Written Statement
of

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

"Oversight of the First Responder Network Authority (FirstNet) and Emergency Communications."

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

Thursday, March 14, 2013

Good afternoon, Chairman Walden, Vice Chairman Latta, Ranking Member Eshoo and Members of the Subcommittee. Thank you for the opportunity to appear before you to discuss the Federal Communications Commission's (FCC's) efforts to strengthen the connectivity, reliability, and resiliency of our nation's critical communications facilities.

INTRODUCTION

The safety of our communities requires effective communications tools. I will address four relevant areas: ensuring the reliability and resiliency of critical communications networks, particularly the 9-1-1 system, through natural or man-made disasters; modernizing the capabilities and increasing the resiliency of our 9-1-1 system through the use of "next generation" technology, or NG911; enhancing our emergency alert and warning systems; and securing our cyber environment.

I. RELIABILITY OF CRITICAL NETWORKS

The severe weather events that affected diverse regions of the United States in the past year underscore the need to promote and ensure the reliability and resiliency of our nation's critical communications facilities. The Commission is very focused on those needs.

Here are two examples.

First, in June, a fast-moving weather storm called a derecho arrived unexpectedly and caused billions of dollars of physical damage and 22 deaths, affecting wide swaths of the United States, beginning in the Midwest and continuing through the Mid-Atlantic and Northeastern regions. Millions of Americans lost electrical power during the accompanying heat wave and the networks of service providers that serve 9-1-1 facilities were severely disrupted, from isolated breakdowns in Ohio, New Jersey, Maryland and Indiana, to systemic failures in northern Virginia and West Virginia. Seventeen 9-1-1 call centers (or "PSAPS") in three states lost service completely, affecting the ability of more than 2 million people to reach 9-1-1 at all. Seventy-seven PSAPS serving more than 3.6 million people in 6 states lost some degree of connectivity, such as vital information on the location of 9-1-1 calls.

At the direction of FCC Chairman Julius Genachowski, the Public Safety and Homeland Security Bureau (Bureau) conducted an extensive inquiry into the causes of the communications failures relating to the derecho and ways to prevent them from occurring in the future. The Bureau found that above and beyond any physical destruction from the derecho, 9-1-1 communications were disrupted in large part because of avoidable carrier planning and system failures, including the lack of functional backup power, notably in central offices. [1] Monitoring systems also failed, depriving communications providers of visibility into critical network functions. [2] In most cases, the 9-1-1 and other problems could and would have been avoided if providers had

[1] "Impact of the June 2012 Derecho on Communications Networks and Services: Report and Recommendations" (*Derecho Report*) at 1, 40-41.

[2] *Id.* at 40-41.

followed industry best practices and available guidance. Although the Bureau had previously issued public notices highlighting some of these best practices and reminding carriers of the importance of implementing them, such reminders apparently had little effect.

Next week, the Commission is planning to consider a Notice of Proposed Rulemaking focused on the areas that the Derecho Report recommended for Commission action to promote the reliability, resiliency, and availability of 9-1-1 communications networks. The Commission will consider proposals aimed at ensuring that service providers: conduct periodic audits of 9-1-1 circuits; maintain adequate backup power at central offices and follow regular maintenance and testing procedures; have adequate network monitoring links; and have a more specific obligation to notify 9-1-1 call centers of breakdowns of 9-1-1 communications. Even in the context of a storm like last summer's derecho, a large-scale failure of communications—particularly 9-1-1 communications—is unacceptable and we must act to prevent similar outages in the future. To quote Chairman Genachowski: "Here's the bottom line: We can't prevent disasters from happening, but we can work relentlessly to make sure Americans can connect with emergency responders when they need to most."[3]

Second, in October, Superstorm Sandy devastated significant portions of the northeastern United States, causing 146 deaths and billions of dollars of physical damage along the Eastern Seaboard. Unlike the derecho, Sandy's arrival on the shores of the continental United States was anticipated and predicted with considerable accuracy, which gave communications providers time to prepare, and implement emergency plans. Nevertheless, Sandy's destructive effect on the communications infrastructure was still dramatic. Again, millions lost electrical power and communications networks were severely impacted. This time, however, most of the impact was not on 9-1-1 call centers, but on the communications networks that the public relies on to communicate with one another and to secure help in emergencies. For example, about 25 percent of mobile antenna sites in the Sandy-affected region, which encompassed all or part of 10 states and the District of Columbia went out of service. In hard hit New Jersey and parts of New York, however, the percentages were much higher. The most common causes were backhaul issues or loss of power to antennas.

Commission staff worked around the clock, including through our 24-hour operations center, to try to assist communications companies in meeting the considerable challenges they faced in maintaining and restoring communications services in the wake of Superstorm Sandy. We issued emergency authorizations that enabled out-of-town utility companies to use their communications frequencies and tools during restoration activities in the stricken areas. We worked with our governmental partners to facilitate fuel delivery to wireless providers so that they could refuel generators and undertake repairs. We worked with broadcasters, issuing temporary authorizations to increase their

[3] *See* News Release, FCC Chairman Genachowski Announces Action to Strengthen Reliability and Resiliency of 9-1-1 Communications Networks During Major Disasters (Jan. 10, 2013), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-318333A1.doc.

power in certain areas to help get local news to the public, and urged other governments to allow broadcasters to access their studios and transmitters in hard-hit areas, and to receive fuel preferences for their satellite trucks and generators. We monitored 9-1-1 call centers, worked with cable companies, and kept in touch throughout with communications companies, including calls from our FCC Chairman to their CEOs, to try to identify and help them meet needs that could preserve or hasten restoration of communications to the public. Additionally, at FEMA's request, the FCC sent a vehicle outfitted with mobile network monitoring equipment to measure the mobile signal strength coverage on hard hit areas of Long Island, New York. We also continued our practice, which began during Hurricane Isaac, of keeping in touch with non-English language broadcasters to help ensure that non-English speaking communities would continue to have a source of important local news during times of emergency.

In the wake of Superstorm Sandy, Chairman Genachowski announced that the Commission would hold field hearings to examine challenges to the resiliency of the nation's communications networks and consider next steps.[4] The first hearing, held on February 5, 2013, in New York City and in Hoboken, New Jersey, focused on the severe impact to communications resulting from Superstorm Sandy, the response, and access to information during the storm's aftermath.[5] A second hearing, held just two weeks ago on February 28, 2013, at Moffett Federal Airfield in California, focused on how innovative network technologies, smart power solutions, social media and mobile applications might improve communications network resiliency in times of disaster.[6] The Commission is currently in the process of reviewing and evaluating the presentations and answers to questions provided on the record in the field hearings to date. At the conclusion of the field hearings, the Commission will consider options to address the information gathered and to explore broader issues of network reliability and resiliency that are not part of next week's 9-1-1 Reliability Rulemaking.

While the issues can be complex, the goal of the Commission's work in this area is simple -- use the information and lessons we learn to enhance public safety by helping to make communications more reliable and resilient.

---

[4] *See* News Release, FCC Chairman Genachowski Announces Post-Superstorm Sandy Field Hearings to Examine New Challenges to Resiliency of U.S. Communications Networks During Natural Disasters & Other Times of Crisis (Nov. 21, 2012), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db1121/DOC-317543A1.pdf.

[5] *See* FCC Announces Date and Locations for the First Post-Superstorm Sandy Field Hearing, *Public Notice*, DA 13-19 (Jan. 8, 2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0108/DA-13-19A1.pdf.

[6] *See* FCC Provides Additional Details Regarding the Second National Hearing on Network Resiliency and Reliability, *Public Notice*, (Feb. 27, 2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0227/DOC-319159A1.doc.

II. PROMOTING RELIABLE ACCESS TO 9-1-1 IN THE FUTURE

It is crucial that our existing infrastructure works well, even as we develop plans for enhancing our systems in the future. But as the *Derecho Report* also noted, the migration of "legacy" 9-1-1 systems to Next Generation technology will improve the reliability and performance of 9-1-1 in future major disasters, thus making it important to move forward on Next Generation 9-1-1 (NG 9-1-1).

The transition to NG 9-1-1 will facilitate interoperability and system resilience, improve connections between 9-1-1 call centers, and support not only traditional voice 9-1-1 calls but also the transmission of text, photos, videos, and data. These new capabilities will enhance the accessibility of 9-1-1 to the public, including people with speech and hearing disabilities, and will provide PSAPs with enhanced information that will enable emergency responders to assess and respond to emergencies more quickly and effectively.

A. First Steps: Text-to-9-1-1

Text messaging has become a part of the fabric of modern day life. CTIA reported last year that more than 184 billion texts – that's billions with a "b" – are sent *monthly*. Persons with hearing and speech disabilities are also increasingly turning to text-based applications to stay connected, leaving behind older technologies like TTY in favor of more mainstream and generally accessible formats.

It is natural, therefore, that in an emergency people will increasingly expect to be able to use text as a means of contacting 9-1-1. While voice services are still preferable for reaching 9-1-1, there are times when a voice call may be impossible, inadvisable, or both. First, text may be the only means for a person with a hearing or speech disability to reach out for help. Second, there are times that a voice call may place someone in danger, such as in a live shooter situation or domestic abuse. Third, when voice networks are congested, text messages may have a better chance of getting through. Multiple text messages can also be open at the same time, enabling PSAPs to prioritize life-threatening emergencies and move them to the top of the queue. It is vital, therefore, that even as we consider the longer path to NG 9-1-1, we start by addressing text messaging in the short term.

The Commission has been working diligently with PSAPs, carriers, consumer groups, and other stakeholders to achieve this first step. Beginning several years ago, PSAPs in several states and localities launched text-to-9-1-1 trials with different carriers and vendors, in Black Hawk County, Iowa; the City of Durham, North Carolina; the State of Vermont; and the State of Tennessee. Results of the trials have been encouraging and have brought concrete public safety benefits, for example, a woman who was at risk of domestic abuse texting for help undetected by her assailant; a child reporting instances of domestic abuse; and an anonymous report of imminent sales of controlled substances. In one case in Vermont, a life was saved when emergency personnel were able to thwart an attempted suicide following a text message to 9-1-1. PSAP participants in these trials have generally reported no negative operational impacts on their systems as the result of the trials.

More recently, some jurisdictions have moved beyond trials and have begun live

deployment of text-to-911. One of the first of these is York County, Virginia, where the PSAP has launched text-to-911 with Verizon Wireless.

In December of last year the two major public safety organizations -- the Association of Public Safety Communications Official-International (APCO) and the National Emergency Number Association (NENA) -- and the four major wireless carriers – AT&T, Verizon, Sprint Nextel and T-Mobile, announced a voluntary agreement under which each of the four would provide text-to-9-1-1 service by May 15, 2014, to PSAPs who request such a service. Under the terms of the voluntary agreement, these carriers will also implement an automatic "bounce-back" message capability by June 30, 2013. The bounce back message will alert subscribers attempting to text an emergency message to instead dial 9-1-1 when text-to-9-1-1 is unavailable in that area.

The Commission issued an NPRM in December that builds on this agreement by proposing rules for implementation of text-to-9-1-1 and bounce-back capability that would apply to all wireless carriers and to certain other providers of text services. The NPRM also seeks comment on what the required timeframe should be for carriers and other text providers to develop this capability. We have asked for expedited comment on the bounce-back requirement, and we may act on this issue soon. The record on the remaining text-to-911 questions remains open, and we will be carefully evaluating these issues as the comments come in.

B. Next Steps: The FCC Report to Congress

Beyond text-to-9-1-1, the Commission has also been working to encourage the evolution of the nation's emergency response networks to an NG 9-1-1 platform. Last month, as directed by the Next Generation 9-1-1 Advancement Act of 2012, the Commission submitted to Congress a report with recommendations on how to address legal and regulatory barriers to this transition. I'd like to take a moment to highlight just a few of the report's findings and recommendations.

The 9-1-1 system has traditionally been managed at the state and local level, and the transition to NG 9-1-1 will necessarily also happen at this level. We also believe, however, that the federal government and Congress in particular, can play a key role in assisting these efforts. In this respect, the report's lead recommendation is for Congress to create incentives for states to become "early adopters" of NG 9-1-1. This will accelerate the NG 9-1-1 transition in these states while also generating valuable experience with NG 9-1-1 implementation that other states can follow. We also recommend that Congress encourage states to establish or empower state 9-1-1 boards or similar state-level governance entities to provide technical and operational expertise. The report also recommends that Congress consider creating a federal regulatory "backstop" to ensure that there is no gap between federal and state authority over NG 9-1-1. These policies would also promote consistency, efficiency and interoperability.

In addition, the report recommends that Congress promote a consistent nationwide approach to key elements of NG 9-1-1 deployment, including standards that support seamless communication among PSAPs and between PSAPs and emergency responders; support reforms to the NG 9-1-1 funding structure; encourage states to adopt appropriate liability protection; and provisions to make NG 9-1-1 fully accessible to people with disabilities. The report recommends that Congress promote the development

of location technologies that will support all NG 9-1-1 applications regardless of the network or device used by the caller. We also recommend that Congress support establishment at the national level of certain databases that support NG 9-1-1 routing and security.

Finally, the report identifies areas where Congress could assist in the elimination of legacy state regulations that are impeding NG 9-1-1 deployment, while providing incentives for states to modernize their laws and regulations to accommodate NG 9-1-1. These reforms would enable service providers to support an expanded array of NG 9-1-1 services and applications, and facilitate a more flexible and resilient network architecture.

Lastly, I would like to briefly address the importance of NG 9-1-1 in relationship to the network to be built by FirstNet. The evolution of the 9-1-1 system to support next generation technologies is a necessary corollary to the FirstNet network, because next generation PSAPs can serve as a hub for data that comes in from 9-1-1 callers, telematics providers, and others, which the PSAP may then disseminate to first responders using the FirstNet network. So when a PSAP receives video of an accident from a witness sending it to 9-1-1, it can send it to the response personnel who need the information quickly and seamlessly. It is imperative that we lay the foundation for these data-rich opportunities.

III. PUBLIC ALERTS AND WARNINGS

Emergency alerts are different than 9-1-1, but are very important to public safety. While calling 9-1-1 is about the public reaching first responders during an emergency, alerting enables the government to provide life-saving information quickly to the public.

A. Wireless Emergency Alerts (WEA)

Wireless Emergency Alerts, or WEA, is a system that allows the public to receive geographically targeted alerts about imminent threats to life and property over cell phones and other mobile devices. Launched in April 2012, WEA allows mobile devices to receive emergency alerts in the area where the emergency is happening, irrespective of which carrier an individual may use or where that person's primary number is located. The alerts are intended to reach the right people, at the right time, with the right messages. A WEA alert consists of a short message that is accompanied by a unique attention signal and vibration, which helps people with hearing and vision-related disabilities recognize the alert, and there is no charge to consumers for receiving these alerts.

Developing WEA has been a team effort. The cooperation of the wireless industry has made the WEA, a voluntary system, into a potent force for public safety. CTIA in particular has been a close collaborator on WEA (formerly known as the Commercial Mobile Alert System) since Congress passed the Warning, Alert and Response Network (WARN) Act in 2006. The wireless industry continues to work with us and other federal agencies, such as FEMA and the National Weather Service, as WEA is fast becoming the leading edge of the Integrated Public Alert and Warning System (IPAWS).

In the less than one year that WEA has existed, it has often provided fast, targeted alerts to people in danger in a manner that gets their attention and directs them to life and property saving action. For example, during the July 2012 derecho, a tornado touched down in Elmira, New York - an area not known for tornadoes. A man packing his car heard the alert and got his family to safety just in time. Similarly, last month in Mississippi, a woman told the National Weather Service that she was about to go to bed when she received a WEA alert on her cell phone warning her of an imminent tornado. She went out her back door and discovered a tornado backlit by lightning moving towards her. She ran back into the house, got her daughter and husband into the bathtub, and within moments, the tornado struck their brick house, heavily damaging the bedroom where she and her husband would have been in bed.

WEA success stories are not limited to tornadoes. In December 2012, the National Center for Missing and Exploited Children began to issue AMBER alerts over WEA. Within weeks of the AMBER WEA launch, a child abduction Amber Alert was issued in the Minneapolis/St. Paul area, and was heard by a teenager who recognized the car described in the alert and called 9-1-1. The police arrived just as the abductor was dyeing the child's hair in preparation for flight out of the state. It is not an exaggeration to say that but for the WEA alert, that child may not have been recovered.

As with all new technologies, there is a shake out period. With WEA, we and other stakeholders are working to improve the specificity of alert targeting, understanding of when to use the system, and to increase the number of WEA-capable handsets. But as the examples I just gave indicate, WEA has already made a real difference.

B. The Emergency Alert System

Just as wireless providers form the backbone of the WEA, broadcasters form the backbone of the Emergency Alert System, or EAS. The cooperation of The National Association of Broadcasters (NAB) and other broadcaster organizations has been essential to the continued modernization of the EAS, and was vital to the success of the first Nationwide EAS Test.

1. CAP Adoption.

For over 50 years, what we now call the EAS has provided emergency alerts to the public, and has ensured the ability of the President of the United States to deliver a message to the public in the event of a national emergency. The FCC, FEMA, and the National Weather Service are charged with maintaining the EAS, and FCC rules require broadcasters, satellite radio and television service providers, cable systems, and wireline video systems (EAS Participants) to install and operate equipment capable of delivering EAS alerts to their viewers and listeners.

The EAS remains the nation's primary alerting system. To ensure its continued relevance, diversify its operation, and enhance its reliability, we are engaged with our federal partners in two major initiatives. First, we have modernized and diversified the

EAS by requiring EAS Participants to also provide a broadband-based distribution architecture. Second, in close collaboration with FEMA, we have taken a series of steps, including a national test, to improve the reliability of the legacy, broadcast-based EAS.

A key step toward modernizing the EAS was taken last year with the requirement that EAS Participants be able to receive alerts using the Common Alerting Protocol (CAP). CAP is a powerful tool that is rapidly becoming the world-wide standard for alert distribution. It is an Internet-based language that allows alert initiators, such as the National Weather Service and state and local alert initiators, to use FEMA's IPAWS to deliver alerts simultaneously over multiple media, including radio, television and wireless devices, and will ultimately allow better service to the deaf and hard of hearing community and those whose primary language is not English. Using CAP has another benefit to the EAS in that it compresses the EAS distribution architecture from the complicated, broadcast-based "daisy chain" I will describe in more detail later to a simple "one to many" architecture that has many fewer single points of failure.

2. Legacy EAS Improvement and Nationwide EAS Test.

The EAS was designed to enable the President to deliver a nationwide live broadcast message after a catastrophic event, when access to electrical power and communications systems may be significantly degraded and when few if any other communications pathways may exist other than battery-powered radios and televisions. The EAS architecture was thus designed to deliver a live audio feed from the President, delivered over a secure line (provided by FEMA) to the Primary Entry Point (PEP) radio stations, a select group of geographically distributed, independently powered and electromagnetic pulse (EMP) hardened radio stations that collectively can reach over 90 percent of the American populace. The PEPs would then broadcast the alert to other EAS Participants, which would receive and, in turn, transmit the alert via the hierarchical broadcast-based EAS distribution system to the public across the U.S.

Although the EAS was tested weekly and monthly on a local and statewide basis, prior to 2011, the national distribution architecture for a Presidential alert had never been tested -- a fact inconsistent with America's need for a back-up, fail-safe alerting system. Accordingly, the Commission, in coordination with FEMA, the NWS, and the Executive Office of the President, scheduled the first Nationwide Test of the EAS for November 9, 2011 at 2 p.m. Eastern Standard Time.

Because the system had never previously been tested nationally, we expected issues would arise. Our key goal was to identify problems and address them to ensure that the system would perform as designed. The Nationwide EAS Test was designed to test the links in the distribution architecture, and the test successfully showed that this architecture was viable. As the alert propagated nationally, the vast majority of EAS Participants were able to receive the alert and, where necessary, transmit it to other EAS Participants. However, the test also revealed a number of problems related to the reception and transmission of the Emergency Action Notification, the code used to activate the National EAS, by EAS Participants. The primary problem was a

transmission anomaly caused by a feedback loop at the initial distribution to the PEPs, a lack of PEP stations at various parts of the country, among which was Oregon, and poor audio quality at various points in the system.

Since the test, the FCC and FEMA have been analyzing these problems and both planning and executing their remediation. First, FEMA has explored alternative alert transmission technologies for the FEMA/PEP connection and plans to introduce satellite conductivity to back up the Public Switched Telephone Network-based connection that FEMA currently uses to send the EAN to the PEPs. Second, FEMA continues to expand the PEP system from the 63 PEPs in operation at the time of the test to a total of 77 by 2015. We understand that FEMA has already completed construction of a number of these additional PEP stations, including PEPs in Portland and Eugene, Oregon. The FCC is monitoring the effectiveness of these improvements through its weekly and monthly EAS testing regime, as well as by reviewing State EAS Plans to ensure that all EAS Participants have available up-to-date and accurate information about what stations they are to monitor in order to receive an audible and decipherable EAS alert.

Under FCC rules, EAS Participants had until December 27, 2011 to submit their test results to the FCC. On coordination with FEMA, we are analyzing this data to determine what worked and what did not, and to make recommendations for improvements as necessary. In the meantime, we are working with FEMA and EAS Participants to learn more about problems that have already been identified and what actions we should take to address them.

C. Next Steps for Emergency Alerting

Looking to the future, the FCC will continue to work closely with FEMA, the National Weather Service, industry, and state and local governments to ensure that the public has access to emergency alerts and warnings over multiple communications technologies. Those efforts will include, of course, our continued work to ensure that the benefits of WEA and EAS are available to consumers in all parts of the country and to ensure that the EAS continues to provide a reliable and effective method to transmit timely and accurate emergency alerts to the public.

IV. CYBERSECURITY

Internet security, or cybersecurity, presents a real and constant challenge to everyone from the casual broadband user to the very core of our nation's critical infrastructure. The world depends on the security of broadband communications infrastructure for commerce and to move vast amounts of data that enable the functioning of industries such as banking and energy. Government also depends on the reliability and security of broadband networks.

The Internet contains built-in vulnerabilities that were mostly absent in legacy circuit-switched networks. The openness of the Internet makes it more vulnerable to certain types of exploits, and specific areas of risk exist in Internet routing and domain name systems. Furthermore, users are exposed to torrents of malware and spam, making

them vulnerable to infection and setting them up as threats to other users and, in extreme scenarios, the communications infrastructure itself.

The Commission has played, and will continue to play, a vital role to promote the nation's communications reliability and resiliency against cyber threats. At the FCC, we are able to work productively with communications providers in a public-private partnership to develop voluntary measures and best practices, and educate stakeholders on threats. We then seek to measure the extent to which these best practices are having the desired result.

The Commission has also been an advocate and educator for consumers and small businesses to help them understand the simple proactive measures that they can take to combat cyber threats. The Commission has, with the aid of the Communications Security, Reliability and Interoperability Council, and in collaboration with the industry and our government partners, developed tools available on our website to promote mobile security, like our tip sheets for international travelers and our "Small Biz Cyber Planner" i.e., for small businesses.

That cybersecurity is a challenge was amply evident in the recent "zombie apocalypse" alert issued over hacked EAS equipment, which we believe could have been largely avoided if the factory passwords on EAS equipment had been changed and adequate security protocols followed.

The Commission has worked to promote cybersecurity through its work with CSRIC. This month, the third iteration of this group will be wrapping its work in the area of domain name system security, botnet remediation, and secure routing, where it has made recommendations to the Commission.

It is essential that the Commission partner with other government entities and the private sector to develop best practices that address new technologies such as cloud computing and distributed authentication, on which the resiliency and reliability of the new communications infrastructure rely.

We are also committed to executing our responsibilities under the Executive Order and the Presidential Policy Directive, as well as any legislation Congress may pass, and to working with our partners and industry to develop and implement best practices more broadly in promoting the security and resilience of critical communications infrastructure on which the Nation depends.

I thank you for your time and the opportunity to testify before you today, and am pleased to answer any questions you may have.