NENA Goes to Washington

Monday, February 23, 2015

Remarks of Rear Admiral (ret.) David Simpson,

Chief of the Public Safety and Homeland Security Bureau

-As Prepared for Delivery-

Trey, thank you for that introduction. Thanks also to NENA President Christy Williams, and to everyone here in the audience joining us here on this cold Monday.

I want to talk with you today about what we've been doing at the FCC on 911 issues – about the important work we've done since I spoke with you all last year, and about the exciting things on the horizon for us. It is always an honor to speak to NENA members, the men and women on the front lines of providing emergency response services to the American public. The work you do every day inspires the work that we do at the Bureau and the Commission, and we are so appreciative of your service. On any given day, at any given moment, we know that you – the nation's first responders – must be prepared to handle emergencies of any kind. You do it with courage, working through every challenge thrown your way. But one thing we know to be true is that no matter the size or severity of the emergency, having effective and reliable communication tools is critical for you to be able to do your job.

As consumer habits continue to change and communications networks increasingly migrate to newer technologies, we at the Commission are committed to making sure that access to critical lifesaving services, most notably 911 services, are preserved for all Americans, and where possible, improved. We are committed to finding ways to leverage existing resources for Next Generation 911 and to developing tools for PSAPs to use to ease the transition to IP-based

networks. It is true that these next generation networks will be more complex and raise certain challenges that did not exist in legacy networks, such as cybersecurity, but these are challenges we can overcome together. Our job at the Commission is not to force new technology on you but to make sure that new technology works to serve **you** and the critical public safety functions you perform.

With that, I'd like to talk a bit about what we've been doing at the Commission, focusing on text-to-911; 911 location accuracy; 911 reliability; the task force on optimal PSAP architecture, and finally, cybersecurity.

Text-to-911

First, we have made significant progress on text-to-911 over the course of the past year. You here in this room know better than anyone else why text-to-911 is so important. For the tens of millions of Americans with a hearing or speech disability, not being able to text to 911 significantly constrains their ability to get help. Moreover, text-to-911 can provide all Americans with a critical means of contacting 911 when a voice call may place someone in danger, such as an active shooter or domestic abuse situation.

When I spoke to you at 911 Goes to Washington a year ago, the Commission had recently issued its Policy Statement and Notice of Proposed Rulemaking, which proposed rules to further the implementation of text-to-911. In August 2014, the Commission acted on those proposals. In its Text-to-911 Order, the Commission required CMRS providers and interconnected text providers to be "text-capable" by December 31 2014 and to begin delivering 911 text messages to requesting PSAPs by June 30, 2015, or six months from the date of each request to begin delivering 911 texts to that PSAP.

The text-to-911 rules provide PSAPs with certainty that "the table is set" for text-to-911 on the service provider side. Now, more than ever, the time is ripe to move forward expeditiously to plan your implementations.

Text-to-911 has proven itself as an important medium for reaching emergency services in times of need, and in some cases, preventing bad situations from becoming tragic. Burglaries in progress and potential domestic abuse situations have been interrupted because a person in distress was able to silently communicate with a 911 call center when a voice call would have compromised their situation even more.

Such stories are possible because of the cooperation of PSAPs and wireless carriers to make text-to-911 service a reality. And there will be more of these success stories because since we adopted rules in August, the number of PSAPs requesting text-to-911 has grown significantly. Today more than 200 PSAPs in 19 states are accepting 911 text messages from the four nationwide providers, including throughout Vermont, New Hampshire, Maine, and most of Indiana. The Greater Harris County, Texas Council of Governments supports text across more than 40 PSAPs. Text-to-911 technology vendors are working with several hundred more PSAPs to prepare them to accept text-to-911 in the near future. The National Capital Region is moving forward with a multistate deployment of text-to-911 and will provide a model to other regions on how multiple jurisdictions can take advantage of shared infrastructure to augment their emergency response capabilities. Massachusetts is implementing a state-wide NG911 system and is on the cusp of introducing text-to-911. South Dakota just executed an agreement with a major vendor for statewide implementation of text-to-911.

As for those PSAPs that don't believe they are ready to implement text-to-911 service into their current operations: I encourage you to look to your colleagues and their success stories as proof of the life-saving capabilities of text-to-911. We have the regulatory tools in place, the carriers are required to do their part, and the public increasingly expects 911 to include text capability. Around the country, PSAPs are stepping up to do their part – it is time to join them. For anyone seeking guidance, NENA has done great work providing best practices and guidance on how to work with vendors and wireless carriers to become text-capable. Following NENA's lead, the Public Safety Bureau has a web page dedicated to Best Practices for Implementation of Text-to-911. Once you are technically capable of handling texts, notify the Commission by filling out the Text-to-911 Readiness and Certification form for your facilities. That will serve as a one-time, single point of notification to all covered providers that your facility is accepting texts and you are ready to begin the coordination process.

Text-to-911 gives us an unprecedented opportunity to implement, evaluate, and monitor a Next Generation 911 service in the near term, which will provide valuable insight as we begin implementing other NG911 functionalities.

Location Accuracy

Let me turn now to location accuracy. When you came to Washington a year ago, the Commission had just adopted its Further Notice of Proposed Rulemaking on improving wireless indoor location accuracy. I told you then that addressing this issue was a Commission priority, and that we all had "a lot more work to do to ensure that PSAPs receive the kind of timely, reliable, and dispatchable location information that they need and that the public expects."

Just last month, the Commission took a milestone step towards achieving that goal. I want to talk a little bit about the specifics of the Commission's location accuracy order, and you will hear more about it tomorrow from David Furth and Tim May. But before I get into the details, I want to extend a huge "thank you" to NENA and its individual chapters and members for all that you have contributed to this proceeding. When the Commission issued its notice last year, we encouraged NENA and other stakeholders to work together to bring us new ideas for how to address the indoor location issue. NENA answered this call, working with APCO and the four largest wireless carriers to negotiate the Roadmap agreement. The Roadmap is the product of months of hard work and strenuous negotiation by NENA's leadership. It has introduced game-changing elements that the Commission has incorporated into its final order. The Roadmap elements, combined with the provisions that the Commission added to "toughen" the Roadmap and make it more comprehensive, have resulted in final rules that I firmly believe improve on our original proposal and will drive rapid, measurable improvement in indoor location accuracy.

I don't need to tell you why indoor location is important: 44 percent of all U.S. households rely solely on wireless, and reliance on wireless is significantly greater among young adults and those living at or near the poverty line. It is estimated that about 70 percent of 911 calls come from wireless phones, and more than half of all calls made to 911 likely originate indoors, meaning that this 911 location accuracy gap is not a theoretical or future crisis; it is an issue **now**.

The order the Commission adopted last month puts us on track to close that gap. It sets clear benchmarks and codifies key elements of the Roadmap. Equally important, we have crafted the order to give PSAPs a direct, participatory role in driving this implementation, in

monitoring carrier compliance through data analysis, and in ensuring that the new indoor location technologies are deployed equitably across your communities.

One of the most promising developments coming out of the Roadmap is the commitment to developing dispatchable location as the preferred indoor location approach. Providing dispatchable location for wireless 911 is truly a game-changer. It puts wireless 911 calls on a par with wireline calls by providing first responders with reliable street address information – what you need to determine where to dispatch the ambulance, fire truck or police car. But dispatchable location goes even further by providing first responders with the caller's location within the building, including floor level and office or apartment number. This will save precious minutes when first responders enter the building and need to get to the site of the emergency as quickly as possible.

A major component of the Roadmap's commitment to developing dispatchable location capability is the proposed National Emergency Address Database (NEAD). The four nationwide wireless providers have committed to populating the NEAD with access point information from multiple sources, and will submit to the Commission a plan for implementing this database within 18 months of the effective date of rules.

The NEAD provides us with another opportunity to engage the public safety community. We encourage you to participate early in the development of the database and in ensuring that the database reflects the access points available in your community when ultimately deployed. Local knowledge of building clusters, multitenant communities, universities, sports complexes, and major retail destinations, to name a few, must be leveraged early to focus the wireless providers on cataloguing these areas in the database. Coupled with that opportunity is the

urgency for your communities, if you are not already doing so, to begin to take advantage of Geographic Information Systems (GIS) and the ability to compile detailed information on the location and morphology of buildings. How tall are your communities' buildings? What materials went into their construction? Do they occupy an entire city block? Do they have controlled access points? These layers of information are known at the local level and can be further leveraged to enhance the NEAD. Ultimately, the success of a robust dispatchable location system will require the cooperation of local law enforcement and fire services, and we encourage you to collaborate and work with the nationwide providers as they implement dispatchable location in your area.

We recognize concerns raised about the privacy of data that will be collected for the NEAD. Accordingly, the Order requires the four nationwide carriers to submit a privacy and security plan for the NEAD to the Commission for approval in advance of the initial launch of the database. We also require all wireless providers that plan to use the NEAD to certify to the Commission that they will only use the NEAD for purposes of 911. We are committed to protecting individual privacy and will continue to work with stakeholders to fulfill this commitment as improved location accuracy is implemented.

We are counting on the development of dispatchable location capability and the launching of the NEAD to be game-changers for wireless indoor location, But it's also worth noting that the they could be game-changers for locating other indoor 911 callers as well, for example VoIP users. If you think about it, the access point information that is registered in the NEAD for a given building could be just as useful for locating a VoIP 911 call within the building as a wireless call. And the potential applications don't necessarily stop with voice calls. As 911 increasingly supports non-voice as well as voice communications, including text,

video, and machine-to-machine communication, the NEAD could serve as an indoor location clearinghouse for all elements of the 911 ecosystem.

While the order provides a path for wireless carriers and PSAPs to develop and deploy dispatchable location, it also ensures that carriers will provide accurate coordinate-based location information in the event that dispatchable location progresses more slowly than is hoped. The order requires wireless carriers to deliver dispatchable location or x/y coordinates within 50 meters of the caller, for 40 percent of all 911 calls, within 2 years. That percentage increases to 50 percent in 3 years; 70 percent in 5 years, and ultimately 80 percent at the six-year mark. With regard to vertical location, the order requires CMRS providers to begin delivering uncompensated barometric pressure data in 3 years from any device that is capable of delivering such information. Also at three years, the nationwide CMRS providers must submit a proposed z-axis metric, supported by test data, to the Commission for review and approval. At 6 years, wireless carriers will need to deploy vertical location technology – either dispatchable location or z-coordinate technology that meets the Commission's approved metric – in the top 25 markets nationwide. In 8 years, they must deploy vertical location technology in the top 50 markets.

The order establishes a new process that is more rigorous than any of our prior rules for ensuring that carriers comply with these requirements. First, it requires establishment of a permanent, independent test bed for testing and certification of the location technologies that wireless providers intend to deploy in their networks. The test bed will provide the opportunity for continuous research and development of location technologies and solutions.

Second, the order provides for use of live 911 call data to ensure that tested technologies are actually being deployed and used in the field consistent with their test bed performance.

Beginning 18 months from now, wireless providers will begin reporting aggregate live 911 call data from six representative cities across the country: Atlanta, Denver/Front Range, Chicago, San Francisco, Philadelphia, and Manhattan in New York City. This data will be used to determine whether wireless providers are in compliance with relevant horizontal and vertical benchmarks. This set of rules is a first: to have improvements to 911 location accuracy driven by a strong permanent test bed regime, and to have progress and compliance measured based on live 911 call data, not test results alone.

In addition to the live call data, carriers must submit periodic reports to the Commission on their progress toward implementing improvements to indoor location accuracy. We will use these reports to gauge progress and assess whether indoor location accuracy is being implemented as promised. If progress lags, the Commission has the option of considering additional steps to ensure that wireless indoor location accuracy is meaningfully improved.

Finally, as a critical component of these rules, the order requires CMRS providers to furnish live call data to PSAPs upon request. This is key to successful implementation because PSAPs are in the best position to assess the performance of 911 location technologies in their own jurisdictions. As carriers begin to implement the new requirements and as data begins to flow, the public safety community needs to be prepared to analyze that data, assess carrier performance, and ensure that all areas of their communities benefit from these new location technologies.

While the Order adopted last month will serve to close the location accuracy gap for indoor and outdoor calls, we are also looking into the issue of misrouted 911 calls, which may happen when a 911 call is made near a jurisdictional boundary. Of course radio waves don't stop

at county or PSAP boundary lines, so calls are simply routed to the nearest cell tower based on initial Phase I information, which includes only the address of the cell tower. However, Phase II location information received later in the call from GPS or other sources may show that the call should have instead been routed to a different PSAP. This requires the dispatcher to re-route the call to the other PSAP, which may result in critical time lost. Here in the Nation's Capitol, PSAPs have maps beyond their jurisdictional boundaries to combat this issue, but many areas nationwide lack such resources. The Bureau will take a closer look at Phase I misroutes and expects to enlist the help of industry and of the Communications Security, Reliability, and Interoperability Council to identify technical options that reduce the incidence of these misroutes. PSAPs however must assess their Geographic Information Systems and ensure that their maps don't "stop at the county line."

NG911

I want to say a few quick words on Next Generation 911. Next Generation 911 provides the opportunity to expand 911 services and to use new media for 911, but also, to evaluate and reinforce the security of our 911 networks. Technology transitions in the telecommunications sector are already happening, and they will continue to have a profound impact on public safety communications as Next Generation 911 is rolled out. As networks transform, the capability for public safety officials to reliably communicate among themselves and with the public must be preserved. Similarly, the ability for individuals to reach help in an emergency is fundamental and must be maintained.

As I mentioned earlier, data analysis will be a powerful tool in our arsenal in a Next Generation 911 environment. One example of this is the ability for a PSAP to see real-time

911call volume in a geographic area, as some of our colleagues in California have been experimenting with. Being able to see real-time call volume, as well as the contents of real-time 911 text messages or other communications, can provide a PSAP with a multi-faceted view of an emergency as it unfolds, which may in turn enable the PSAP to dispatch a better informed and more dynamic response team to the incident.

The Bureau staff has been working not only on improving how the public reaches emergency services through 911, but also on how emergency managers can provide "one-to-many" alerts and vital information to the public. Traditionally, 911 and emergency alerts have operated in isolation from one another usually under entirely separate governance structures. We need to rethink this approach, because emergency communications are becoming increasingly dynamic and two-way as the world becomes increasingly interconnected through the Internet and social media. For example, consider an active shooter scenario inside a school – in addition to calling 911, students may take to text or social media seeking help from parents or law enforcement, causing concerned parents to descend upon the school and possibly compromise the efforts of police SWAT teams setting up a critical safety perimeter. If PSAPs were able to send a targeted emergency alert out to all cell phones and wireline phone numbers in a geographic area, indicating awareness of the emergency and directing recipients to remain calm and stay away from the school, both parents and students would be informed that emergency response is under way, parents would be more likely to follow the directive to stay away from the school, and the SWAT team could do its job more effectively. To this end, the Bureau is looking at how we can improve the use of "one-to-many" alerting platforms like the Wireless Emergency Alert system, as communication from one to many can be a critical part of effective emergency response.

911 Reliability

The Commission is also continuing its work to ensure the reliability and resiliency of 911 networks themselves. As you will recall, about a year ago the FCC responded to the 2012 derecho storm by adopting rules requiring 911 service providers to take reasonable measures to provide reliable service, and certify annually whether they have implemented best practices in the areas of critical 911 circuit diversity, central office backup power, and diverse network monitoring. These rules are now in effect, and the initial certification deadline is October 15, 2015.

The FCC has also strengthened requirements for 911 service providers to notify PSAPs in the event of an outage that may affect 911 service. Covered 911 service providers must now notify PSAPs within 30 minutes of discovering a 911 outage and follow up with additional material information within two hours.

While our initial 911 reliability order focused on maintaining 911 networks when challenged by storms and power outages, outage trends in 2014 revealed that we must also deal with new 911 reliability challenges as networks transition to IP. These new and transitional networks increasingly rely on consolidated infrastructure such as servers and databases to process calls for multiple jurisdictions, giving rise to the risk of "sunny day" outages caused by poor network design or inadequate testing. We learned in 2014 that this was not a theoretical concern. The April 2014 multistate 911 outage, which shut down 911 service for six hours throughout the State of Washington and in portions of six other states -- showed that a single software error can be just as damaging to 911 service as a hurricane or other natural disaster. Our approach to 911 reliability must respond to these new risks.

In November 2014, the FCC adopted a Notice of Proposed Rulemaking seeking comment on additional proposals to improve NG911 network reliability in cooperation with state and local partners, including PSAPs. Eric Schmidt of our staff will be presenting more information about this proceeding in the first session this afternoon. Comments on our NPRM are due March 9 and replies April 7. We welcome insight from NENA and its members about what we can do to improve 911 reliability as we continue to develop NG911 systems and incorporate Next Generation functionalities into our existing approach to 911.

TFOPA

Another of our recent efforts to improve 911 functionalities is the Task Force on Optimal PSAP Architecture, or TFOPA. In the Text-to-911 Order, the Commission directed the Public Safety Bureau to establish the Task Force, and the Task Force was launched in January of this year. The Task Force includes a diverse selection of experts from across the 911 community, including representatives from PSAPs, state and local 911 authorities, carriers, technology companies, federal agencies, and consumer groups. You will be hearing more about the Task Force later this afternoon from Brian Fontes of NENA, Steve Souder of Fairfax County – the Task Force Chair – and Dana Zelman from the Bureau staff. The purpose of Task Force is to examine the current structure and architecture of the nation's PSAPs and to make recommendations on how to optimize these elements as we transition to Next Generation 911. In this new environment, what are the appropriate circumstances under which PSAPs should consolidate facilities or functionalities in order to promote greater efficiency of operations, improved safety of life, and optimized cost effectiveness, while still retaining important integration with local first responder dispatch and support?

The Task Force is broken into three working groups. The first working group will address cybersecurity issues and make recommendations for PSAP-specific cybersecurity practices based on the NIST Cybersecurity Framework and other foundational sources. It will also identify resources and tools for PSAPs to use when developing cybersecurity strategies, and make recommendations for PSAP cybersecurity workforce development and training, in hopes of developing a comprehensive and user-friendly guide for PSAPs to equip their facilities and personnel with a cybersecurity plan that best fits their needs. APCO's Jay English is the chairman of this working group, and I have full confidence that he and his fellow working group members will help us take some meaningful steps forward on making cybersecurity an omnipresent part of PSAP facilities and operations.

The second working group will focus on a broader set of issues related to PSAP consolidation and efficiency. The working group will develop recommendations on how PSAPs can improve 911 functionality and cost-effectiveness through consolidated NG911 network architecture design and operation, including optimal NG911 system and network configurations for a range of existing PSAP use cases (for example, large urban and rural PSAPs); projected costs and transition periods associated with optimized configurations; and ensuring and improving access to NG911 for people with disabilities. It may be necessary to reduce the technical variation of PSAPs in order to improve resiliency, efficiency, and functionality, but we should also strive to preserve the more local community-based aspects of 911, and this working group will help us do that. David Holl of the National Association of State 911 Administrators is heading up this working group, and I have great confidence that this working group will produce a useful, informative report.

Finally, our third working group will examine funding and cost issues, which I know loom over all of your day-to-day operations. This working group will develop recommendations on optimal resource allocation and budgeting for PSAPs to transition to NG911, and identifying potential models for sustainable funding of PSAP NG911 operations. The group will also look at strategies to optimize use of state 911 fees to expedite the migration to NG911 and create incentives to discourage fee diversion. We are excited to have Commissioner Phil Jones from the Washington State Transportation and Utilities Commission leading the charge for this working group.

Last month, the Task Force convened for the first time here in Washington and really hit the ground running. I'd like to take this opportunity now to thank all Task Force members that are with us here today. These folks are generously giving their time on top of their already busy schedules, and we are grateful for your participation.

Cybersecurity

I'd like to close today with a brief discussion of the Commission's efforts in cybersecurity, a strong theme throughout our entire 911 portfolio. PSAPs are increasingly moving to IP-based systems which, on the one hand can provide significantly enhanced functionalities and cost savings, but also bring exposure to a greater number of vulnerable entry points and an ever-expanding threat landscape. We have all watched the growing number of large-scale cyber attacks against major companies, but we cannot overlook the fact that PSAPs are also a very attractive target for cyber threat actors.

I mentioned earlier our efforts to improve 911 reliability, which ultimately comes back to the security of our nation's public safety communications networks. NG911 networks, which

rely on IP-supported architecture rather than traditional circuit-switched TDM architecture, introduce promising new capabilities, such as more flexible call routing and the ability to provide PSAPs with a greater range of information (such as video). For example, call control in legacy 911 networks was primarily performed in a central office switch that was close to the customers it served, whereas IP-supported networks increasing rely on geographically-remote servers and software-based components to support key 911 functions, such as 911 call routing, across multiple states and jurisdictions. Consequently, a 911 outage in an IP-supported network has the potential to affect a much greater number of PSAPs and people, across multiple states, as demonstrated by the multistate "sunny day outages" that we experienced last year.

A core mission of the FCC is to ensure that the Nation's communications infrastructure is secure and reliable. We take this seriously and recognize that the responsibility is universal, and it extends to Americans in every part of the country, however remote. Private sector companies own and control the vast majority of our Nation's networks and share the same commitment towards public safety. As we look forward, the challenge of keeping networks reliable and secure is too important and increasingly sophisticated for organizations to "go it alone." Effective information sharing is a critical component of cyber defense, so we must work together with the public safety community, with telecommunications companies, and with cyber-capable government organizations.

Representatives from all facets of the communications landscape – including large, small, and rural communications companies; academia; public interest groups; government partners; and other stakeholders – contribute their time, expertise, and unique perspectives to tackle some of the most challenging cybersecurity issues facing us today. The FCC has long taken a collaborative approach, working in partnership with private sector stakeholders through our

federal advisory committees, the Technical Advisory Committee (TAC), Working Group 1 of the TFOPA, and the Communications Security, Reliability and Interoperability Council (otherwise known as CSRIC). I want to applaud the work of CSRIC in this arena, as its Working Group 4 will be issuing their final report on application of the NIST Cybersecurity Framework to the Communications sector in March of this year. We look forward to their findings and hope to use them as a foundation for our next steps in cybersecurity.

It is clear that public safety, disaster response and homeland security communities must remain reliable and secure under a wide range of stressful conditions – they must be available when we need them, and effective cyber risk and threat planning, management, mitigation, and response is crucial for our shared mission to ensure the resiliency and reliability of the nation's communications networks.

Conclusion

In closing, I want to thank the executive leadership of NENA for hosting this important event and for bringing this community together. We have made a lot of progress in the past year to improve 911 and lay the foundation for the transition to Next Generation 911. But we still have unfinished business and many challenges ahead. I look forward to continuing to work with you to successfully, securely, and creatively implement NG911 to better serve our communities and enhance emergency response. Thank you.