been – to its knowledge – the victim of a concerted Denial of Service (DoS) attack. A DoS attack on the website T-Mobile.com, although disruptive, would not necessarily affect T-Mobile's network service to consumers. And not all unusual events are cyberattacks. Certain television shows, such as *American Idol*, can cause unusual spikes in network traffic from text messages and calls, yet are benign.<sup>34</sup> In addition, website- and value-added service-related concerns are different from network service-related concerns, and require different security measures and protections. The Commission also should carefully distinguish between cybersecurity events and network outage events. To the

---

<sup>33</sup> Press Release, U.S. Department of Homeland Security, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center* (Oct. 30, 2009), (NCCIC “provides an integrated incident response facility to mitigate risks that could disrupt or degrade critical information technology functions and services,” combining the U.S. Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications) [http://www.dhs.gov/ynews/releases/pr\\_1256914923094.shtm](http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm).

<sup>34</sup> *FCC Cybersecurity Workshop* at 19-20 (Nagengast comments).

extent that other Government agencies are focused on cybersecurity, the FCC should defer to those agencies and not impose reporting of cyber events to the FCC in the same manner that network outages are reported via the Part 4 NORS reporting framework.

Given the varied security needs and requirements of different service providers, T-Mobile believes that one of the best venues for addressing cybersecurity may be the upcoming CSRIC advisory committee proceedings.

#### V. IMPLEMENTATION OF WIRELESS EMERGENCY ALERTS IS WELL UNDERWAY

As noted above, T-Mobile has filed a letter of intent to transmit CMAS alerts “in whole or in part.”<sup>35</sup> T-Mobile has been a consistent and committed supporter of wireless service programs designed to advance public safety. For example, T-Mobile offers Wireless Priority Service, which provides government agencies with access to wireless services in times of emergency. T-Mobile also was an active participant in the National Capital Region Digital Emergency Alert System, a FEMA pilot program using digital television broadcast spectrum for wireless alerting. In addition, T-Mobile participates in the Wireless AMBER Alerts Initiative, a voluntary partnership between the wireless industry, the Department of Justice and the National Center for Missing and Exploited Children. T-Mobile encourages subscribers to enroll in this initiative to receive AMBER alerts, which are sent free of charge. And, with regard to wireless emergency alerts, T-Mobile actively engaged in the CMSAAC’s work, under the WARN Act,<sup>36</sup> in developing the “System-Critical Recommendations” for the deployment of an alert system by commercial mobile service providers.

---

<sup>35</sup> Letter from Kathleen O’Brien Ham, T-Mobile, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 08-146 (Sept. 8, 2008).

<sup>36</sup> See *supra* note **Error! Bookmark not defined.****Error! Bookmark not defined..**

The end result of CMSAAC's year-long consultation process is a complex, balanced set of proposals that fully satisfies the requirements of the WARN Act and the Commission's goal of creating a CMAS that is workable, realistic, and truly usable for consumers, providers, and public safety agencies in the foreseeable future. All providers, regardless of their transmission standards, should be able to provide CMAS alerts under the CMSAAC's proposed protocols and guidelines. These requirements were designed carefully to avoid imposing any obligation that would favor one technology over another. Once the standards are issued, carriers likely could begin testing CMAS technologies by 2010.

In a similar vein, CMSAAC concluded that incorporating additional technology into mobile devices is unnecessary for a CMAS system. The Committee, which included broadcaster representation, considered amendments relating to proposals for technology such as FM chipsets and DVB-H. The Committee concluded that these technologies are not part of the CMAS architecture.<sup>37</sup> FM chips in particular raised feasibility concerns because of their drain on handset batteries, inability to receive FM alerts when the FM receiver is turned off (which would occur the majority of time given antenna issues), imprecise geo-targeting, and cost.<sup>38</sup> The

---

<sup>37</sup> See, e.g., *Commercial Mobile Service Alert Advisory Committee Meeting 95-114* (Oct. 3, 2007), <http://www.fcc.gov/pshs/docs/advisory/cmsaac/pdf/meeting-transcript100307.pdf>. Although some parties expressed support for an FM chipset solution, "[t]he CMSAAC ... considered the costs and benefits of Radio Broadcast Data System (RBDS) and other FM-based alert and warning solutions, and found them to be infeasible for the CMAS." *In re The Commercial Mobile Alert System*, First Report and Order, PS Docket No. 07-287, 23 FCC Rcd. 6144, 6160 ¶ 37 (2008).

<sup>38</sup> See Letter from CTIA—The Wireless Industry Association® to The Hon. John D. Rockefeller, IV, Chairman, Committee on Commerce, Science & Transportation, The Hon. Kay Bailey Hutchison, Ranking Member, Committee on Commerce, Science & Transportation, The Hon. Rick Boucher, Chairman, Subcommittee on Communications Technology and the Internet, Committee on Energy & Commerce and the Hon. Cliff Stearns, Ranking Member, Subcommittee on Communication Technology and the Internet Committee on Energy and Commerce (June 10, 2009).

CMSAAC likewise balanced the notice requirements with a respect for the flexibility carriers need to determine the unique details of the carrier-customer relationship,<sup>39</sup> and the needs of the disabled and the elderly and other special needs individuals with the technological limitations of the service and end-user equipment. And finally, the Committee considered the methods through which CMRS providers could receive alert messages from government agencies, while mitigating any potential burdens on the agencies and carriers. T-Mobile actively participated in CMSAAC's process and supports its recommendations regarding the complex, highly technical issues underlying the deployment of a new and – by statute – voluntary CMAS regime.

T-Mobile also has met with FEMA regarding emergency preparedness and CMAS standards. The industry will begin testing and deployment once FEMA issues final CMAS specifications, which are expected to be released in the near future. T-Mobile has expressed its intention to participate in this voluntary effort under the standards recommended by CMSAAC and the CMAS regulations adopted by the Commission at the time the intent letter was filed.<sup>40</sup>

In the interim, T-Mobile has developed a plan for mobile alerting. Using cell-broadcast technology, T-Mobile's program will permit instant alerts of 60 characters or less. Although cell-broadcast is not a broadband technology, it is compatible with 3G handsets, as well as backwards-compatible with EDGE and 2G. Existing cell broadcast technology was not designed to support alerts, and indeed, the capability is not even activated or available in many handsets.<sup>41</sup>

---

<sup>39</sup> CMSAAC determined that voluntary participation in CMAS would be advanced by allowing carriers to set their own deployment schedules and permitting consumers to make the choice concerning whether and when to upgrade to new CMAS-capable handsets. *See* Commercial Mobile Service Alert Advisory Committee, Commercial Mobile Alert Service Architecture and Requirements at 3.1-3.4 (Oct. 12, 2007) ("CMSAAC Recommendations"), attached as Appendix B to *The Commercial Mobile Alert System*, Notice of Proposed Rulemaking, PS Docket No. 07-287, 22 FCC Rcd. 21,975 (2007).

<sup>40</sup> *See supra* note 35.

<sup>41</sup> *See, e.g.*, CMSAAC Recommendations at 7.4, 12.2.

Likewise, SMS is not an ideal technology for supporting an emergency alert system as SMS does not offer real-time delivery support, but instead, operates under a store-and-forward regime.<sup>42</sup>

T-Mobile is committed to serving all its subscribers, including those in need of additional language support and other special needs. As the systems and technologies needed to support alerts for these communities become available, T-Mobile intends to explore these options as they offer opportunities to better serve customers. As a part of the broadband plan, T-Mobile urges the Commission to maintain continuity and certainty in the CMAS process, which is well underway. Since the enactment of the WARN Act, all participants have worked cooperatively to bring this system to where it is today. Changing obligations or requirements at this point will only serve to delay implementation of this important service.

---

<sup>42</sup> See CMSAAC Recommendations 5.2; *see also generally Traynor EAS Report.*

## VI. CONCLUSION

Broadband has the potential to improve communications among public safety/homeland security agencies, as well as communications between public safety agencies and the public. A broadband-interoperable network for public safety is best achieved by using the D Block to generate a dedicated pool of revenues for such a plan. As Next Generation 911 and wireless alerting systems are deployed, other public safety communications benefits will materialize. A comprehensive examination of all these efforts seems useful with particular attention placed on ensuring that any requirements are technically feasible. With respect to cybersecurity, carriers have significant market incentives to manage their networks in a manner that upholds system integrity and should be given the flexibility to do so.

Respectfully submitted,

/s/ Kathleen O'Brien Ham  
Kathleen O'Brien Ham  
Harold Salters  
Jim Nixon  
Shellie Blakeney  
T-MOBILE USA, INC.  
401 Ninth Street, NW Suite 550  
Washington, DC 20005  
(202) 654-5900

Date: November 12, 2009