Prepared Remarks of Admiral (ret.) David Simpson,

Public Safety and Homeland Security Bureau (PSHSB) Chief

Preservation of 911 Accountability

NARUC 2014 Summer Meeting

Dallas, Texas

July 16, 2014

Good afternoon. I'd like to thank you for having me here in Dallas for the NARUC summer meeting.

An essential mission of the FCC is to ensure that the Nation's communications infrastructure is secure and reliable. We take this obligation seriously, and recognize that we serve Americans in every part of the country – in every one of the states you serve. We cannot do this, however, without the efforts and partnership of state and local regulators. You are the "cops on the beat," and we rely on your eyes and ears and the familiarity you have with your communities and local providers. You also help ensure the resiliency of our nation's communications infrastructure, including access to 911. In maintaining the security and reliability of the Nation's communications infrastructure, the federal-state partnership is crucial, as has been shown time and again, over many decades. By working together, we promote and protect the public safety of all Americans. Now, with the technological changes that are underway, we must take that partnership to a new level of efficiency and effectiveness. Lives depend on it.

Advancements in communications have bestowed amazing benefits on us all, including the security of knowing that public safety assistance is simply a 911 call away and that broadband connections deliver content and communications in endless variety, quite literally, to nearly everywhere we may roam. But with brilliant innovation comes a new set of challenges: ensuring that public safety authorities are accessible in times of crisis, creating a safe communications environment that enables us to conduct business without fear that our personal information will be stolen, and ensuring that new IP-based networks are reliable and resilient. As technology advances create new and unforeseen seams, we need to work together with the states to ensure that accountability across jurisdictions is not diluted. What was once local can quickly become interstate, or even global, and what was once global can just as quickly become local. Technology transitions change relationships, but together our combined jurisdiction is clear, and we need to adjust our governance to make that clear as well.

April 2014 Multi-State 911 Outage

Let me begin with a prominent example that you are all quite familiar with – many of you, because it affected your state directly. Earlier this year, we experienced one of the most widespread and significant 911 outages to date. On April 9th and 10th, a multi-state 911 outage occurred in IP-based facilities used to support delivery of 911 calls in Washington state, as well as portions of California, Pennsylvania, Minnesota, Florida, North Carolina, and South Carolina. According to preliminary reports, in Washington alone over forty-five hundred 911 calls to "PSAPs," or 911 call centers, did not get through during a six-hour period beginning just before midnight on April 9th. This outage is a clear example of the inherent risk in technology transitions. It is symptomatic of larger trends in communications reliability and resiliency, and it is a warning to us all that we do not have the luxury of time to address issues as networks change under our feet. These issues need to be addressed now. We cannot afford to let another outage, let alone a multi-state outage like this, happen again. We cannot afford another instance of failure when it comes to the safety and lives of the American public.

As you all know, the FCC opened a public docket and invited all interested parties to provide information concerning the causes, effects, and implications of this multi-state outage. What some of those comments have revealed is that the outage was not caused by failures of the primary provider's network, but by a technical problem in third-party vendor equipment. A simple, technical problem, in a system outside of the 911 service provider's line of sight prevented the 911 network from properly processing emergency calls in multiple states for about six hours. Even though this outage was not caused by failures or malfunctions of the primary carrier's network, it demonstrates a need for close coordination between critical service providers in the end-to-end 911 chain. While there is a decent understanding of the technical interdependencies for links in the end-to-end chain, we put public safety at risk where there is not a shared operational picture, common situational awareness, or a clearly designated "tier one"-level operations center empowered to coordinate rapid localization of problems discovered by other providers. This, in turn, negatively impacts identification of backup alternatives and rapid restoration of full functionality. We were lucky this time. Still, while there were superb individual contributions to the recovery from this outage, the information we have gathered thus far indicates that a lack of common situational awareness created widespread local confusion, which could have resulted in failures to effectively meet the emergency needs of citizens and communities.

The FCC and our state counterparts have end-to-end oversight responsibility for 911. The carriers under that governance structure have the responsibility to build end-to-end resiliency and reliability into the 911 communications infrastructure and ensure that it is sustained – regardless of which portions are being handled by whom, and regardless of the legacy or next-generation nature of the underlying technology. Together, collectively, we have the legal authority and the public imperative to oversee each of the increasingly complex component pieces of the 911 ecosystem, and to make sure that the providers within our

respective jurisdictions are held accountable for proactively addressing the enhanced need for reliability with respect to 911.

Don't get me wrong, the increased innovation and enhanced competition that we are seeing in the 911 ecosystem have a tremendous potential to enhance the functionality and utility of 911. But these transitions must be managed in a manner that at the very least safeguards, and preferably improves, the current reliability of 911. This must be a basic requirement for all providers operating in this space, whether old or new, and is a trust that we must uphold.

Let me pause here and be very clear: Incumbent providers that have taken a responsibility for making 911 work have undertaken a public trust that cannot be shirked. Improved functionality is great, but decreasing 911 reliability by not effectively addressing new threats introduced through that new functionality is not acceptable. It will never be acceptable to tell an elderly woman living alone that she can't connect to 911 because of "innovation in the cloud" or a new business model, or because a new communications function has superseded carrier responsibility. So, changes in the way an incumbent carrier or any other critical provider carries out 911 responsibilities must embody the following principles: First, do no harm to 911. Second, change must be coordinated with the FCC and state commissions. Third, any new elements of the end-to-end service must have confirmed accountability safeguards and appropriate regulatory oversight to ensure that their introduction does not degrade 911 availability.

As 911 functionalities migrate to the cloud, and as traditional 911 service providers seek to evolve or exit lines of business making way for new providers in this space, we must ensure that the transition process is open and transparent, so that we can assess the accountability of both traditional and new providers for 911 network integrity. We must also identify and close accountability gaps that affect our ability to address 911 reliability issues throughout any transition. We must take these steps before a failure occurs. When we do this best, it facilitates on-ramps for innovation by providing clarity around our expectations. Lack of transparency – and more importantly, a lack of clear agreement on substantive changes – among stakeholders and regulators with respect to the integrity of the elements of the 911 infrastructure is not acceptable. Seeking to shift responsibility for failures to third parties does not make those failures acceptable and does not absolve incumbent carriers of their responsibilities. And just as importantly, this shifting of risk and responsibility will not promote systemic improvements that go beyond a single provider.

Together with our state partners, we have clear authority to address these concerns, and to ensure that transitions of critical 911 infrastructure and services are managed appropriately, seamlessly, and in a manner that preserves the integrity of the system. We cannot wait until the system fails to consider these crucial questions – by then it will be too late, and the stakes are too high. To the extent that the carriers or any player in the 911 ecosystem perceives that there are regulatory or oversight gaps, we need to fill those gaps, and we will fill them with your assistance.

In the coming months, we intend to explore these issues, and to consider the means to ensure each participant in the 911 ecosystem is fully accountable to its individual responsibilities and fulfills its public trust to support the fundamental value of reliable 911 access. But let me

tell you the bottom line: Carriers will be fully accountable. Yes, it is an ecosystem, but the buck stops with the carrier. The transition to IP does not – and will not – absolve providers' responsibilities for ensuring that 911 functions as our citizens expect it to function. While providers are entitled to make decisions about their businesses, they are not entitled to do so in a manner that endangers 911 or puts the public at risk. They are also not entitled to do so without consultation, without complete transparency among stakeholders about who is accountable for what element of the service, or in a manner that puts other stakeholders in the dark with respect to the functioning of the combined network.

These issues are critical because our entire country relies on 911 whenever there is an emergency. It is the first telephone number American children learn. It is the number that automatically pops into all Americans' heads in an emergency. Regardless of visibility, regardless of responsibility, regardless of accountability, 911 has to be as close to perfect as we can make it. It has to work in times of crisis regardless of whatever else is going down, whatever else is failing. It has to be fail-safe, and it is up to all of us – the local, state and federal regulators – to ensure in cooperation with industry and the public safety community that this goal is achieved. Access to 911 is a core value in our society, a service that must be maintained even as technology evolves and the new replaces the old. With one foot in the old world of PSTN infrastructure and one in the new, 911 has an inherent interoperability challenge. We cannot let un-governed or under-governed links in the chain prevent proper oversight for what needs to be the highest achievable availability end-to-end.

We also do not want to freeze technology advances as a backwards-looking way to solve this problem, and we cannot "wish away" PSTN-to-IP interface challenges. To ensure that the transition continues to be innovation-driven, 911 service providers and federal, state, and local authorities charged with governance responsibility must communicate better to make the full transition to all-IP networks as seamless as possible and to prevent more failures like the one that occurred this past April. NG911's IP-based architecture is built with resiliency in mind, and the use of IP means that in a well-designed network, calls can be rerouted seamlessly to an alternate PSAP without losing information about the call. Not only do we expect NG911 be more resilient than traditional 911, we also believe that it will ultimately allow for more efficient public safety operations. So getting on with the transition is part of the answer. I'm mindful, however, that while the Advanced Research Projects Agency, or ARPA, decades ago designed Internet Protocol networks to radically improve the survivability of critical communications by building in mesh routing opportunities, this did not mean that communications availability challenges ended. We have learned since – sometimes the hard way – that essential elements of connectivity pass through every layer of the Open Systems Interconnection, or OSI, model of network architecture. From transport to application to session, all of these layers must work. Failing to account for resiliency of design in every layer can result in lower reliability with newer technology, and implementation of "lowest cost" IP designs can negate the resiliency gains in other parts of the end-to-end network. We must ensure that all-IP networks are secure, reliable, and resilient in implementation, as well as in design.

CSRIC

So how does the FCC approach these issues? Taking a step back from the 911 discussion, the FCC relies on the Communications Security, Reliability, and Interoperability

Council, or CSRIC, to help us fulfill these broad objectives. CSRIC is a formal advisory committee for the FCC, comprised of experts from the private and public sectors. Its mission is to provide recommendations to the FCC to safeguard, among other things, the security and reliability of our communications systems, including communications networks, media delivery systems, and public safety services. NARUC is a CSRIC participant, and I encourage you to be vocal on that council, particularly when it comes to determining the sufficiency, from your states' perspective, of an industry-proposed best practice.

Cybersecurity

CSRIC has been at the forefront of the FCC's efforts to improve the security of the Nation's communications networks through appropriate measures to manage cybersecurity risk. In 2011, CSRIC III completed recommendations for voluntary measures pertaining to Internet domain name security, route hijacking, and an Anti-Bot Code of Conduct to reduce the incidence of DDoS attacks. This was important foundational work. These recommendations, if implemented broadly, will "harden" our nation's communications backbone against cyber threats with potentially wide-scale industry implications. We will shortly be asking CSRIC participants to update us on their progress implementing these measures.

The last set of comprehensive cybersecurity best practices was recommended by CSRIC in March 2011. In the time that has passed, cybersecurity threats have become more pronounced and visible, and our nation's cybersecurity policy has evolved. In 2013 the FCC asked CSRIC to evaluate the most critical existing cybersecurity best practices and to determine how best to improve them to account for changes in cybersecurity practice and the threat landscape. More importantly, we asked CSRIC to harmonize these best practices with the recently released NIST Cybersecurity Framework and to explore aspects of a business environment in which cybersecurity-specific practices will be effective, efficient, and sustainable.

The NIST Framework is designed to give organizations in sectors throughout the economy the tools to manage cybersecurity risks themselves – in a measurable and accountable way – without the need for issuing mandatory regulations. CSRIC's work will help communications providers to "operationalize" the Framework by using updated cybersecurity best practices and risk management methods to evaluate and improve their cybersecurity posture, and communicate needs and expectations internally and with external stakeholders. These best practices can be of particular assistance to small to mid -sized telecom companies, who may not have the resources or know-how to formulate detailed cyber practices on their own. The bottom line on this is that the solutions to managing and mitigating cyber risk must be found as close as possible to the owner-operator level. We cannot dictate from Washington how companies should secure their networks. Instead, together – federal and state – we must empower them to do so themselves, and then help give them the information and tools to make it happen. As in the specific case of 911 reliability, securing our networks more broadly will take a new level of federal-state-private sector partnership.

The implementation of measurable, accountable cyber risk management best practices is crucial to commercial networks already transitioning to an all-IP infrastructure. Like commercial networks, public safety will face similar challenges as 911 systems migrate to NG911 and public safety radio increasingly relies on IP-based technology. Public safety entities

should not wait to address cybersecurity issues during, or at the end of, this transition. Rather they should begin now to develop the identity management, credentialing, priority access, and any other protocols that are necessary to create a secure public safety network. Regardless of the final decisions on network architecture, undertaking this exercise will give all public safety entities better visibility into their cyber risk profile. One thing is certain, if a public safety entity fails to plan now, critical decisions will eventually be made for them rather than by them. And that is not the best answer to this challenge. We need proactive management and mitigation of risk, not reactive response to problems after they have occurred.

The FCC wants to, and needs to, work closely with NARUC, with the state and local regulators, so we don't leave gaps in awareness and oversight. For instance, without access to information on changes in the cyber risk environment for a provider, federal and state governments cannot effectively perform their oversight roles. The current system of information reporting on communications resilience provides neither governments nor industry stakeholders with the reliable situational awareness they need to address emerging cyber threats effectively. The FCC will work with stakeholders to catalyze the information sharing process and the quality of the information it produces.

Measuring and evaluating this cyber risk information is very hard. Unlike financial risk, for which we have several centuries of quantified data on which to draw, quantifying risks to our communications networks is relatively immature. But that doesn't mean we just give up and decide it is too hard to do. There are some solid ideas that are emerging from our dialog with communications providers and other commercial entities that have begun to consider how they will measure these risks.

In short, the process is to identify the cyber risk space, develop internal controls to mitigate risk, assess implementation, and monitor effects. This is how enterprise risk management has always been done, across all types of risks that companies face, and now we need to apply this to cyber risk management in the communications sector and to our public safety entities and networks. To quote FCC Chairman Wheeler, "[c]ompanies must have the capacity to assure themselves, their shareholders and boards – and their nation – of the sufficiency of their own cyber risk management practices. These risk assessment approaches will undoubtedly differ company by company. But regardless of the specific approach a company might choose, it is crucial that companies develop methodologies that give them a meaningful understanding of their risk exposure and risk management posture that can be communicated internally and externally."

Chairman Wheeler's remarks apply to PSAPS and other public safety entities as well. Importantly, those of you here today, the state and local regulators of NARUC, are in the best position to encourage public safety entities to review their weaknesses and assess their cyber vulnerabilities and risk mitigation practices. You also play a key role in implementation of the NIST Framework at the state and local level. This will facilitate improved engagement with the private sector and provide an end-to-end assessment of cyber risk to public safety communications. Indeed, cybersecurity means much more than just securing communications networks. We also need to be thinking about the cyber vulnerabilities of communities' public safety. One single hacker could pose a major public safety hazard. PSAPs regularly experience

denial-of-service attacks, spoofing, and other cyber events that have the potential to prevent a PSAP from being able to receive and respond to emergency calls.

Now of course, like many things, the "devil" is in the details. I would like to round out this discussion by coming back to three key areas for public safety communications where our work with the states is critical: (1) emergency alerting, (2) 911, and (3) FirstNet. In all of these areas, together we need to demand proactive steps by the entities that we oversee to ensure that these crucial communications functions operate reliably and effectively. And to do so – I'll say it again – we need to take our federal-state cooperation to a new level.

Emergency Alerting

First, we must protect public safety through emergency alerting systems like the long-standing and well known Emergency Alert System, or EAS, and the newer Wireless Emergency Alerts, or WEA.

As you all know, EAS is a national public warning system that replaced the Emergency Broadcast System in the mid-1990s. EAS is the distribution pathway that sends warnings via broadcast, cable, satellite, and IP television services, such as U-Verse and FiOS. EAS may be used by state and local authorities, in cooperation with the broadcasters and other EAS participants, to deliver important emergency information, such as weather information, AMBER Alerts, and local incident information targeted to specific areas. EAS also requires broadcasters, satellite digital audio service and direct broadcast satellite providers, cable television systems, and wireless cable systems to provide the President with communications capability to address the American people within 10 minutes during a national emergency. EAS is an added layer of resiliency to the suite of available emergency communication tools.

Communications systems of all kinds, including those that provide vital public safety services, have always been the target of actors intent on malice or disruption. EAS was recently attacked. In 2013, a hacker obtained unauthorized remote entry via the internet into EAS equipment in California, Montana, Utah, Michigan, and New Mexico. This attack transmitted a false alert that "zombies" were rising from the grave. We are working through CSRIC to close the cyber readiness gaps that led to this incident.

WEA is a newer public safety alert system that allows customers of participating wireless carriers to receive geographically-targeted, text-like messages warning them of imminent threats to safety in their area. Alerts from WEA cover three types of critical emergency situations: alerts issued by the President; alerts involving imminent threats to safety or life; and AMBER Alerts. WEA enables government officials to target emergency alerts to specific geographic areas. Through cell broadcast technology, we can now geo-target WEA alerts to select audiences so that only phones in the affected area receive alerts.

Wireless companies volunteer to participate in WEA, which is the result of a unique public/private partnership between the FCC, FEMA, and the wireless industry to enhance public safety. While this is a tremendous capability, I think we have only scratched the surface of capabilities for the geo-targeted employment of WEA. In many jurisdictions, input into alerting

has not become an "on call" ready resource for PSAPs – but it should. This is a challenge we should work to tackle together.

Text-to-911

Second, back to 911 – and specifically to text-to-911 capabilities. As we transition our emergency response architecture to NG911, in addition to the efforts of CSRIC, there are other ongoing initiatives and proposals that will help ensure the safety of the American public in the interim. While we at the FCC are focused on facilitating the transition to an all-IP environment, we remain fully committed to ensuring that core values, including public safety, are protected in the current communications environment. In order to accomplish this, we need to examine and respond to how our world functions today. In times of emergency, consumers expect to be able to reach 911 emergency services using whatever means of communication are most familiar to them and most easily utilized. Increasingly, that means text messaging.

As a nation, we send and receive almost 6 billion text messages a day. In certain circumstances, such as domestic violence or kidnapping situations, or when faced with network congestion, texting 911 may be the only practical way to get help. In almost all circumstances for people who are deaf or hard-of-hearing, texting is the primary means for reaching out for emergency assistance. Today, 91 percent of American adults own a cell phone, and 81 percent of cell phone owners use their phones to send or receive text messages. And survey data suggests that over 85 percent of people with disabilities also use text to communicate. But, as hard as it may be to believe in 2014, most Americans still can't text 911 and receive help.

This January, the FCC adopted a Policy Statement that all text providers should support text-to-911 and a Further Notice that proposes this be accomplished by the end of 2014. And, in fact, all four of our nationwide wireless carriers recently reported to the FCC that they have already met the commitment to be ready to deliver text-to-911 to any requesting PSAP within their service territories.

However, making text-to-911 a reality by the end of 2014 is not solely dependent on the actions of communications providers. It will require action on the part of PSAPs as well. The unfortunate truth is that, on the whole, PSAPs are not where they should be and need to be on text-to-911. It has been more than a year since the FCC secured a commitment from wireless carriers serving 90 percent of Americans to deploy text-to-911 by 2014. Yet today, only a small fraction of PSAPs support text-to-911. While we have seen encouraging recent signs of increased PSAP implementation of text, the fact remains that most PSAPs have yet to move forward on this crucial step. We are asking you, the state and local regulators, to help us push forward this agenda with your PSAPs and their funding bodies. Let's take this step together and make text-to-911 a reality across our great nation.

911 Location Accuracy

Another 911-related step we have recently taken, with the objective of continuing to protect the American public while we are still operating within the existing 911 architecture, was the adoption in February of a Further Notice of Proposed Rulemaking to modify our E-911 location accuracy rules to reflect the new realities of the ever-increasing mobile world. Our

E911 location accuracy rules were originally written when wireless phones were a secondary means of communication, and were mostly used outside. Today, more and more consumers use wireless phones as their primary means of communication and more and more 911 calls are coming from wireless phones, from inside residences and office buildings and businesses.

Our proposals to address this new reality are simple – when wireless customers call 911, location information must be delivered to the PSAP with sufficient accuracy to support successful, timely dispatch of first responders regardless of whether the call is made from inside a 50-story high-rise or outside at a public park. Consumers already have that expectation when it comes to the commercial apps they use every day. If Google Maps can find them in a mall within a couple of meters, 911 should be able to find them, too. I realize that I've glossed over significant parts of the technical challenge at this stage. However, it is not the technology that is lacking, but leadership within the sector to integrate proven technologies into this ecosystem. I expect the FCC to move quickly to adopt rules once the record on this proceeding is complete.

The FCC encourages and welcomes your input on this important issue, as you are closer to the folks who operate these systems and better understand possible local obstacles or impediments and how to best get around them. Together, let's improve our first responders' ability to reach people who need help.

FirstNet

Finally, FirstNet: The First Responder Network Authority, known more commonly as FirstNet, is the entity licensed to establish a nationwide public safety broadband network. FirstNet is tasked with establishing and overseeing a nationwide, interoperable public safety broadband network, which is no small task. Everyone in this room knows the first thing it's going to take to get FirstNet off the ground is cash. Congress has targeted $7 billion in long-term funding for FirstNet. This funding will come from the FCC's auction of wireless spectrum. These auctions will provide FirstNet with the funding it needs to build out and fill the gap identified by the 9/11 Commission over a decade ago. We do need to keep in mind that this is a complicated process. There are a lot of moving parts, and there are places where states and localities can look to themselves to make more efficient use of scarce resources.

FirstNet has stated that it plans to conduct its first consultation meetings with states and territories beginning in the next few weeks (late July). This, therefore, is the best time for states and localities to review and discuss ways to address the challenges and costs of both FirstNet and NG911.

This is an opportunity, during the planning stages of both public-safety initiatives, to make efficient use of scarce resources. FirstNet will need a significant amount of bandwidth to operate, which can only be provided by broadband networks. Likewise, the ESINets which will support NG911 will require bandwidth to support video and a number of other media, which means we are going to depend on secure broadband networks. While these two networks are each self-contained, and will have to be built separately as they do separate things to support different areas, they can share underlying infrastructure. Because FirstNet and the ESINets will incur significant operational expenses, due largely to the amount of bandwidth and backhaul that will be required to run them, the more that these two services can utilize the same infrastructure,

personnel, and services, the more we will be able to mitigate expenses and improve performance. The same principle applies to the credentialing and identity management processes necessary to access these networks, which will be far more secure and efficient if shared functions are coordinated. Thus, there is a key opportunity for convergence in the build-out of FirstNet and the deployment of ESINets that provide NG911, but this benefit can only be achieved through cooperative planning.

Once again, we need proactive stakeholders and effective collaboration between all the players in the system. Let's make it happen, together.

Conclusion

We know that we should avoid imposing "one-size-fits-all" rules when the telecommunications infrastructure – and our nation itself, with all of the states and communities you represent – is diverse and dynamic, and when carriers and public safety entities and different states and local communities need the flexibly to respond to each situation in the way that best suits their particular circumstances. I want you to hear from me that we at the FCC know that state and local officials are often in a better position to effectively address situations with their own PSAPs and with their own public safety providers. We also know we need to work in concert with our state and local partners to accomplish all of the tasks we have before us as we move our communications and public safety functions into the new world of IP technology.

With all of that said, the FCC remains strongly committed to continuity of effective governance for public safety communications, both today and in the future – particularly as new IP-based communications networks change what were once purely local concerns into highly complex systems that span multiple jurisdictions or even the entire nation. In that respect, let me end where I began and emphasize again the critical importance of a cooperative, careful and vigilant approach to securing the reliability of the end-to-end 911 ecosystem. If we can solve that problem together, then we can solve the others too. Let's develop a model for federal-state-local-stakeholder responsibility and accountability in end-to-end 911 that can serve as a model for all of these public safety communications challenges in an IP-based future.

We each have our roles to play in asserting the authority we already possess to hold accountable those providers that support this critical national infrastructure. We cannot do this alone – and we do not want to do this alone. The states – you all – are essential partners with unique governance capabilities and authority. Let's work together to implement effective and efficient governance mechanisms for the all-IP environment, and to keep our people safe. They are counting on us.