APCO Emerging Technology Forum
Keynote Address
Wednesday, March 11, 2015

Remarks of Rear Admiral (ret.) David Simpson
Chief of the FCC's Public Safety and Homeland Security Bureau

-As Prepared for Delivery-

It's always a privilege to address APCO and its members. We appreciate the leadership role that APCO has taken on with respect to so many important public safety issues, and the key contributions you have made in our proceedings.

As you well know, Chairman Wheeler has made clear that public safety is a priority, and it is no coincidence that the past year has been one of the most productive in the Commission's history on public safety issues. I'll mention some of those accomplishments, but what I'd really like to focus on is not what we have done, but instead where we are going.

Location Accuracy

I'll start with 911 location accuracy. The Report and Order that the Commission adopted in January was a milestone achievement, and it was made possible in large part by the hard work that APCO, NENA, and the four nationwide wireless carriers invested in negotiating the Roadmap agreement. But as hard as everyone worked to get to a final order, the real challenge now is implementation: establishing the test bed, setting up the reporting of live call data that will begin in 18 months, and beginning the development of the National Emergency Address

Database (NEAD) to support dispatchable location. We are glad to see that APCO, NENA, and the carriers have already begun these implementation efforts. We look forward to monitoring your progress, but we also are also committed to assisting and facilitating your efforts whenever needed.

As we start the implementation process, I'd like to highlight several points that I hope APCO and its members will focus on. First, while the Roadmap and the Commission's order focus largely on steps that the carriers will take to improve location technology and information, it is also of critical importance that PSAPs develop up-do-date and accurate mapping systems that can effectively incorporate the location data provided by the carriers. This will require engagement with multiple stakeholders in the communities they serve. Dispatchable location data from the NEAD will be far more effective in jurisdictions where PSAPs have fully leveraged Geographic Information Systems. This includes compiling detailed information on the location and morphology of buildings, floor plans and building diagrams. How tall are your communities' buildings? What materials went into their construction? Do they occupy an entire city block? These layers of information are known at the local level and can be leveraged to enhance the NEAD in its planning stages. If this sounds like "Next Generation 911"…it's because it is! These details won't just appear one day; PSAPs must partner with

public safety officials and city and county planners to take affirmative steps to develop and sustain this level of information.

As you all know, we are well into the implementation phase for text-to-911. This is yet one more reminder that NG911 is not some shiny vision of the future – it's upon us now. Over 200 PSAPs are up and running with text-to-911 and hundreds more are scheduled in the next six months. We all need to proactively manage the integration of these new functionalities.

I would also like to talk about a topic that has gotten some attention since the Commission adopted its location accuracy order: the potential to use location-based smartphone apps to enhance 911 location. At the Commission meeting, Chairman Wheeler asked the question that many consumers ask: if a commercial app such as Uber can find me, why can't that same technology be used to find me when I make a 911 call? We know, of course, that the answer to this question is not as simple as we – and you – might wish it to be. First, while commercial apps like Uber work well in some locations, there are many locations where they *can't* find you. Second, even where commercial apps could provide location information, they have not been designed to support emergency use, are technically incompatible with the most current 911 systems, and may actually delay or impede the user's ability to call 911 directly.

But even if there is no 911 app that is going to magically solve all of the challenges of 911 location, this doesn't mean we should ignore the potential for apps to improve 911 location accuracy. Indeed, there are brilliant software engineers out there who are looking for innovative ways to improve 911 service, and we should be able to harness that innovation. This is why the Chairman has directed the Public Safety Bureau to take a closer look at the potential use of apps in 911 service and how they could be best integrated into the 911 ecosystem. We are not going to build an app – that is not the Commission's or the Bureau's role. But we do plan to work with 911 stakeholders (including APCO), technologists, and others, to determine how app-based approaches can best be configured and standardized to improve 911 location. Let me be clear on this point, this is not to replace the "Public Safety Grade" work by the carriers to improve Phase One and Phase Two locations; rather the focus will be on apps that can provide value-added location information. When consumers have opted-in for use of 911-related apps (such as some safety, campus security, or medical apps), we ought to be able to ensure that a PSAP displays the provided information in a consistently recognizable manner and that this information in no way disrupts the carrier-provided 911 service. We look forward to working with you on this important initiative. I expect we will want to initially focus on defining what it means to be a

911 application service provider and partnering with standards bodies to provide a single PSAP interface.

NSI phones

Now I'd like to shift to an item we recently placed on circulation at the Commission, proposing to resolve the issue of non-service initialized (NSI) phones. As many of you know, the Commission has long required wireless carriers to forward 911 calls originating from non-service initialized (NSI) devices. The NSI call-forwarding rule was adopted in the early days of cellular to ensure broad access to 911, and it had significant initial support from the public safety community. However, as wireless service has evolved and expanded, the NSI rule has also had an unfortunate and unintended downside – the ease with which NSI phones can be used to inundate PSAPs with non-legitimate and often harassing calls. This negative trend has increased over the years, and PSAPs across the country consistently tell us that the overwhelming proportion of 911 calls they receive from NSI phones are fraudulent or harassing calls. In addition, the need for the NSI rule to ensure 911 access appears to have declined as a result of dramatically increased public access to wireless services, including low-cost and prepaid options. As a result, APCO and NENA, both original supporters of the NSI rule, and many other public safety entities, have come to the conclusion that the NSI rule no longer serves its intended purpose and should be eliminated or

phased out. Recognizing this trend, the Commission has on circulation a draft notice of proposed rulemaking which, if adopted, would seek comment on sunsetting the NSI rule after an appropriate transition period.

We remain committed to the principle of preserving access to 911 for all Americans, but it is important to remember that fraudulent 911 calls undermine such access by tying up PSAP resources and diverting them from legitimate emergencies. We recognize that eliminating NSI 911 functions will not eliminate all fraudulent calls to 911. It will also be increasingly important to ensure that PSAPs can protect themselves against fraudulent calls in the more complex NG911 environment. We look forward to hearing the ideas from APCO and its members on how we might work together on further reducing the incidence of fraudulent calls.

Alerting ("One-to-Many" Communications)

With that, I'll shift to alerting. As our public safety networks transform, the ability for individuals to reach 911 is fundamental and must be maintained, but it is equally important for public safety officials to be able to reliably and authoritatively communicate with the public in an environment where the velocity of information dissemination over social media during crises continues to accelerate. Often that informal information dissemination lacks creditability, is not authoritative, and can even be counter-productive.

The IP transition is enabling a convergence of alerting platforms into a powerful tool for emergency managers and the communities they serve. The Emergency Alert System (or EAS) is now combined with Wireless Emergency Alerts within FEMA's IPAWS architecture, a combination that allows local emergency managers to combine EAS alerts with geographically targeted alerts to their citizens' handsets. All too often when I visit PSAP, they have not incorporated alerting into their set of emergency response tools. We envision an alerting model in which the EAS and other "one-to-many" systems will work hand-in-glove with "many-to-one" services, such as 911. This should be available in PSAPs, which are typically the best operational center in a community to develop and maintain immediate situational awareness when the first call for help is received. Members of the public could contact emergency managers to inform them of a particular danger and PSAP emergency managers could communicate critical information back to the "at risk" public in the affected community. A good example of how this could work involves the active shooter incident that occurred in Seminole County, Florida last year. In that instance, the Seminole County Sheriff's Department received an anonymous 911 call reporting an active gunman was in the school. School administrators took immediate action by placing the school on lockdown as police responded. However, the call was a hoax. Although the school and sheriff's department coordinated effectively to neutralize the

situation, the threat did not exist. However, before the hoax was exposed, news of the supposed incident was distributed via social media, and concerned parents converged on the school to collect their children. Whether or not the shooter had been real, the cordon of armed police surrounding the school combined with the convergence of parents complicated the situation, and an even more dangerous incident could have occurred. Imagine on the other hand, if the police and other emergency managers could use targeted alerting to inform the parents that all was ok – and even more, to send them a marked-up map of the protected perimeter, give them instructions, or even solicit feedback on aspects of the crisis.

While enhanced functionalities have created opportunities for us to improve alerting systems, this will be wasted if communities are not ready to use them and are not confident in their protocols. To this end, we must ensure that alerting systems are reliable and secure. Security breaches in alerting infrastructure have become all too common; I'm sure many of you are familiar with the purported "zombie attack" back in early 2013, as well as a more recent trip-up involving popular radio personality Bobby Bones and the unauthenticated re-dissemination of an EAS test. Accordingly, the FCC convened a working group of the Communications Security, Reliability and Interoperability Council (otherwise known as CSRIC) to make recommendations on actions that can be taken to improve the security of the EAS. Having received their recommendations, we

must now work with alert providers to improve the confidentiality, integrity, and availability of alerts.

We at the Commission are working alongside you to advance this new alerting paradigm. The Commission currently has an Order on circulation that will evaluate the fixes to resolve operational issues uncovered by the November 2011 Nationwide EAS Test. The Bureau also continues to work on increasing the availability of the EAS to people who do not speak English as a primary language, and examining the extent to which the challenge of multilingual alerting can be addressed through the existing state EAS plan process. We plan to build on this foundation by integrating other systems, including Wireless Emergency Alerts, into the alerting exercise paradigm and improve the ease and availability of local managers to conduct relevant testing and exercise. We will work closely with all stakeholders to help ensure that communities are ready to respond to natural disasters and other emergencies through effective, community-initiated alerting.

Spectrum

Now let me turn briefly to public safety spectrum issues. One of the Commission's most important missions is to enhance public safety's ability to make effective use of allocated spectrum. We have been pursuing this mission on a number of fronts. First and foremost, we are working closely with FirstNet to support its efforts to launch the public safety broadband network in the 700 MHz

band. But we also recognize that the FirstNet network is still some years away, and we are therefore continuing to pursue significant initiatives in other parts of public safety's spectrum portfolio.

Perhaps one of the most significant, but relatively unheralded, accomplishments of the past year was the Commission's updating of the rules for the 700 MHz public safety narrowband spectrum. Since the completion of the DTV transition, demand for licensing and use of this band has been increasing steadily. But prior to the Commission's action last October, the technical rules governing the band were significantly outdated. The Commission has now updated those rules to enable use of newer technologies, and has opened up access to much-needed reserve channels in the band.

We are also finally nearing the long-awaited end of the 800 MHz rebanding process. In the non-border and Canadian border regions of the U.S., the vast majority of public safety licensees are now operating on their new channels, which affords them greater protection from interference as the rebanding program intended. We still have to complete the rebanding process in the Mexican border region, but the progress already made has also opened the door for the Commission to adopt a recent NPRM proposing to open up 800 MHz interstitial channels for licensing. This proposal is a good example of how we can re-use scarce spectrum capacity more efficiently.

Finally, let me suggest that you keep an eye on the 4.9 GHz band this coming year. The 4.9 GHz band is significant because it is the largest single band of contiguous spectrum (50 MHz) dedicated to public safety. It is also notable because while it has been allocated to public safety for over a decade, it is not heavily used in much of the country. In 2012, the Commission sought comment on ways to stimulate increased use of the band, including expanding eligibility to critical infrastructure entities and other commercial users, establishing more structured frequency coordination, and allowing aeronautical mobile use. In 2013, NPSTC proposed a revised band plan that would implement some of these changes. We are now working on a draft Further Notice proposal that we expect to incorporate elements of the NPSTC plan, as well as other proposals to encourage introduction of new technology that will support next-generation public safety applications. This might, for example, allow officials to incorporate public safety controlled WiFi or LTE-U technology into this band, should local officials feel it best fits their communications needs.

Overall, our goal in all these initiatives is to ensure that public safety has access to sufficient spectrum to meet its needs, but also that such spectrum – always a scarce resource – is optimized to ensure efficient and effective use. We believe the best way to do this is through rules that incentivize public safety to take

full advantage of technological innovation, efficiency, and flexibility to achieve its mission-critical goals

Cybersecurity

I'd like to close today with a brief discussion of the Commission's efforts in cybersecurity, a strong theme throughout our entire portfolio. Public safety is increasingly moving to IP-based systems which, on the one hand, can provide significantly enhanced functionalities and cost savings, but, on the other hand, brings 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 public safety communications are also a very attractive target for cyber threat actors.

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.

The FCC has long taken a collaborative approach to cybersecurity, working in partnership with private sector stakeholders through our federal advisory committees, including the Technical Advisory Committee (TAC) and the CSRIC. I want to applaud the work of CSRIC in this arena. CSRIC Working Group 4 will vote on its final report at a public meeting next week on application of the NIST Cybersecurity Framework to the communications sector. We look forward to reviewing their findings and hope to use them as a foundation for our next steps in cybersecurity. As commercial communications providers improve their ability to assess and mitigate cybersecurity risk, it will be important for federal, state, and local public safety communications professionals to develop the capacity to assess risk in the part of the information environment that they operate and maintain. To that end, the recently formed Task Force on Optimal PSAP Architecture includes a working group devoted to cybersecurity. It is led by APCO's own Jay English and is working hard to tailor the NIST Cybersecurity Risk Management Framework to PSAPs.

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. Indeed, cybersecurity is not an extra expense; it is as basic of a requirement in this networked world as paying the electric bill and should be an omnipresent consideration in all facets of public safety communications. Again, there is no reason for any one of us to "go it alone" when it comes to cybersecurity, and we at the Commission are here to help public safety communicators in any way we can.

Conclusion

In closing, I want to thank the executive leadership of APCO for hosting this event and for bringing this community together, but I also want to thank all of you for letting me speak with you today. We are just beginning down this path of the technology transitions and the improved functionalities that come with them. How we prepare for them, how we take advantage of the data they will unleash, and how we creatively, efficiently, and securely utilize new media is up to us. The Commission stands ready and willing to help in any way we can, and we hope that we can continue this dialogue as the technology transition continues. Together, we can securely and successfully implement IP-based networks and functionalities to better serve our communities and enhance emergency communications. Thank you.