Remarks of Rear Admiral (ret.) David Simpson

Chief, Public Safety and Homeland Security Bureau

California 911 Town Hall Meeting

Wednesday, October 5, 2016

-As Prepared for Delivery-

Thank you for inviting me to speak to you today.

As you well know, FCC Chairman Tom Wheeler has made public safety a priority. It is no coincidence that the three years of his tenure have been among 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.

Today, there are approximately 6,500 Public Safety Answering Points (PSAPs) in operation across the nation, which handle about 240 million 911 calls annually. As of year-end-2015, California itself had 450 PSAPs, 399 Primary and 51 Secondary, and last year you handled approximately 29 million 911 calls, 22.7 million of which were wireless 911 calls. That's approximately 12 percent of total 911 calls made in the U.S.!

But as you, the front line emergency response professionals, know better than anyone, in too many communities, the communications technology behind the 911 system is dangerously out of date. Chairman Wheeler has been very vocal about the urgent need to improve our 911 system. The recent events in Orlando, Louisiana, and too many other cities highlight the importance of 911 in times of crisis. PSAPs face constant challenges to maintain adequate funding for ongoing operations, and the

challenge is even greater to incorporate Next Generation capabilities and functions into their operations.

The Commission has taken action to improve the quality and accuracy of 911, and there is good news to report. We see industry is stepping up to many of the challenges, improving 911 location accuracy, supporting text-to-911, and generally investing to improve network reliability and resiliency.

We at the FCC are committed to doing everything in our power to help you make the current 911 system as strong as possible but to also encourage and support as rapid a transition as possible to Next Generation 911 (NG911).

Effective 911 service depends on our nation's 911 call centers. These PSAPs must have technology to receive and process calls quickly, accurately locate callers, and dispatch an appropriate response. The unfortunate fact is that 911, designed originally for analog voice, doesn't scale effortlessly to the advanced digital, wireless, and multimedia technology landscape. In too many communities, the PSAPs are relying on dangerously out-of-date technology, and the transition to NG911 – envisioned by Congress in 1999 when it established 911 as the national emergency number – has not started or is stalled. Resource-strapped local jurisdictions struggle to maintain existing 911 service, let alone to achieve Congress's NG911 vision.

Industry and many states, counties, and cities are working hard to address transition risk and achieve NG911 capabilities. Nearly 20 percent of U.S. counties now support text-to-911. Here in California, you have 39 text-capable PSAPs across the counties of San Bernardino, Los Angeles, Monterey, Contra Costa, and Riverside.

Many jurisdictions are building out their Emergency Services IP Networks – the basic backbone for NG911 in their communities. California is leading the way with its two ESInet projects – the Regional Integrated Next Generation project, supporting 21 PSAPS in the Los Angeles County and Pasadena areas, and the Mendocino County ESInet project, supporting the Mendocino County Sheriff, Ukiah Police Department and Willits Police Department. These are important projects to demonstrate how a network-based NG911 service will allow PSAPs the ability to take 911 calls at any workstation at any PSAP that is part of the ESInet project and allow the PSAPs to use policy-based routing to route call based upon static or dynamic rules. PSAPs throughout California should be paying close attention to the lessons learned from these implementations.

On a nationwide basis, however, these islands of progress are the exception, not the rule. Unless we find a way to help the nation's PSAPs overcome the funding, planning, and operational challenges they face as commercial communications networks evolve, NG911 will remain beyond the reach for much of the nation. Let me be clear on this point: 911 service quality will not stay where it is today, it will degrade if we don't invest in NG911.

As Chairman Wheeler has stated, Congress has the unique ability to accelerate the transition to NG911. A clear national call to action, with timely application of resources, would actually lower NG911 transition costs by shortening the transition period and enabling 911 authorities to retire costly legacy facilities more quickly. Chairman Wheeler has outlined three ways that Congress could help:

- *National NG911 Implementation Date with Matching Funds*: Currently, there is no national timetable or target date for completing the transition to NG911. Congress could establish a nationwide NG911 implementation date; for example, calling for completion of the transition by the end of 2020 and authorizing matching funds to help state and local communities achieve this goal. Congress can further jumpstart this effort by ensuring that federally run PSAPs and Emergency Operations Centers make achievement of NG911 capability a funding priority.
- *National 911 Map*: PSAPs are increasingly dependent on electronic maps for 911 routing and location, but the maps that they rely on should not end at the county or state line. Congress could authorize and fund the FCC, in collaboration with its federal partners at the Department of Transportation's National 911 Program Office, to create a national 911 map that would be available to every PSAP and would eliminate the seams between commercial communications network infrastructure and emergency response dispatch systems.
- *Cybersecurity Defenses for PSAPs*: PSAPs face the same cyber vulnerabilities that have proven so challenging to both government and commercial organizations, but most lack a cyber-trained workforce and the necessary tools for cyber defense. Congress could bring PSAP IP Networks under the protective umbrella of DHS's "EINSTEIN" program by funding the deployment of intrusion detection sensors for NG911 networks.

As part of the NG911 transition opportunity I just highlighted, I'd like to call on the California public safety communities represented here today to continue to help chart the path forward for NG911 in three specific areas: (1) closing the indoor location accuracy gap; (2) integrating NG911 with FirstNet and emergency alerting; and (3) developing public-safety-grade cybersecurity programs for PSAPs.

LOCATION ACCURACY

The Commission's 2015 Location Accuracy Report and Order 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 the Roadmap Agreement.

We are pleased to see the concrete progress being made to implement the requirements of the Order and the commitments made in the Roadmap. The location technology test bed was launched in August, and planning is well underway to develop the National Emergency Address Database (NEAD). Initial testing is being conducted in two stages: Stage 1 involves testing technologies currently deployed in carrier networks. This month, Stage 2 has commenced, enabling location technology vendors to test near-term emerging horizontal and vertical location technologies that are not yet deployed by the nationwide wireless carriers.

Next February, carriers will begin providing live 911 call data in six test cities, one of which is San Francisco, and elsewhere at PSAPs' request. Also due in February are carriers' implementation plans and progress reports as well as their Privacy and Security Plan for the NEAD. And then in April, just seven short months away, the first

horizontal location accuracy benchmarks require that service providers meet 50 meter accuracy or provide dispatchable location for 40 percent of calls.

But our rules – though a major step forward – represent a floor, not a ceiling. Working together, PSAPs and carriers have the potential to get well above the floor and a lot closer to the ceiling in providing accurate location information, but for that to happen, PSAPs will need to track 911 performance in their communities so that they can hold carriers accountable for service in local 911 "hotspots."

In addition to holding carriers accountable, PSAPs must hold themselves accountable as well. For example, dispatchable location data provided by the carriers from the National Emergency Address Database will be far more effective in jurisdictions where PSAPs have fully leveraged their own GIS data, and have compiled detailed information on the location and morphology of buildings, floor plans, and building diagrams.

Similarly, in order to make the most of improved location information provided by the carriers, PSAPs need complete, authoritative maps to assist with call locating and dispatching, and those maps should not end at the county or state line.

There have been too many tragic incidents where a 911 caller was not found in time because a PSAP lacked an accurate map that extended beyond its own jurisdictional borders. In December 2015, Kevin Vroome collapsed in his Wake County, North Carolina home with a heart attack, and his wife desperately called 911 from her cell phone and reported her exact location. The 911 call was answered by the neighboring Chatham County PSAP, which did not have mapping information to pinpoint the caller's location on the other side of the county line. Kevin Vroome was

reportedly 50 yards away from where the County's electronic map data stopped, and he died before help arrived.

The tragic examples of Kevin Vroome and others demonstrate how lack of the most basic coordination between jurisdictions can put the public at risk. We trust that PSAPs throughout California are working collaboratively with their neighbors to ensure that they are sharing critical geographic information with each other. Let's dedicate ourselves to making 2017 the year that we resolve the mapping issues and ensure that map providers include adjacent jurisdictions.

The Communications Security, Reliability, and Interoperability Council (CSRIC) V, an FCC advisory committee dedicated to providing recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications and public safety, recently completed work on two important location accuracy tasks.

In March, CSRIC adopted the Evolving 911 Services Working Group's report and recommendations pertaining to a top-to-bottom review of wireless service providers and PSAPs' Cell Sector Routing practices. The Council reviewed 51 existing, legacy standards and best practices from prior CSRIC Working Groups, Reports to Congress, PSAPs, NENA, and the FCC that directly or indirectly impact call routing/re-routing. It found that six best practices were valid and of continued relevance, but another six best practices required modification to make them relevant in the current 911 environment. The Council recommended a new best practice to optimize call routing/re-routing.

Of great interest to the PSAP community, particularly here in California, is the use of device-based location for initial call routing. In September, the Council voted to approve a report and recommendations on location-based routing methods that could potentially be used for wireless 911 call routing. Under current practice, a wireless 911 call is routed to a PSAP based on the originating cell sector that handles the call. Location technologies for wireless E911 and commercial location-based services have evolved and may provide a sufficiently accurate quick-fix to use for call routing. Provided location fixes are obtained in five seconds or less, location-based routing (LBR) for wireless 911 calls would allow for delivery of the call to the jurisdictionally appropriate PSAP, thereby reducing call transfers between PSAPs.

Working Group 1 identified and reviewed several location-based routing methods that could potentially be used for wireless 911 call routing. Each LBR method has its own characteristics and considerations. Among the Working Group's numerous recommendations is that the FCC work with device manufacturers, device operating system providers, and wireless service providers to assess the feasibility of enabling all devices used for static and nomadic purposes with the ability to validate if it has been moved and alert the network of its status. The Working Group found great merit in further study of device-based hybrids solutions, which are already moving the performance needle to locate wireless callers in challenging indoor environments. What we see with the CSRIC report is that technology is rapidly advancing and great improvements in location accuracy and 911 call routing are within sight.

INTEGRATING NG911 WITH FIRSTNET AND ALERTING

Let me turn from 911 location to the impact of the technology transition on public safety communications platforms that were previously stove-piped but are now converging and increasingly interdependent. The IP transition makes it possible but also imperative to integrate the NG911 system with other IP-based public safety communications platforms.

In August, the Commission adopted an Order and Notice of Proposed Rulemaking related to FirstNet. In the Order, the Commission provides a mechanism to facilitate the relocation of public safety narrowband incumbents currently operating on FirstNet's spectrum. In the Notice of Proposed Rulemaking, the Commission seeks comment on proposed procedures for administering the state opt-out process as provided under the Public Safety Spectrum Act, as well as on our implementation of the specific statutory standards by which the Commission is obligated to evaluate state opt-out applications. Those comments are due on October 21 and reply comments are due November 21.

FirstNet is in the process of selecting a bidder on its RFP and in due course will be developing its detailed network design and buildout plan. On July 19, the National Telecommunications and Information Administration (NTIA) released a version of guidelines for a state to use if it chooses to opt out of FirstNet's nationwide LTE broadband public safety communications network. The NTIA notice relates to NTIA review criteria, not to the FCC process. In general, states need to focus on how to implement FirstNet regardless of who runs the Radio Access Network.

Integration is particularly critical with respect to NG911 and FirstNet. This makes it important to accelerate the NG911 transition so that that we "bake in" integration

between FirstNet and NG911 as part of this initial design phase. If we can't develop NG911 on a parallel timeline with FirstNet, integrating them later in the process will be more costly and difficult.

At the same time that FirstNet is moving forward and we are focused on the NG911 transition, emergency alerting is also in the midst of a technology transition. In the past year, we have made significant strides towards a public safety communications model in which the "one-to-many" systems that support emergency alerts will enhance the 911 system's "many-to-one" capability. Our objective is nothing less than spurring the deployment of public safety communications platforms that are converged and interoperable so that information can pass across them seamlessly, reliably, and securely.

In this converging landscape, PSAPs, who field incoming emergency calls, should have the means of sending out critical information to the public through alerts and real-time photos and video to emergency responders. In August 2015, we held a workshop on how local emergency officials can leverage the use of alerting systems. Panelists supported the proposition that state and local emergency management offices that fully integrate alerting, 911, social media, and other emergency communications functions into an integrated whole are far more effective in notifying their communities about danger than those that silo these functions or do not use alerting at all.

There is an effective tool already available that local public safety officials can use for alerting. The Integrated Public Alert and Warning System, or IPAWS, maintained by the Federal Emergency Management Agency, is an integrated gateway through which authorized public safety entities, including PSAPs, can initiate alerts.

The alerts may be sent through the Emergency Alert System (EAS), which delivers the information via radio, television, and other media, and/or Wireless Emergency Alerts (WEA), which are delivered to consumers' cell phones. An increasing number of PSAPs across the country are taking advantage of this important information dissemination resource, but more needs to be done. As of August, 41 California organizations had been certified by FEMA to act as Alerting Authorities, including 32 of the state's 58 counties. Another seven California authorities' applications are in progress, including four military installations (Camp Roberts Maneuver Training Center, Fort Hunter Liggett, US Army Garrison Presidio of Monterey, and USAG Fort Irwin). I encourage state, local, tribal and territorial emergency managers to consider supporting direct participation in IPAWS from their PSAPs. It is not difficult to obtain, and some PSAPs have already done so.

We know that PSAPs play an integral part in emergency response. The transcript of the 911 call the Orlando Pulse nightclub shooter made during his June 12 rampage inside the club, illustrates how deeply involved PSAPs and 911 call takers can become in a crisis. It is not difficult to imagine that PSAPs working in an IP environment will (1) manage the flow of information to and from the scene of an emergency, (2) help to de-escalate an emergency by warning the public; and (3) enhance situational awareness of local communities and first responders. In the IP world, PSAPs should be able to seamlessly move critical information directly to and from the public and first responders during emergencies.

We strongly encourage State Single Points of Contact (SPOCs) to connect now with Statewide Interoperability Coordinators (SWICS), State 911 Administrators, and

State Emergency Communications Committees (SECCs) to ensure that everyone is rowing in the same direction and that NG911 is integrated with FirstNet and emergency alerting.

CYBERSECURITY IN OUR 911 CALL CENTERS

Finally, I'd like to turn to the issue of cybersecurity and encourage you to redouble your efforts to promote cybersecurity in your PSAPs and Emergency Operations Centers (EOCs).

One of the most important missions of the FCC is to ensure our nation's commercial communications infrastructure supports public safety and national security. The vulnerability of advanced telecommunications networks to physical and cyber-attack is not lost upon us. We have and will continue to work closely with industry and our agency partners to identify, mitigate and, where possible, reduce cybersecurity risk.

Cybersecurity principles – availability, integrity, and confidentiality – are now routinely incorporated in our engagement with industry. Our advisory committees are doing important work tackling tough cybersecurity issues for current and future networks. Our approach is to have communication providers and their industry partners lead while the FCC brings useful assistance and transparency to ensure that this effort benefits from early peer review and serves to accelerate development of secure IP-networks capable of supporting the advanced services promised by NG911 and future 5G devices and services.

As PSAPs and EOCs move to IP-based platforms, they will benefit from significantly enhanced functionalities and reliability, but they must also be prepared to contend with an expanded threat landscape. We already know that public safety

communications are an attractive target for cyber threat actors. In April 2016, the Department of Justice and DHS issued a report highlighting the fact that local law enforcement agencies have been victims of ransomware attacks. This should be a wake-up call for all PSAPs and public safety agencies to back-up their files off-site so they are not at risk of losing essential data or having to pay ransom to recover it.

Public safety entities relying on IP-based networks also need to "bake in" public-safety-grade cybersecurity programs to their strategic planning going forward. While the task may seem daunting, we stand ready to help. We have long advocated a collaborative approach to cybersecurity, working in partnership with Federal partners, public safety organizations, and private-sector stakeholders through our federal advisory committees.

To help develop cybersecurity strategies specifically tailored to PSAPs, we also made cybersecurity a major focus of the Task Force on Optimal PSAP Architecture (TFOPA). TFOPA's Working Group 1 developed a key set of recommendations, which were incorporated into TFOPA's consolidated report, to help PSAPs protect themselves against cyber threats as they transition from the circuit-switched world to the IP world.

Specifically, TFOPA recommended establishing Emergency Communications Cybersecurity Centers (EC^3) to help protect PSAPs against cyber-attack. The intent of the EC^3 concept is to create a centralized function for securing NG911 networks and systems. PSAPs must be able to rapidly perceive threats and share information with the Federal Government, and the Federal Government must be able to share threat indicators with PSAPs in order for local PSAPs to take mitigation steps.

To facilitate these information flows, the EC^3 model begins at the local level with the Originating Service Provider (OSP) and NG911 Core Services elements, encompasses the ESInet IP Transport network within and between disparate PSAPs, and provides for centralized monitoring of call statistics, system health, anomaly detection, data sharing, mitigation and recovery while still allowing local agencies to maintain local control of day-to-day operations within their specific PSAPs. The flow of information from local PSAPs continues through the state or regional EC^3, which would interface directly with trusted partners at the Federal level, such as the Multistate Information Sharing and Analysis Center (MS-ISAC) and the Department of Homeland Security's National Cybersecurity and Communications Integration Center (DHS-NCCIC). These trusted partners would then send information back through the EC^3 to the local PSAPs to help facilitate a response to a cyber-attack.

By centralizing cybersecurity under the EC^3 model, PSAPs will be able to save costs and will be better equipped to identify, protect, detect, respond and recover from cyber-attacks. The benefits of this approach also can readily be extended beyond PSAPs EOCs and potentially FirstNet. And over the longer term, EC^3 provides an opportunity to can capitalize on technological advances in machine-to-machine learning to enhance our first responders' abilities to manage cybersecurity risks.

Since the issuance of the TFOPA report in January, Working Group 1 has been tasked to more fully develop the EC^3 concept and to conduct an in-depth study of this model, including what operations and costs might look like if established on the local, regional, or state level; alternative solutions that achieve the same end goal and their associated costs; and specific opportunities for the EC^3 to integrate efficiently with the

NCCIC and MS-ISAC models. A critical aspect of this work will be recommendations with respect to how identity credentialing and access management should be addressed in the EC^3 environment. They will present their report and recommendations to the Task Force later this year.

CONCLUSION

In closing, I want to thank Representative Torres 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 continuing down this path of the technology transition 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 communications platforms 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.