Rear Admiral (ret.) David Simpson
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission
Keynote Remarks for
APCO Emerging Technology Forum
"Public Safety Communication Readiness in a Broadband Age"
February 26, 2014

It is a pleasure to attend my first APCO meeting. Though I've only been at the Commission for roughly 100 days, I've already had the opportunity to meet with APCO leadership several times as the Commission has taken three significant actions during this period to strengthen and modernize 911 communications, which I'll discuss in a few moments. I am glad to have this opportunity to continue the dialogue.

I'm new to my role as Chief of the FCC's Public Safety and Homeland Security Bureau, but I'm not new to the Bureau's mission – and yours – of using communications technology to promote public safety. My more than two decades of experience supporting the communications needs of the Department of Defense, including U.S. troops deployed abroad, give me the greatest appreciation for the responsibilities you face in supporting the communications needs of public safety.

As we've increasingly seen, emerging technologies – the focus of this meeting – are less "emerging" and more commonplace every day. The "Internet of things" has placed technologies in our homes that were pipe dreams a few years ago. There are now more wireless phones in America than there are people, and by the end of 2014, the International Telecommunications Union says that this will be true on a worldwide basis. Consider that for a moment: there will be more mobile phones in the world than the entire population of the planet. And an estimated one in six phones in current use are smartphones that put the web at your fingertips anytime, anywhere, with a vast ecosystem of apps that range from the mundane to the remarkable –from finding a Starbucks to health and safety apps that may literally save your life. As these advanced

technologies are embraced by consumers in the commercial marketplace, this creates both challenges and opportunities for public safety, and for us as a federal regulator in this space. We need to ensure that core public safety functions continue to be served as technology changes, and we need to look for every opportunity to help public safety leverage new technologies to serve the public more effectively – and more cost-effectively.

Today, I will highlight some of the areas in which the Bureau and the Commission are actively pursuing these emerging technology goals. I will also talk a little about the road we see ahead and how APCO and others in the public safety community can help us get there.

These key issues for the Commission include: (1) the transition of the nation's commercial infrastructure from the legacy circuit-switched network to an IP-based environment; (2) enhancing the reliability of the nation's legacy 911 infrastructure and supporting the rapid transition to Next Generation 911; (3) FCC efforts to support the deployment of the FirstNet nationwide interoperable public safety broadband network; (4) public safety's important role in disaster response and alerting; and (5) the Commission's increased focus on collaborative cybersecurity efforts. Transitioning our communications network to meet new technological expectations encompasses all of these issues. APCO as well as other stakeholders are key participants in the transformative process; we need you to help ensure that our communications infrastructure will meet the public's growing expectations and public safety's needs.

IP Transition

The nation's communications sector is rapidly transitioning from legacy technologies to more advanced communications platforms. Copper is being retired in favor of fiber optics. Switched data and telephony are being replaced by all-digital Internet Protocol transport. Traditional cellular networks that primarily supported voice are making way for wireless broadband networks that support voice, data, and video. Broadband is the watchword, and the demand for resources that support the applications that take advantage of these platforms is growing exponentially.

Consumer utilization of communications services is likewise changing. Americans are increasingly moving from wireline connectivity to wireless options. In 2012, nearly 40 percent of American households reported going wireless-only. VoIP and other broadband voice applications have replaced traditional phone services in many homes, offering enhanced features that narrowband technologies cannot achieve. As the Commission has stated, we expect there will come a tipping point where the adoption of new communications technologies reaches a critical mass and most providers will wish to cease offering legacy services.

Changing technology, however, does not diminish our commitment to public safety communications. Rather, it opens up new possibilities for services and systems. In fact, public safety is the first of the core statutory values entrusted to the Commission, which the Chairman refers to as part of the "Network Compact." This is reflected in the technology transitions order that the Commission released in January to launch a series of experiments in the coming year.

The Commission's mission and responsibility are to ensure that core statutory values endure as we embrace modernized communications networks. To learn how the technology transitions will affect consumers, the Commission's January order (1) calls for voluntary tests of real-world applications; (2) proposes targeted experiments and cooperative research; and (3) seeks to improve data collection and feedback.

The order further makes clear that all experiments will be expected to support and protect core public safety functions, and will be evaluated based on how effectively they do so. Core functions that must be sustained include the ability of the public to reliably reach 911, first responders, and other emergency response authorities without interruption; provision for assistance to law enforcement; and the protection of first responder radio systems and other wireless communications systems used for public-safety-related communications. Furthermore, we will require experiments to ensure that in the event of a public safety failure, the provider will be able to immediately restore legacy service, fix its IP-based service, or provide a comparable service.

I strongly encourage your active participation and input into these experiments. Whether public safety initiates its own experiments or participates in experiments initiated by others – your participation is vital to the success of the transitions. These experiments offer an opportunity to "bake in" public safety needs from the beginning, and not tacked on as an afterthought after disaster strikes. They also offer an opportunity for you to trial your own technologies and protocols, learn from others, and develop use-cases that can help you justify the funding and resources for the parallel public safety transitions that need to occur. I think we all know at this point the IP transition is no longer an "if." It is a "when" that we must be prepared for.

911 Reliability/Next Generation 911

As communications networks migrate to newer technologies, both wireline and wireless, and as consumer habits change, we must make sure these changes preserve and improve Americans' access to critical lifesaving services, most notably 911. We must also ensure that legacy technologies remain reliable during their useful lives. For this to occur, public safety and commercial stakeholders in the 911 ecosystem must work in concert to make sure that 911 calls get through to emergency providers, and that they are received with the information necessary for first responders to do their jobs and dispatch help promptly.

At the Commission, we are committed to doing our part to ensure that the 911 system works effectively and that it keeps pace with technology and the needs of the public. This includes a significant focus on three key aspects of the 911 system: (1) the reliability of the 911 infrastructure during disasters; (2) advancing the enhanced capabilities of Next Generation 911, with an initial focus on text-to-911; and (3) enhancing the location information PSAPs receive for wireless 911 calls to ensure that callers in all localities, including indoor environments, can be found quickly when in need.

Reliability of 911 Systems

In December, the Commission adopted landmark rules to help ensure that Americans' phone calls to 911 will be delivered during disasters. The rules are designed to improve 911 communications networks nationwide by requiring 911 service providers – generally, the

wireline phone companies that route both wireline and wireless calls to 911 call centers – to take reasonable measures to provide reliable and resilient 911 service, as evidenced by an annual certification. We also strengthened our rules to ensure that 911 service providers give 911 call centers timely and useful notification of 911 network outages.

The new rules are designed to maximize flexibility for 911 service providers and account for differences in network architecture without sacrificing reliability. Accordingly, the rules require service providers to certify annually that they have either implemented industry-backed best practices or acceptable alternative measures that are reasonably sufficient in light of their particular circumstances.

The best practices cover three core areas: auditing 911 circuits for physical diversity, maintaining backup power at central offices that directly serve PSAPs, and maintaining reliable and resilient network monitoring systems. If needed, the Bureau may follow up with service providers to address deficiencies revealed by the certification process. The FCC will review these rules in five years to determine whether they are still technologically appropriate, adequate, and necessary.

Text-to-911

In today's world, mobile wireless communications are increasingly central to the day-to-day lives of Americans. Moreover, wireless usage has become increasingly text-based. Yet if you send a text message to 911 during an emergency in most parts of our country, it won't be received. In light of these trends and the importance of ensuring effective 911 service – particularly for those who cannot access 911 call centers with a voice call – the Commission has identified text-to-911 as a necessary first step in the development of Next Generation 911 capabilities. Being able to text during an emergency is essential for the tens of millions of Americans with hearing and speech disabilities. Texting can provide an additional means of contacting 911when a voice call may place someone in danger, such as in an active shooter or domestic abuse situation. When voice networks are congested, text messages may provide an alternate means of getting through to 911 call centers.

APCO has played a major role in meeting this challenge, through the voluntary agreement that it and NENA entered into with the four largest wireless carriers, in which the carriers committed to develop text-to-911 capability by this coming May. We fully expect the carriers to meet their commitment and make this service a reality. In addition, over 45 PSAPs in 14 states have stepped up and are already accepting texts to 911. We know that the ability of these call centers to receive texts has made a difference in consumers' lives. For example, in Vermont, which launched text-to-911 in early 2012, the service has enabled first responders to intervene in, and even stop, suicide attempts and domestic violence situations.

For our part, last month the Commission adopted a Policy Statement expressing the Commission's intent to establish functional standards for text-to-911 that will ensure its availability on all text platforms that support interconnected texting. The Policy Statement recognizes the leadership role that the four largest wireless carriers have taken in working with NENA and APCO, and encourages other wireless providers and interconnected text providers that are not parties to the carrier-NENA-APCO agreement to work with the public safety community to develop similar commitments to support text-to-911 in a timely manner, so that all consumers will be ensured access to text-to-911 regardless of what text provider they choose.

If the multistakeholder process achieves these values in a timely manner, the Commission stated that Commission rules would be needed only to codify the multistakeholder standard so it applies to all providers equally (including future entrants into the market) and brings regulatory clarity so that all participants in the 911 ecosystem can plan accordingly.

At the same time, to enable a regulatory solution if a voluntary solution is not forthcoming, the Commission also adopted a Further Notice of Proposed Rulemaking to round out our record on many of these issues, particularly on questions related to interconnected text providers – those "over the top" texting applications that use phone numbers to send text messages. The Commission also proposed rules that would require all text providers, including small wireless carriers and interconnected text providers, to begin providing text-to-911 services by the end of the year.

All of this, of course, merely sets the table for text-to-911. For it to become a reality, as the Chairman said in January, the PSAPs need to do their part, and that is where we need APCO and others in the public safety community to lead. Some of you have already shown leadership by taking up the challenge in your own PSAPs, and demonstrating that text-to-911 works. For other PSAPs, we know – and the Chairman knows – there are funding and operational challenges in adopting text-to-911. Together, we need to raise the visibility surrounding the resource decisions that will be needed to support this. These challenges, however, can be overcome. More and more, the citizens you serve are expecting this service, and public safety officials must respond to that expectation. So I am asking you now to be active participants in this dialogue. This will need to include PSAP governance and industry. The Commission will work with all stakeholders to facilitate commitments that will support your mission and protect your constituents.

Wireless Location Accuracy

Following on the Commission's efforts with respect to text, we also recognize that there have been significant changes in location technology and how consumers use wireless devices since the Commission last made changes to its wireless location accuracy rules. More than 70 percent of 911 calls come from wireless phones, and an increasing number of those calls originate from indoors. Consumers expect that when they make a 911 call, emergency responders can locate them precisely and quickly. However, when consumers call 911 from a wireless phone indoors, a PSAP may not automatically receive adequate location information to locate that caller.

Just last week, the Commission adopted a Third Further Notice of Proposed Rulemaking that proposes rules to ensure that PSAPs have access to the best available location information with each wireless 911 call, no matter where it originates.

In particular, the Further Notice proposes to bridge the gap in the Commission's rules by proposing location accuracy standards for wireless 911 calls originating from indoors, as well as modifications to the existing E911 Phase II rules to improve the speed and accuracy of location information for wireless 911 calls from all environments. It also encourages carriers, technology

vendors, and PSAPs to present collaborative solutions to meet these objectives. These proposals result largely from the input we received from the public safety community and the Commission's recent workshop. The Further Notice is intended to foster a continued dialogue between all stakeholders on how to achieve these location accuracy goals in both the near and long terms, with the objective that wireless 911 calls ultimately will be delivered to PSAPs with precise dispatchable address information.

So again, here is where you come in. I urge you to get involved and participate in these proceedings so we know the challenges you face, the needs that you have, and how the Commission and industry can work with you to achieve the best possible level of public safety to our communities.

FirstNet

In parallel with the transition the commercial sector is undergoing, public safety communications are also transforming to embrace broadband technologies. Broadband has the potential to offer public safety not only the same features consumers already use, but also to provide enhanced functionality that will better support public safety's core mission: to protect life and property, and to ensure the safety of our public safety personnel while they serve their communities.

Of course, the public safety broadband landscape has been dramatically reshaped by a single event -- the establishment of FirstNet. With FirstNet, Congress has authorized a major "down payment" in the broadband transformation of public safety communications and the eventual establishment of a nationwide interoperable public safety broadband network. I am here to tell you that the Commission is committed to doing all it can to help FirstNet succeed in this vital mission.

As you are well aware, the Middle Class Tax Relief and Job Creation Act of 2012, which created FirstNet, also delegated specific tasks to the FCC to support FirstNet's mission.

The statute made the FCC responsible for the Technical Advisory Board for First

Responder Interoperability, which developed minimum technical requirements to ensure a nationwide level of interoperability for the FirstNet network. The Commission approved and transmitted the Board's recommendations to FirstNet, which will provide the core set of requirements for the network when FirstNet initiates its RFP process.

In 2012, the Commission issued a new license to FirstNet, providing the spectrum that Congress designated in the Act, to enable FirstNet to move ahead with its mission. More recently, in October 2013, the Commission adopted a Report and Order consolidating basic technical rules for this spectrum, which were supported by FirstNet. This will help to prevent harmful interference and promote prompt certification of equipment to be used in the band. We expect that this unified set of rules will facilitate competition and innovation in the equipment market, including new entry.

But our work to help FirstNet is not done. The Act requires the Commission to take all actions necessary to facilitate the transition of the 700 MHz public safety broadband spectrum to FirstNet. In this regard, we have more to do. For example, in some areas, there are incumbent public safety narrowband operations in the FirstNet spectrum, which predate the designation of this spectrum for broadband use. We have solicited public comments on how to address this question.

The Act also provides that in the event that any state seeks to exercise the "opt-out" rights that are provided for it under the Act, the Commission is responsible for reviewing and either approving or disapproving the state's opt-out plans based on specific statutory criteria. We intend to provide states and FirstNet with clear guidance on how that will work before states have to choose whether to opt-out under the Act.

More generally, the Act envisions that the Commission will play a consultative role with FirstNet as FirstNet moves forward with its planning and deployment efforts. Our job is not to tell FirstNet how to do their job, but to provide our assistance and expertise when they need it. We take that responsibility seriously and have begun regular staff-level contact with FirstNet's management over the last several months. We look forward to continuing to work with FirstNet

and offering guidance from the Commission where it is needed.

We must also recognize that FirstNet, while a huge achievement in and of itself, is only a part of a larger ecosystem. Moreover, while FirstNet has the benefit of $7 billion in federal funding, we know that such funding is not enough by itself to achieve – and sustain – Congress' vision of a nationwide network. We must develop creative strategies to sustain FirstNet and the larger ecosystem. Investment in all aspects of public safety broadband is vital because all of the data that is being generated – whether by consumers, by vehicles and remote monitoring devices, and by our public safety personnel – is useless if it cannot be transmitted to the people that can do something with it. Consumers are buying and using smartphones in droves – information is being generated that can vastly improve your core missions if you are able to tap into it and use it. Thus, we must develop strategies for investment in NG911 – to "pull" that information from consumers – that go hand in hand with investments in the public safety communications infrastructure to "push" that data into the field. A surveillance video of a suspect is useless if an officer cannot see it. Schematics and telemetry of a high rise on fire cannot assist a Fire Chief who cannot view it.

In today's data-rich world, we are obligated to make sure that information is used in a manner to support public safety, and not left on the table for lack of funding or lack of institutional will to plan for a broadband revolution that is no longer on the horizon, but a part of our present.

Emergency Response

Another way in which we are focused on supporting disaster preparedness, response, and recovery is through our work with our Federal partners to increase the reach and capability of alert and warning systems. Technology provides us with more ways of reaching people than ever before, and we must continue to take advantage of new systems and avenues to interact with those in our community in times of need.

For example, with over a third of U.S. households relying solely on wireless communications, technological advancements in mobile alerting are helping save lives. The

FCC, along with commercial wireless service providers and the Federal Emergency Management Agency, enabled the Wireless Emergency Alert system, or WEA, in 2012. The WEA is a tool that allows authorized emergency personnel the capability of sending geo-targeted messages onto WEA-enabled mobile devices to alert the public. These alerts utilize advanced technology to ensure immediate delivery of text-like messages, without a charge to the mobile user, in the case of an emergency. State, local, and tribal governments have the ability to use this vital system to reach the public in times of need, and I urge you all to ensure that emergency managers in your jurisdictions are aware of what WEA can offer. An increasing number of mobile devices are WEA-capable, and the proliferation of smartphones makes this alerting system more valuable each day.

Once disasters strike, we all know how important communications are to the public and first responders. The FCC's 24x7 Operations Center helps ensure we are prepared to assist all of you when there is an emergency, at any time. We track communications outages and conduct outreach to identify issues because we know how important communications are for life-saving and life-sustaining operations.

Technological advancements continue to increase the capability of responders to coordinate activities or to gain situational awareness, whether on communications or disasters writ large. By taking advantage of wireless and broadband technologies, valuable information can be provided to incident response teams in a more thorough and timely manner. Capabilities such as video sharing or blue force tracking can give first responders greater information about hazards, or about victims, and information can be shared broadly or in a targeted manner as defined by the situation on the ground. As technology progresses from the LTE environment being built out today to the eventual public safety broadband network that will be operated by FirstNet, the tools and applications available to the response community will only become more valuable to the public safety mission.

One of the recurring problems in a disaster is the fact that networks often experience congestion during emergencies or events, which is when they are needed the most. The FCC is working with Federal departments and agencies to ensure that we can maintain priority

communications for national security and emergency preparedness (NS/EP) personnel, even in an IP environment. The Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) allow Federal, state, and local users with priority access to wireline and wireless networks during emergencies and when services are congested. We must make sure that service providers are ready to handle priority services over next generation technologies so that response personnel never miss an opportunity to assist people in harm's way because of a failure to communicate.

Cybersecurity

And last, I'd like to discuss cybersecurity. In the world of rapidly developing technology and the ongoing transition to "EoIP," or "Everything over Internet Protocol," threats to the communications capabilities of America's networks are growing at a rate that matches – and may exceed – the pace of this technological development. The first priority of the FCC – indeed, a primary reason for the creation of the FCC – is to ensure that the nation's core communications infrastructure remains secure and reliable.

To fulfill this part of our mission with respect to cybersecurity, we must work on several fronts. We must understand both the technology and the cyber threat environment. We must engage our government partners. We must engage private sector entities. In these respects, we are approaching cybersecurity in the way we approach many other public safety issues.

There are some unique cybersercurity challenges: first, the incredibly fast pace of change; second, critical broadband infrastructure now underpins service not only in the communications sector but also every other critical infrastructure sector; and third, the potentially large-scale consequences of even one cyber incident generated potentially from halfway around the world. Defining our cyber role as the independent federal regulatory agency in this environment is challenging.

So far, we've approached cybersecurity much the same as we have approached overall network reliability. This is to say we start by working with industry and other stakeholders to develop best practices. (In the case of legacy commercial networks, we assess the effectiveness

of the best practices through outage reporting. We're not there yet with broadband services, and need to improve the reporting for outages induced from cyber actions.) We collaboratively develop best practices with industry through the Communications Security, Reliability and Interoperability Council (or "CSRIC"), our federal advisory committee on these issues. APCO is an active participant and has held the chairmanship of CSRIC in the past. Over the last several years, CSRIC has made recommendations to address several key cybersecurity threats. Next month, CSRIC will take another step in cybersecurity and initiate work on recommended best practices to operationalize the recently released NIST Cybersecurity Framework.

The FCC has applied a great deal of resources over the last year to the massive effort, led by NIST at the U.S. Department of Commerce, to help develop a voluntary Cybersecurity Framework for 16 critical sectors, including communications. This work emanates from the February 2013 Presidential Executive Order on cybersecurity and companion Presidential Policy Directive on critical infrastructure protection that directed federal agencies, in an overall effort led by DHS, to develop the first comprehensive nationwide framework to protect our nation's critical infrastructure. The FCC actively participated in the drafting of the framework, and we continue to work to support its adoption, both through the framework process and through CSRIC. NIST will play an active role in helping our industry-led working group determine how best to use the framework for telecommunications.

Since I'm talking to a public safety audience, I want to mention other CSRIC work that touches on both public safety and cybersecurity – the Emergency Alert System. The "zombie" attack in February 2013, helped to focus everyone on just how much even the EAS requires a secure cyber environment. In case you didn't hear about it, a hacker or hackers obtained unauthorized remote entry into EAS equipment at various broadcast facilities and transmitted a false EAS alert that "zombies were rising from the grave." The issue was related to individual EAS participants' network and equipment security –though not the Emergency Alert System itself. While we worked with broadcasters to address the issue at the time, we believe that more can be done. We tasked the CSRIC with recommending improvements to EAS security. These recommendations will include methods for ensuring that critical measures are implemented so that the vital EAS alert and warning function is more capable of defending against cyber attacks.

I would be remiss if I failed to mention the significant work on cyber-related issues coming out of our Technological Advisory Council, another FCC advisory committee (that our current FCC Chairman used to chair). For the next year, we've charged TAC with looking at the potential for improvements to telecommunications cyber readiness for long-lead targeted hardware and software development. We'll be looking for cyber "game changers."

Where do we go next as we seek to ensure a secure cyber environment? We're not presuming that the answer involves regulation. We're moving forward with the public-private multistakeholder work in CSRIC and TAC. We're continuing to support adoption of the NIST Cybersecurity Framework and related work with our federal partners under the Executive Order and Presidential Policy Directive. Our role in cybersecurity will continue to evolve and become a Commission-wide program. I believe that the best defense for our nation in cyber is an industry-led, vibrant, innovative cyber posture that the FCC — if it does anything —helps the owners and operators of critical communications infrastructure to see threats that they wouldn't otherwise see on their own, to recognize accepted cyber risk, and to systematically close their readiness gaps.

As the nation's dependence on communications infrastructure continues to increase and cyber threats continue to grow, the FCC remains committed to preserving the reliability of public safety communications. The FCC will work with its public and private sector partners and to facilitate development of cybersecurity best practices, real-time cyber threat information sharing and awareness, early involvement in hardware and software development, and coordination for international cybersecurity policies.

Conclusion

In closing, I would like to again thank you for the opportunity to speak to you today. If you take one thing away from this discussion, I hope it would be a renewed commitment to get involved, motivate your colleagues, and engage constructively in creating a safer, more secure public safety future. The American public has embraced the next generation of communications technologies that has enhanced life in so many ways, and so must the public safety sector. I

challenge us all to be responsibly creative and take the initiative to define a better future for first responder communications. We are looking forward to the collaboration with you.

-#-