

Questions for the Record

David S. Turetsky
Federal Communications Commission
Public Safety and Homeland Security Bureau

Before the
Subcommittee on Communications and Technology
U.S. House of Representatives

May 16, 2013

The Honorable Henry Waxman

1. The Public Safety and Spectrum Act requires public safety users to vacate the T-Band in 11 years. First responders in Los Angeles rely heavily on the T-Band and tell me they have no reasonable alternative for voice communications at this time. LA-RICS, a coalition of Los Angeles public safety agencies, recently filed a waiver request with the FCC seeking permission to apply for new voice channels to ensure that first responders in the LA market have the ability to communicate after they are required to vacate the T-band.

I am pleased that the FCC sought comment on the LA-RICS waiver request.

Can you provide an update on the status of that proceeding? More specifically, when do you anticipate that the FCC will make a decision in regard to the LA-RICS waiver request?

The Commission has received comments and reply comments from interested parties in response to the Commission's *Public Notice* on the LA-RICS waiver request. Commission staff also met with LA-RICS representatives on May 8, 2013 to discuss the details of the proposed waiver. In addition, LA-RICS' proposal for use of 700 MHz reserve channels is being addressed in a *Notice of Proposed Rule Making* released on April 1, 2013. Comments in that rulemaking proceeding are due on June 18, 2013, and reply comments on July 18, 2013. Staff is working diligently to complete its review of the record in the proceeding, and is cognizant of LA RICS' need for resolution in a timely manner.

2. As you may be aware, last Congress several Democratic members of this committee wrote Chairman Upton and Chairman Walden to request a hearing on issues related to "superstorm" Sandy. Simply put, communications services failed to perform as needed during and after the storm. We thought it was important to examine the impact of the storm and reliability of communications services, especially in the larger context of our transition to wireless and IP networks.

Although we cannot predict the next disaster, we know that these kinds of events are on the rise. So we need to consider whether we need to take additional steps to prepare our networks for this more common occurrence.

We were pleased that the FCC decided to examine this issue in more detail.

What can you tell us about the FCC's field hearings on this topic? What new information about network reliability and resiliency has come to light as a result of these hearings?"

The Commission convened two field hearings to examine challenges to the nation's communications networks during natural disasters and in other times of crisis. The first, held in New York City and Hoboken New Jersey on February 5, 2013, explored, among other issues, lessons learned from Hurricane Sandy. The second hearing, held at NASA's Ames Research Center in California, built upon information received at the first hearing and examined innovative technologies to improve network resiliency in times of disaster.

Testimony taken during the first hearing emphasized the critical link between the electric grid and telecommunications networks. While this link was previously recognized, the event dramatically underscored its importance. A substantial portion of telecommunications network outages were due to the widespread power outages caused by the storm. Additional testimony demonstrated the critical role that broadcasters play in ensuring the dissemination of information to the public during such events, the growing role of social media in enhancing communications during such events, and an interest in obtaining further information about outages of service providers' wireless networks in disasters.

The Commission is evaluating what additional steps may be appropriate in light of the issues discussed in the hearings. The Commission has an open proceeding regarding network reliability and resiliency (*see Reliability and Continuity of Communications Networks, Including Broadband Technologies, Notice of Inquiry, 26 FCC Rcd 5614 (2011)*). The transcripts from both hearings have been placed in the record of that proceeding.

The Honorable John Dingell

1. What percentage of calls to E911 emergency dispatchers are made using wireless devices?

While the Commission does not track the information requested, we can provide an estimate using publicly available data. According to the National Emergency Number Association (NENA), an estimated 240 million calls are made to 9-1-1 in the U.S. each year.¹ CTIA – The Wireless Association estimates that approximately 400,000 E911 calls were placed per day by wireless devices during the month of December 2012.² Extrapolating the CTIA data - approximately 146 million wireless calls were made to 9-1-1 in 2012. Therefore, an estimated 61 percent of calls to 9-1-1 are originating from wireless devices.

2. Does GPS allow E911 dispatchers to locate wireless callers indoors?

¹ National Emergency Number Association, 9-1-1 Statistics, available at <http://www.nena.org/?page=911Statistics>.

² CTIA – The Wireless Association, Wireless Quick Facts, available at <http://www.ctia.org/advocacy/research/index.cfm/aid/10323>.

Generally, the Global Positioning System (GPS) is designed to provide geographic location as measured by a wireless device's latitude and longitude. A GPS receiver in a wireless device relies on line of sight to the constellation of satellites used to determine location of the device. Typically, the effectiveness of GPS is limited indoors because the GPS satellite signal cannot reach handsets inside many buildings. Indoor environments can also dramatically attenuate, or weaken signal strength, of Radio Frequency (RF) transmissions, in particular GPS signals. When wireless customers take their mobile device to an indoor location, the radio signals that the device receives and transmits (both GPS and cellular) are subject to degrading interference, including additional RF attenuation, scattering (diffusion of signal), and multi-path propagation (fading of signal). The extent of signal degradation depends on the nature of the building's construction materials and the layers of construction obstructing the various signal paths. Consequently, indoor environments, such as office buildings and complexes, condominiums and apartment buildings, college dorms or hotel rooms, present significantly more challenging circumstances than outdoor environments for wireless carriers attempting to generate accurate location estimates of 9-1-1 calls made by their customers.

3. Similarly, are the FCC's location accuracy standards for Phase II of E911 applicable to indoor environments?

Generally, the FCC's Phase II location accuracy standards are not applicable to indoor environments. In September 2010, the Commission adopted new rules requiring CMRS wireless carriers to provide more specific automatic location information to 9-1-1 call centers in areas where they had not done so in the past. In doing so, the Commission recognized the impediments that wireless carriers face in transmitting location information for indoor 9-1-1 calls. Specifically, because indoor use poses unique obstacles to both handset-based and network-based location technologies, the Commission clarified that the amended location accuracy standards for CMRS wireless carriers apply to outdoor measurements only.

4. NextNav/Progeny are currently awaiting FCC approval before they can begin providing indoor position location services to support emergency first responders. When does the Commission expect to grant or deny NextNav/Progeny's request?

Under our rules, NextNav/Progeny (Progeny) must demonstrate that its use of spectrum within the Part 15 band would not cause unacceptable levels of interference to other Part 15 spectrum users. An order addressing Progeny's request has been placed on circulation and is currently awaiting decision by the Commissioners.

5. Additionally, please describe the approval process for NextNav/Progeny's request?

On March 10, 2011, the Wireless Telecommunications Bureau (WTB) released a public notice seeking comment on a request by Progeny seeking waiver of certain of the Commission's rules relating to Multilateration Location and Monitoring Service (M-LMS). On December 20, 2011, the WTB and Office of Engineering and Technology jointly adopted an order granting a waiver to Progeny conditioned on Progeny conducting field testing prior to commercial operation of its network sufficient to demonstrate that it does not cause unacceptable levels of interference to other Part 15 users of the spectrum. On January 27, 2012, Progeny submitted test results in support of its claims that its network does not cause unacceptable levels of interference to Part 15 devices. Following Progeny's submission of test results, on February 14, 2012, WTB and

OET released a *Public Notice* seeking comment on Progeny's field testing report. At the request of the Commission, Progeny conducted additional testing on a joint basis with three Part 15 spectrum users and filed three test reports with the Commission. On November 20, 2012, WTB and OET placed the second set of test results on public notice. The comment period ended on January 11, 2013. Recently an order addressing Progeny's request has been placed on circulation and is currently awaiting decision by the Commissioners.

The Honorable Mike Doyle

1. According to the National Broadband Plan wireless backhaul is "critical to the deployment of wireless broadband and other wireless services," particularly "[w]hen fiber is not proximate to a cell site." I understand that the existing wireless backhaul networks face a number of regulatory and technological constraints that limit their potential capacity. These independently-powerable backhaul services are important to undergird FirstNet, the national first responder network.

How did public safety and mobile networks perform during natural events, like Hurricane Sandy, and man-made events, like 9/11?

During Hurricane Sandy 9-1-1 communications performed remarkably well. Although calls to many 9-1-1- Call Centers were rerouted to other 9-1-1 Call Centers, there were almost no instances where it was impossible for a Call Center to receive a 9-1-1 call. Most land mobile radio public safety systems worked well. Commercial wireless networks were affected by loss of commercial power at the cell towers and loss of backhaul from the cell towers to the Mobile Switching Centers. Approximately 25 percent of cell sites within a 164-county area (across 10 states and Washington, D.C.,) were out of service. In the hardest hit areas like New Jersey, the percentage of cell site outages was considerably higher and more than double in some counties.

2. Can public safety networks and mobile networks work without backhaul?

Mobile communications use backhaul to access the network for handling user traffic to reach the Internet or other users on the same or different networks, e.g., the Public Switched Telephone Network, as well as signaling traffic needed to authenticate, control and manage the call. We are not aware of any deployments for mobile cellular networks that deviate from this principle. Standards-setting bodies are working to provide near proximity direct device- to- device communication without transporting user data over the backhaul to the network; however, these capabilities are not available currently.

Generally, when backhaul of some kind is not available, calls cannot get through. There are two ways to fix this problem: 1) repair the backhaul or 2) set-up alternate backhaul arrangements. It is always preferable to repair the backhaul as long as the repairs can be done in a reasonable time. This is what most of the carriers did as a result of damage from Hurricane Sandy.

Current public safety network deployments are based on narrowband LMR (Land Mobile Radio) technologies. These networks, while local or regional in nature, also use backhaul connections

to expand the reach of the network. LMR user devices also support direct communication (also known as talk around) which allows users to communicate directly without any use of the network or backhaul in a limited area.

3. If the FCC ultimately reclaims spectrum in the 24 and 39 GHz range, how long will it take, including the necessary legal proceedings, for a new wireless backhaul provider to build-out a backhaul service with the seized spectrum?

The Commission recognizes the importance of freeing up additional spectrum to support the growing demand for wireless services, including the backhaul services that constitute a critical element of our nation's wireless infrastructure. At this time the Commission has not initiated any proceeding to reclaim spectrum in either of these bands. Nor has the Commission initiated any proceedings seeking information on the timetable for building out in these bands in the circumstances you address.

The Honorable Ben Ray Lujan

1. The danger of cyber threats to our emergency networks could cripple the ability of our responders to react to an emergency and bring additional harm. In your written testimony, you describe the FCC's efforts to work with communications providers to develop voluntary cybersecurity measures and best practices as well as educate shareholders on threats. My district is home to Los Alamos National Laboratory, which provides some of our nation's leading work on supercomputing and cybersecurity. Has the FCC considered consulting with the lab on these cyber threats?

At the Commission, we are very interested in consulting with leading experts in the field of cybersecurity in an effort to improve the availability, reliability, and resiliency of our nation's communications networks. We are aware of Los Alamos National Laboratory's focus on national security threats to the nation's cyber infrastructure. We are aware of the lab's research and papers regarding the development of innovative technologies for detection, response, and predictive vulnerability analysis that can be used by service providers and enterprise networks to defeat today's intrusions into both government and critical infrastructure systems as well as to predict and prepare for potential attacks in times of conflict.

At the Commission, our cybersecurity focus has been concentrated on reducing the public communications infrastructure vulnerabilities associated with domain name fraud, Internet route hijacking, and botnets. We do plan to reach out and consult with the National Laboratories that responded to the recent NIST Request for Information concerning the development of a framework to improve critical cybersecurity infrastructure as part of the Department of Homeland Security consultative process.

We look forward to other opportunities of mutual benefit to engage the National Labs and seek their expert advice regarding cybersecurity threats to the nations' public networks, and recommendations for improving the resilience of the networks to these threats.

