NPSTC
National Public Safety Telecommunications Council

National Public Safety Telecommunications Council (NPSTC)
Full NPSTC Meeting
Office of the Chief Technology Officer (OCTO), Washington, D.C.
September 6, 2017

Welcome and Opening, Ralph Haller, NPSTC Chair. Mr. Haller called the meeting to order at 8:30 a.m. EDT. Participants on the phone were asked to send a record of their attendance to Attend@npstc.org. A quorum was present. Mr. Haller thanked OCTO for the use of their facility and Mike Corey, American Radio Relay League (ARRL), for transporting the audio visual equipment. Mr. Haller welcomed Tom Gallagher, Chief Executive Officer, ARRL, to the meeting. He asked for a moment of silence to honor the first responders and those affected by Hurricane Harvey. Lloyd Mitchell, National Association of State Foresters (NASF), was not present at the meeting as he had been deployed to Houston to assist in operations there. Jason Matthews, Vice Chair, Interoperability Committee, was also preparing for Hurricane Irma, which was forecast to head for Florida.

Federal Partners Update

Department of Homeland Security (DHS), Office of Emergency Communications (OEC), Jim Downes, Federal Partnership for Interoperable Communications (FPIC) Manager. Mr. Downes, reporting for Adrienne Roughgarden, provided an update on OEC activities. The Communications Unit Working Group at OEC has agreed on a new federated governance model to identify developing solutions for improved communications. The group evaluated options for a new and expanded ICS structure that would better reflect Communications Unit Leader (COML) responsibilities. The Communications Unit (COMU) mission statement, COMU 2.0, may include strategies to transition from an LMR platform to support of integrated multi platforms for coordinated response. The group held a conference call in August, where it developed goals, recognized instructor requirements, and reviewed a workshop proposal for instructors.

OEC is waiting for the Office of Personnel Management (OPM) approval to release the SAFECOM nationwide communications baseline survey, which will inform the development of the 2019 National Communications Plan. Based on results from the Border Interoperability Demonstration Project (BIDP), OEC developed best practices for rural and urban interoperability. The Rural Emergency Medicine Communications Demonstration grant continues to make progress; 475 individuals have completed training, and 676 have completed the program since its inception.

OEC is considering enhancing Statewide Communications Interoperability Plan (SCIP) workshops based on feedback from practitioners and from the National Governors Association (NGA) Policy Academy. The program will be expanded to include broadband, LMR sustainment, NG 911, and the use of alerts for warning systems. Stakeholders have been willing to share information and needs. OEC is updating the 2018 Technical Assistance (TA) guide. Regional coordinators have received a draft and been encouraged to share the guide with their SWICs.

OEC printed and mailed new Government Emergency Telecommunications Service (GETS) cards. The new card is simpler to use with clear instructions for toll-free dialing. Registrations for the program in June were up about 20 percent due to requests related to the safety of expected large crowds for the solar eclipse.

The CANUS team has been working with Canadian counterparts to host a September 20 webinar. The webinar will focus on spectrum management Above Line A and NG911 coordination. OEC continues to support the resilience experiment, which will be held in Bellingham, WA, this year. The Southwest Border Communications Working Group was scheduled to meet next week in Waco, TX, but that meeting has been canceled due to the hurricane.

OEC plans to become more involved in a number of tribal events and will present at the National Tribal Emergency Management Council in California and at the National Congress of American Indians in Norman, OK.

Eddie Reyes, International Association of Chiefs of Police (IACP), commented on the changes in the COMU program. These changes have been generated by the advent of FirstNet and the Internet of Things (IoT), which will require expanded knowledge of these new applications and technology.

Department of Homeland Security (DHS), Science and Technology (S&T), First Responders Group (FRG), Sridhar Kowdley, Program Manager. Mr. Kowdley reported on the recent 2017 First Responder Electronic Jamming Event. He recognized OEC and Chris Kindelspire for their assistance in making the event a success. The First Responder Electronic Jamming Exercise initiative focused on conventional spectrum interference against public safety and law enforcement communications systems. The 2016 and 2017 First Responder Electronic Jamming Exercises focused on illegal commercial-grade jammers that are bought online and illegally imported. Testing examined how jammers impact public safety communications systems and a first responder's ability to complete the mission. Impacted bands included GPS, cellular, land mobile radio (federal, state and local frequencies), Wi-Fi, Bluetooth, over the air TV, etc.

The goals of this exercise were to help federal, state, and local public safety and law enforcement recognize, respond to, report, and resolve jamming incidents and to better understand the volume and severity of the threat through increased awareness and analysis of reported jamming incidents. The end goal is more resilient communications and critical infrastructure for federal, state, and local partners and greater understanding of spectrum threats.

In 2016, the exercise occurred in a live-jamming environment at White Sands Missile Range. Participants tested first responder communications systems against commercial jamming; anti-jamming technologies against commercial jamming; Unmanned Aircraft Systems (UAS) against complex GPS and commercial jamming; and fixed timing receivers against complex GPS and commercial jamming.

The 2016 Exercise defined how jamming can disrupt first responder communications; next, DHS evaluated solutions to increase resiliency during the 2017 First Responder Electronic Jamming Exercise. JAMX 2017 was a very successful event with participation from 260 primary participants and an

additional 29 VIPs. All participants benefitted from participation and were able to collect data to understand the impact of illegal, commercial-grade jammers. Initial results suggest that several of the tactics were successful at mitigating the impact of jamming under specific conditions. Final results will be determined after analysis and will be used to create best practices and training materials. Several vendor participants identified areas for improvement based on the data gathered during the exercise.

Mr. Kowdley offered recommendations for mitigating jamming, saying communications failures are often assumed to be equipment issues. He said agencies should set operators up for success through equipment purchasing, setup, and fleet map management. Education is key – operators must understand jamming threats to take them seriously. Operators need to ensure all levels of the organization are aware of jamming threats, consult with legal counsel to understand state and local jamming laws, encourage regular radio training drills for operational personnel, and use communications systems in multiple bands for backup.

Basic mitigation strategies include shielding and increased vertical or horizontal distance between the jammer and the communications equipment. Jamming requires prompt reporting of "equipment issues" to the communications team. He also said operators should switch on Automatic Gain Control in radio programing for all LMRs. For special events, FRG recommended that agencies develop a PACE (Primary, Alternate, Contingency, Emergency) plan for communications. Agencies should alert coordinating jurisdictions of potential jamming threats, symptoms, and reporting procedures. Also, train is needed for event security teams on jammer identification and mitigation tactics, monitor event with spectrum analyzers and use direction-finding tools to locate interference sources. All suspected radio frequency interference MUST be reported to the Federal Communications Commission as soon as possible at FCCOPS@fcc.gov.

Joe Heaps, National Institute of Justice, asked if there is reference list that documents the states and areas where jammers are illegal. Mr. Kowdley said unfortunately there is not. John McIntosh, Association of Fish and Wildlife Agencies (AFWA), asked who deploys jammers. Mr. Kowdley said users range from high-end resorts to ministers who do not want their sermons disturbed. They have also been used in robberies in defeat alarm systems.

Technology and Broadband Committee, Kim Coleman Madsen via teleconference, Committee Chair; Andy Thiessen, Vice Chair; Dr. Michael Britt, Vice Chair

Video Technology Advisory Group (VTAG), John Contestabile, Chair. Mr. Contestabile said the VTAG is currently working with DHS S&T's Video Quality in Public Safety (VQiPS) as it plans the annual conference, which is tentatively scheduled for November/December. VQiPS has been focused on creating a charter and rules for that advisory group.

The VTAG priorities for the coming year are to monitor advances in video and analytics to support public safety; for example, the development of first responder devices that analyze the words and behavior of a suspect stopped on the side of the road. VTAG is reviewing content to determine if there is a trigger in the video to alert first responders that action is needed. This is a research project in association with Washington State University. The goal is ultimately to develop a system that could detect an event escalation and send a data alert. Another area of interest is first responder devices that analyze images

and text. This work is being done in association with the National Institute of Standards and Technology (NIST). The system would "read" a hazardous material placard and pull that data automatically.

Broadband Emerging Technologies Working Group, Kim Coleman Madsen, Chair. Mark Golaszewski, Director of Applications, and Joe Martinet, Director of Devices, presented on FirstNet applications and devices. Some of the issues addressed included how agencies will manage applications on the user device. Regarding shared devices, the question was asked about a Mobile Data Terminal (MDT) used by two officers in a patrol car or a device used by a patrol officer on day shift and also used by a patrol supervisor on evening shift. This would also include issues surrounding a cache device that may be used by law enforcement, fire, or EMS first responders. The presentation generated some substantive questions such as the following:

How will "Bring Your Own Device (BYOD)" be managed? Will Internet access be provided for users whose agency does not provide it? How is VPN traffic prioritized when a VPN connection may carry multiple message streams (video, data, and voice)?

How will apps be interoperable? For example, how is interoperability achieved in the case of three fire departments on the scene of a building fire, where each agency has selected a different situational awareness app, or a fire department working with the police department at the scene of a hostage event with each agency using different apps to track personnel location?

How will Mission Critical Push to Talk (MC PTT) be managed? Will MC PTT be a single nationwide PTT service that is common and interoperable across all agencies? How will MC PTT be interoperable with other PTT services offered by FirstNet (Kodiak and WAVE), and how will Kodiak users on FirstNet communicate with WAVE users on FirstNet?

LMR to LTE Integration and Interoperability Working Group, Chris Kindelspire, Chair. Mr. Kindelspire reported the LMR LTE Integration and Interoperability Report is being finalized. Some early conclusions of the Working Group include the following:

- Mission Critical Voice services are an essential element of the Nationwide Public Safety Broadband Network (NPSBN).
- An open standards environment is required, so public safety agencies may access a robust multi-vendor eco system.
- Integration of LMR and LTE PTT voice services will be required.
- 3GPP Standards on Direct Mode communications are not keeping pace with the speed of deployment of PTT networks.
- Encryption is an important component for certain tactical voice communications.
- A nationwide standard to define a PTT ID is needed.
- A set of LTE talkgroup names for nationwide interoperability talkgroups is needed.

There is uncertainty on how 3GPP standards will be implemented by manufacturers and network operators. Video chat with full duplex voice is an important capability for EMS and other first responders.

LTE consoles will play an important role in the evolution of PTT voice and (eventually) all mission critical services (MC PTT, MC Video, and MC Data).

It was noted that 3GPP standards have not yet defined a public safety dispatch console, which will be a critical component for PSAPs as the NPSBN is deployed. These consoles will play an important role in the evolution of PTT voice and (eventually) all mission critical services (MC PTT, MC Video, MC Data).

Mr. Heaps asked about the impact of inconsistent encryption. Mr. Kindelspire said the LMR network would have whatever encryption had been adopted on the LMR network. The LTE device would need a transcoding point. Mr. Haller thanked Mr. Kindelspire for his hard work on this important effort.

Unmanned Aircraft Systems (UAS)/Robotics Working Group, Dr. Michael Britt, Chair. Dr. Britt said there are four main areas of focus for the Working Group: Continuing review of the public safety role for UAS; coordination with the National Council on Public Safety UAS; monitoring of the rapidly expanding use of UAS devices; and documenting the use of UAS as a communications platform.

The Working Group recently heard an AT&T Presentation on the Flying Cow (Cell on Wheels). In response to Hurricane Harvey, AT&T had deployed 46 site inspection drones with 58 on standby at one time.

In news about drones, Dr. Britt reported the U.S. Army ordered troops to stop using consumer drones made by the Chinese manufacturer of DJI Drone Units, per an August 2, 2017, memo. The memo cited "increased awareness of cyber vulnerabilities associated with DIJ products." Also notable, he reported, Africa is now the world's testing ground for commercial drones. The world's first commercial drone delivery service operates from Rwanda. Zipline, a San Francisco-based robotics company, delivers blood by drone to almost half of all Rwanda's blood transfusion centers.

Radio Programming Compatibility Requirements Working Group, Dan Robinson, Chair, via teleconference. Mr. Robinson reported that DHS S&T has completed testing of the PAM Tool, which will be posted to the SAFECOM website soon. NPSTC is making a final quality assurance check and relocking the spreadsheet. NPSTC is working with the Telecommunications Industry Association (TIA) on a project to create a standardized way for radio manufacturers to export and import basic radio programming data. Jim Holthaus, Telecommunications Industry Association (TIA), is leading this project.

TIA Update on Interchange Standard, Jim Holthaus, TIA Representative, via teleconference. Mr. Holthaus provided an update on a draft data exchange schema. The schema was distributed in February; it would standardize the data field names and sequence to support import and export of code plug (programming) information between P25 manufacturers. This was originally proposed to be a TIA Technical Bulletin, but the group felt it should instead be a TIA Standard. Comments were requested from TIA members and are being reviewed. A revised draft of the standard will be presented at the October TIA meeting. The normal TIA process would then be to conduct a 30-day ballot. Additional revisions could result from the ballot process.

Public Safety Internet of Things (IoT) Working Group, Barry Fraser, Chair, via teleconference. Mr. Fraser said the Working Group is continuing to schedule educational presentations with a focus on examining the complexity of IoT data that may be available to first responders. For example:

- IoT data from government entities may flow through government IT networks to the appropriate government entity (e.g., traffic sensors, lake level monitoring). Some of this data may be shared with a PSAP.
- IoT data from companies and industry may flow through their networks to a local control center or to a third party monitoring center. Some of that data may need to be shared with a PSAP or directly with first responders.
- IoT data from citizens (wearable technologies and home systems, including medical monitoring) may flow to third party monitoring centers and/or directly to a PSAP.
- IoT data from certain systems may flow directly to the PSAP (first point of transmission), including voice, video, and data supporting a 911 call.
- IoT data from first responders that would flow through FirstNet to the PSAP.
- IoT data may be shared by different organizations and eventually be routed to a PSAP or to a first responder. This includes data from hospitals, fusion centers, and government and private analytics centers.

This supports the next phase of concern for the Working Group, including the following issues:

- What level of trust do public safety agencies place in IoT data?
- Is the sensor owned/operated by a government entity vs. a public sensor?
- Is there sufficient security (cyber and physical) to prevent the sensor data from being manipulated?
- Is the data transmitted by the sensor consistent with results expected for the incident?
- Is the data from the sensor consistent with data from other nearby sensors and devices?

What do agencies need to know to answer these questions?

- Device and network technical standards and minimum requirements.
- Operational standards, analytics plus artificial intelligence will equal actionable intelligence, and data limitations.
- Other Issues include privacy, confidentiality, data ownership, data sharing across agencies, etc.

Public Safety Communications Research (PSCR), Dereck Orr, Division Chief, via teleconference. Mr. Orr reported on recent activities of PSCR. PSCR hosted the User Interface Roadmap Summit last month with the summit report to be published this fall. There is an upcoming deployable summit in Boulder, CO, on October 18-19. There will be an upcoming grant program offered in the next 4 to 6 weeks for the development of a virtual test environment that will facilitate implementation in large-scale prototypes of earlier ideas. Mr. Orr estimates this to be a $5 to 6 million grant program. Next June, PSCR will host its meeting in San Diego, CA. PSCR plans to do three live prize challenges on deployables at that meeting using some type of challenge based on in building coverage. There is an ongoing prize challenge to develop five professional videos describing PSCR topic areas of research and development, including location based services and analytics. PSCR is also researching algorithms to remove data sets to allow researchers to use the information in a meaningful way without divulging personal or proprietary information.

Topical Presentation

Public Safety Policy, Don Brittingham, Vice President-Public Safety, Verizon. Mr. Brittingham addressed the group to discuss Verizon's public safety services and recent announcement of plans to build a core public safety network. He noted Verizon has had a longstanding commitment to public safety for many years. When asked why Verizon did not bid on the FirstNet RFP, he said Verizon didn't have an interest in the spectrum allocated to FirstNet. He said Verizon's plans meet or exceed the vast majority of NPSTC's public safety grade requirements. Many of Verizon's network and facility design requirements (e.g., environmental protections and back-up power) exceed the requirements recommended by NPSTC. Some requirements, such as deployables with standalone capability, mission critical push-to-talk, and other applications are evolving, but are being developed to address public safety's rigorous requirements.

He said Verizon does not view FirstNet as a competitor. Verizon is committed to being interoperable. Verizon offers a dedicated public safety network core investment at zero cost with Push to Talk Plus with LMR interoperability and future investment in mission-critical voice. He said this includes priority and preemption services at zero cost. In the past, Verizon said they could not provide priority and preemption, but the creation of FirstNet and AT&T has changed that mindset. He said Verizon offers enhanced data plans and a Band class 14 device portfolio.

He added that the Verizon public safety core will be dedicated to public safety communications. There will be no CAPEX/OPEX expenditure for public safety; Verizon will make the infrastructure investment. These competitive alternatives will result in the greatest ongoing innovation. Verizon is planning to offer preemption by the end of this year, and the company needs public safety input on local control and priority and preemption.

Kevin McGinnis, National Association of State Emergency Medical Services Officials (NASEMSO) and FirstNet Board member, asked how Verizon will seek public safety input. Mr. Brittingham said Verizon would assemble an advisory team and that the company has reached out to FirstNet.

Charlie Sasser, National Association of State Technology Directors (NASTD), and Committee Vice Chair, Spectrum Management Committee, asked if Verizon was planning to provide the same coverage commitment. Mr. Brittingham said Verizon has a very extensive network. The intent is to make it available over the entirety of the network and via the rural partners. Mr. McGinnis asked if Verizon has a data roaming agreement with AT&T. Verizon does not have a roaming agreement, but the company does not see the roaming issue as critical.

NextNav, Gary Parsons, Chairman. Mr. Parsons presented an update on 3D indoor location and improved outdoor location. Geolocation and situational awareness is paramount in emergencies and incident management. Today, GPS is used to provide that awareness outdoors with some success; however, until now, no solution has existed for indoors. Indoor location requires horizontal accuracy, vertical accuracy, mission critical/yield (ability to operate in the absence of power and withstand extreme weather conditions), and ubiquity and consistency (needs to work everywhere in the market).

Metropolitan Beacon System (MBS) is a wide area location and timing technology designed to provide services in areas where GPS or other satellite location signals cannot be reliably received. MBS consumes significantly less power than GPS and includes high-precision altitude. NextNav operates its MBS network over its spectrum licenses in the 920-928 MHz band. Mr. Parsons said MBS is essentially a network of terrestrial "satellites" broadcasting from rooftops and towers. It provides the following:

- An overlay network, dedicated to provide 3D (X, Y, and Z axis) positioning with unique, proven floor-level vertical and horizontal accuracy.
- Wide area coverage; it can cover an entire market, much smaller than a cellular build. The San Francisco Bay Area is built to cover over 900 sq. miles with ~ 100 beacons.
- Long-range, low-cost broadcast beacons placed on cell towers and rooftops that are not building specific with a typical range 0.5-5 miles (depending on environment).
- Deployed and managed to deliver mission critical services (ability to withstand power outages and storms) location with multi-layer reliability. There is beacon redundancy and a battery backup to ensure continuity during power outages.
- Complementary to GPS.
- Designed to be built into phones standard with no accessories required.
- Initial beacon network operational for six years in Top 47 markets.

With the x, y, and z axis, comes the ability to create 3D Context Visualization Service:

- Supports real time 3D tracking of 9-1-1 callers and first responders with accurate 3D representations of all structures. Floor plans ingested into hosted platform where available.
- In addition to visual display, supports user context information and other building details where available (e.g., address, floor, suite/room). This could be integrated with body camera systems and other sensors.
- Information can be displayed via web interface, dedicated tablet/phone application.
- Fully-featured UI – breadcrumbing, pan/tilt/zoom, prioritized identification of individuals or groups, buildings, etc.
- APIs available for integration into existing tools and applications where preferred.

Rick Comerford, International Association of Emergency Managers (IAEM), asked if the MBS is available in handsets. Jim Goldstein, International Association of Fire Chiefs (IAFC), said IAFC, IACP, and NASEMSO all meet quarterly as part of the CTIA advisory group. They have filed two FCC ex parte comments together with the National Sheriffs Association, one dealing with amount of disclosure by carriers. They feel CTIA has not provided enough information. The Association of Public-Safety Communications Officials (APCO) International and the National Emergency Number Association (NENA) are also working this issue regarding the definition of dispatchable location. IAFC faces the worst case scenario in terms of indoor location. The definition of dispatchable location one only refers to an access point; dispatchable location two governs the location of a person. Dispatchable location one is not usable by public safety. Mr. Goldstein said it is important to point out that the FCC order calls for a dispatchable location. The breakdown of dispatchable location into levels one and two are a creation of CTIA and ATIS. These levels are inconsistent with the FCC order definition.

Tom Sorley, Public Safety Advisory Committee (PSAC) Chair, Houston Update, via teleconference. Mr. Sorley thanked everyone for their emails and concern. The area is in full blown recovery mode now. The water is beginning to recede. His communications system lost only one site in the flood and main electrical service in one area. They turned on all the generators at the onset of the storm to avoid sporadic power surges. Mr. Sorley said he learned the generators used about a quart of oil a day to his surprise.

Governing Board Member Update

ARRL, National Association for Amateur Radio, Tom Gallagher, NY2RF, Chief Executive Officer, and Mike Corey, Kl1U, Emergency Preparedness Manager. Mr. Corey introduced Mr. Gallagher, who has led the Amateur Radio Relay League (ARRL) since this April. Mr. Gallagher expressed gratitude on behalf of ARRL and its 160,000 members, 40,000 volunteers, and 750,000 amateur operators in the U.S. for its inclusion in NPSTC. He said ARRL is transitioning a new population of amateur radio operators. The number one reason for acquiring a license is a desire to assist in emergencies. He said there is a generation who has not experienced a disaster. Technologies and procedures have changed over the years. ARRL wants to enable hams to be genuinely helpful in emergency situations and to expand their "Swiss army knife" skills. For example, in Texas, a group of amateurs built a network connecting hospitals. In Connecticut, hams are building a network between ARRL headquarters and two first responder agencies.

ARRL seeks support for passage of the Amateur Radio Parity Act. Ninety percent of new housing in the U.S. is covered by homeowners associations. HOAs do not like antennas in their neighborhood. Hams need some type of antenna. If this bill does not pass, the next opportunity to address the issue will not be possible for another 10 years. There are 69 million members of HOAs; there are 750,000 hams. Mr. Gallagher asked the individuals in NPSTC to support this bill.

Mr. Haller called support of the bill a good idea. Mr. McGinnis asked ARRL for examples of public safety support from hams that the Governing Board members could take back to their individual organizations such as providing assistance to hospitals. Mr. Goldstein suggested ARRL ask other organizations to provide their named support regarding the bill.

Executive Session Level IV. Mr. Haller recessed the meeting at 11:10 a.m. EDT until resumption of the open meeting at 1:00 p.m. EDT.

FirstNet NPSBN Development

FirstNet, Amanda Hilliard, Deputy Chief Customer Officer, and Kevin McGinnis, FirstNet Board Member. Mr. McGinnis introduced Ms. Hilliard and Chris Sambar, senior vice president-FirstNet for AT&T. Ms. Hilliard thanked the Technology and Broadband Committee for its important work in developing public safety needs and requirements. The FirstNet Chief Customer Office consults with public safety, engages around network experience and use cases, and advocates for enhancements, upgrades, and improvements.

She discussed the timeline for the development of state plans. The state plan timeline comprises various stages of the state plan review process. FirstNet released plans in June, with much dialogue between

June and the August 4 deadline, resulting in some modifications to the state plans. FirstNet will resubmit to the SPOCs and the governors, starting the 90-day deadlines for decisions. Discussions included SPOCs, AT&T, and FirstNet and provided excellent feedback. The following states have opted in:

Alaska	Maine	Puerto Rico
Arizona	Michigan	Tennessee
Arkansas	Montana	U.S. Virgin Islands
Hawaii	Nebraska	Virginia
Iowa	Nevada	West Virginia
Kansas	New Jersey	Wyoming
Kentucky	New Mexico	

Mr. Sambar said he is familiar with NPSTC's commendable work, including the public safety grade report. He apologized for remarks that may have been misleading concerning whether AT&T was committed to deploying a public safety grade network. He said AT&T has a total commitment to public safety and its requirements. The term public safety grade is a vast topic. During Hurricane Harvey, AT&T had 30 central offices – the "brains" of the network – in the affected flood zone. He described the extreme measures AT&T undertook to keep the offices running.

Regarding whether or not all towers need to be at the level of public safety grade, he said AT&T is working on identifying the critical towers. Addressing rumors that AT&T will not use Band 14, he said it is not true. AT&T will use Band 14 for capacity and coverage. As AT&T builds out, the company will deploy Band 14 broadly as well as commercial spectrum.

Paul Fitzgerald, National Sheriffs' Association (NSA), asked for AT&T's position on enhanced location services. Mr. Sambar said the requirements are compliant with E911 but not as stringent as they should be for public safety. Most use barometric pressure to compare pressure with the device and surrounding areas, but burning buildings exhibit changes in barometric pressure. AT&T is looking for the best solution, which he believes will be a combination of hardware and software. He expects to have something in place by 2020, but policy and privacy issues are complicated.

When asked if AT&T has a strategy on how it will implement Band 14, Mr. Sambar said this is valuable spectrum for first responders. The spectrum came with significant commitments associated with that band. The strategy is to deploy everywhere capacity is needed and for all new rural sites. In the first 5 years, Band 14 will comprise over 50 percent of the network. The end user will not be aware of which band they are using.

Mr. Contestabile asked about the app store and how it will be rolled out. AT&T will vet all of the apps, making sure they are safe, secure, and function as promised. AT&T is also required to have a third party review apps. The Boulder lab will also be reviewing independent apps. Mr. Goldstein asked about the use of deployables, particularly in rural areas, as a back-up solution to broadband rural. Mr. Sambar said deployables are not considered a long-term solution to rural broadband; however, he said, in Texas, AT&T used deployables as the company was working to get the backhaul repaired. Deployables could also be used for wildfires in remote areas that don't really need towers.

Mr. Sasser asked if the help desk/call center would rely on the NPSTC public safety grade definition. Mr. Sambar said it would. Alan Tilles, Shulman Rogers Gandal Pordy & Ecker, asked Ms. Hilliard to describe some of the "good feedback" she mentioned FirstNet was hearing from the states. Mr. Sambar said states like the fact that AT&T is willing to work with them on their specific needs; for example, needs based on difficult terrain. Mr. Tilles asked if FirstNet had learned things it didn't know before this interaction. Mr. Sambar said AT&T learned about the need for towers next to the PSAP, the fear smaller states have regarding resources in competition with their larger neighbors, and sensitive political issues.

Marilyn Ward, NPSTC, Executive Director, asked about encryption on AT&T's spectrum/channels. Mr. Sambar said all public safety will be on the FirstNet encrypted core network although the system will choose the strongest band to communicate with the user.

Barry Luke, NPSTC, Deputy Executive Director, noted some findings in the Broadband Deployables Report included the need to communicate over the border that would require a core-to-core connection. Mr. Sambar said interoperability can be controlled in many ways. AT&T is building based on 3GPP standards; however, when networks operate core-to-core, it's a slippery slope. AT&T is not comfortable with a core using Chinese hardware. When there are seams in the network, you create vulnerability.

Mr. Haller encouraged FirstNet and AT&T representatives to continue to provide updates to NPSTC.

FirstNet Public Safety Advisory Committee (PSAC), Paul Patrick, Committee Vice Chair. Mr. Patrick provided an update on the July Tribal Working Group Meeting. The discussions took place with the Navajo Nation Council, Navajo Nation leadership, and Tribal-Interior Budget Council (TIBC) Public Safety and Justice Subcommittee Meeting. Presentations included a FirstNet solution overview, tribal consultation policy, rights-of-way streamlining, federal agency participation, and contract vehicles. There will be a PSAC webinar on Wednesday, September 27, 2:00 p.m. EDT and an in-person PSAC meeting during the week of December 11, in Atlanta, GA. Mr. McGinnis noted one of the weaknesses of the legislation that created FirstNet was that it did not include a provision for tribal consultation. Over the last 3 years, FirstNet has created an informal consultation process.

Interoperability Committee, John Lenihan, Chair; Jason Matthews, Vice Chair

Monitoring the P25 CAP Advisory Panel. Chief Lenihan reported a P25 meeting was held on August 16 at the APCO meeting in Denver, CO. The 2017 Baseline Common Air Interface (CAI) Testing Requirements Compliance Assessment Bulletin (CAB) is online. P25 published a draft minimum feature requirements CAB for a 30-day public comment period that ended August 21. The implementation of the Encryption Requirements CAB is ongoing, which requires P25 AES encryption if encryption is offered in a radio.

The Committee is monitoring the increased adoption of non-P25 digital systems by government and public safety agencies. Agencies on VHF and UHF are more likely to adopt NXDN, DMR, and IDAS. Rural agencies work with local radio shops, which typically do not deal with P25. Local radio shops may recommend systems that they can install and support. The cost of non-P25 devices is a significant factor,

only $700 for a Tier 3 DMR radio with GPS, non-standard encryption, and emergency button functionality. Some agencies need to purchase DMR equipment to supplement their interoperability resources to support adjoining areas using that technology.

Common Channel Naming Working Group, Don Root, Chair. The Working Group is completing the scope of work for the new LTE Interoperable Talkgroup Naming Standard. FirstNet will provide a nationwide interoperable network that will eventually provide Mission Critical Push to Talk (MC PTT). MC PTT systems use virtual radio channels called LTE talkgroups. A nationwide set of LTE interoperability talkgroups will be needed to support first responder communications.

The Working Group held a face-to-face meeting yesterday, where it finalized a list of issues to be considered. NPSTC will be announcing a call for participation in September, and the Working Group will begin regular meetings in October.

Emergency Medical Services Working Group, Paul Patrick, Chair. Mr. Patrick reported the Working Group is monitoring how new technology is changing EMS. There are new products, services, and solutions available for first responders, including analytics, the IoT, and sensors to track citizens with medical conditions. UAS drones are emerging as a support to EMS. Mr. Patrick said the University of Virginia, which presented to the group, is working on an analytics and communications hub for EMS personnel. The Working Group is finalizing an outreach report on Mobile Personal Emergency Response Systems (mPERS), a GPS-enabled pendant that works on commercial cellular networks and automatically detects a fall and sends a data alert. This is the first of many medical sensor alert devices that will impact the PSAPs and EMS agencies.

Cross Border Working Group, Steve Mallory, Chair. Chief Lenihan, reporting for Mr. Mallory, said a draft report on 911 Data Sharing has been sent to U.S. and Canadian carriers requesting feedback. The Working Group is creating a list of all interoperability frequencies that are available at the U.S./Canadian border. The report will also identify which specific channels and/or systems are in use in each region. The goal is to extend outreach to agencies along the border and educate them on available options. The following is a list of the states and the provinces with which they interact:

<u>British Columbia Province</u>
State of Washington
State of Idaho

<u>Alberta Province</u>
State of Montana

<u>Saskatchewan Province</u>
State of Montana
State of North Dakota

<u>Manitoba Province</u>
State of North Dakota
State of Minnesota

<u>New Brunswick Province</u>
State of Maine

<u>Ontario Province</u>
State of Minnesota
State of Wisconsin (water)
State of Michigan
State of Ohio (water)
State of Pennsylvania (water)
State of New York

Quebec Province
State of New York
State of Vermont
State of Maine

Nova Scotia Province
State of Maine (water)

Radio Interoperability Best Practices Working Group, Mark Schroeder, Chair, via teleconference.
Mr. Schroeder reported *Best Practice #7 on After Action Review* has been completed. It states that any After Action Review (AAR) generated when Interoperability resources are used to support a significant/working incident or event should include both operational and technical components. This Best Practice includes an AAR Checklist as a companion document to illustrate the many areas of inquiry during an incident review. Motion and Vote: Paul Szoc, International Municipal Signal Association (IMSA), moved to approve Best Practice #7. Mr. Reyes seconded. Approved.

Spectrum Management Committee, Don Root, Chair; Charlie Sasser, Vice Chair.
Committee Issue Update, Don Root.
FCC Notice of Inquiry on 3.7 GHz to 24 GHz. Mr. Root reported the FCC released a Notice of Inquiry (NOI) on the 3.7 GHz to 24 GHz spectrum. A key focus is the 5.925 GHz – 6.425 GHz band. FCC records show over 27,000 point-to-point licenses. This is a key band for public safety microwave. The NOI seeks information on the potential for additional flexible broadband use of the band:

- Unlicensed use to expand the 580 MHz U-NII devices can already access at 5 GHz.
- Licensed broadband.
- Protection of existing fixed operations.
- Possibility and cost of repacking existing fixed operations.

Mr. Root said comments are due Monday, October 2; replies are due November 1, 2017. The Spectrum Management Committee discussed this NOI on its August call. The group is gathering information on 6 GHz microwave link reliability requirements and plans a specific call to discuss this further. The Committee will provide a draft of NPSTC Comments to the Governing Board by September 22. Any rule changes would require a subsequent Notice of Proposed Rulemaking (NPRM) with the opportunity to comment again.

Follow-up on 800 MHz Cellular Power Level Decision. The FCC issued a decision March 24, 2017, allowing cellular systems to use power flux density and higher power. The decision directed the Bureaus to assemble a "multi-stakeholder" meeting to address co-existence. Stakeholders include public safety, the carriers, and equipment manufacturers. The meeting is tentatively set for November 6, 2017. NPSTC and APCO have offered representatives to participate.

Mr. Root announced that Mr. Sasser has been appointed to the FCC's Communications Security, Reliability, and Interoperability Council Working Group 1 – Transition Path to 911. The CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.

Federal Communications Commission (FCC) Filings, Charlie Sasser. Mr. Sasser reviewed anticipated and completed filings. All filings are available for review on NPSTC's website.

Date Filed	Topic	Type of Filing
10/02/17	FCC NOI on 3.7 GHz to 24 GHz	Comments (Anticipated)
7/31/17	Blue Alerts	Comments
7/31/17	Arizona Pub Svc Co (Utility)	Comments
6/03/17	WRC-19/LMCC 460-470 MHz	Letter, FCC
5/24/17	Broadband Healthcare	Comments, FCC
5/01/17	700 MHz A-G Border	Comments, FCC
4/12/17	V2V Mandate & Standardization	Comments, DOT/NHTSA
3/24/17	Wilson/Cellular Boosters	Comments, FCC
3/06/17	Higher Ground	Comments, FCC
1/27/17	North Dakota on-VLAW 31	Comments, FCC
1/22/17	P25 Encryption Capabilities	Letter, DHS/OIC

Federal Partners Update

Federal Partnership for Interoperable Communications (FPIC), Jim Downes. Mr. Downes discussed three current priorities:

- Encrypted interoperability and key distribution.
- P25 Inter RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) implementation challenges and resolutions and suggested improvements toward interoperability.
- Memorandum of understanding for public safety access to NTIA VHF/UHF I/O channels.

Encryption. The FPIC Security Subcommittee, in coordination with the National Law Enforcement Communications Center (NLECC) and other public safety agencies, developed a standardized Storage

Location Number (SLN) assignment list for National Encrypted Interoperability (June 2015). OEC and FPIC continue to encourage public safety agencies to coordinate SLN and Key ID assignments with the NLECC. An accurate database can minimize conflicts, resulting in improved encrypted interoperability. As a result of challenges identified during recent implementations, the NLECC and FPIC are evaluating key distribution procedures and the SLN Table.

The FPIC Security Subcommittee is working closely with the NLECC and key public safety agencies to address the challenges recently identified that impact interoperability. Subcommittee efforts include:

- Addressing specific recommendations to revise the standards relevant to encryption.
- Recommending more stringent requirements for compliant standards. (Minimize optional standards.)
- Minimizing the use of non-standard solutions.
- Accelerating the standards development for two key interfaces.
- Reevaluating key distribution procedures and the use of "static keys" for interoperability.

The FPIC Security Subcommittee formed a small focus group comprised of knowledgeable SMEs to address the following topics:

- Major areas relevant to standards, including P25 standard adoption by manufacturers and to minimize optional standards that impact interoperability.
- The Subcommittee is also considering more effective methods to educate the user before implementing encryption.
- There is a focus group meeting scheduled on September 14-15, at the NLECC in Orlando, to develop recommendations and to draft a position paper to be presented to TIA TR8 in October.

ISSI Overview. The Inter RF Subsystem Interface (ISSI), a P25 Phase 2 technology, enhances public safety's ability to interconnect multiple P25 systems. Many users have successfully implemented ISSIs, and to a lesser extent the console subsystem interface (CSSI), to expand coverage and provide enhanced interoperability between P25 systems regardless of vendor. Because ISSI is a relatively new technology, there is a learning curve for users and manufacturers alike to understand ISSI expectations and standards.

The standards supporting the P25 ISSI and CSSI are still in progress, and both user and manufacturer involvement is critical. The FPIC is leading an effort to address misunderstandings and miscommunications concerning the ISSI/CSSI. In May 2016, the FPIC sponsored a working session to share ISSI/CSSI implementation successes, challenges, and experiences between users and manufacturers.

The ISSI/CSSI User Focus Group was established to consolidate information from users and identify successes, challenges, and mitigation experienced during implementations. Participants identified several action items for consideration by the group. Two of the more immediate actions are to develop an action plan and baseline interoperability requirements and to develop discussion topics and hold follow-up working sessions between users and manufacturers. Initial discussions revealed challenges were both technical and governance/funding related.

Preliminary findings revealed a wide range of misunderstandings, including:

- Users may not understand the functionality covered by the standard.
- Some manufacturers may not have implemented standard functionality desired by the user.
- Manufacturers and users may have different interpretations of the standard definitions of functionality desired by the user.
- Manufacturers may have different interpretations of the users' desired standard functionality.
- Manufacturers may have implemented the functionality requested by the user, but not covered by the standard.
- Some challenges are not technical, but deal with governance and funding.
- The best time to identify these misunderstandings is during the planning or testing process.

The upcoming FPIC ISSI/CSSI User Working Session is scheduled for September 19-20, in Arlington, TX. This meeting is open to any user employed by a government user agency (both days) and any manufacturer (second day) that provides or supports ISSI/CSSI. This meeting will focus on suggestions and recommendations developed by the Focus Group in a collaborative environment with both users and manufacturers. If interested in attending the upcoming working session, email FPIC@hq.dhs.gov.

Memorandum of Understanding (MOU) for Interoperability Channels. FPIC is working with state, local, and federal users to enhance interoperability across the nation. The NTIA revised procedures within the NTIA Manual to allow the public safety agencies easier access to the NTIA interoperability channels. The Department of Interior (DOI) led an effort in coordination with the DOJ, DHS Spectrum Management Offices, and FPIC Spectrum Subcommittee to develop an MOU. The MOU was accepted by FCC, NTIA, and the SWICs to share interoperability channels in each state. Chris Lewis, DOI, is the federal signatory, and the SWIC (or designated representative) will sign on behalf of the state. To date, five states have executed the MOU, and several others are coordinating efforts with DOI.

Mr. Powell asked about the priority use of NTIA channels. During a large wildfire, channels get grabbed and interfere with other communications. Nothing in the MOU stipulates priorities.

Federal Communications Commission (FCC), David Furth, Deputy Bureau Chief. Mr. Furth provided updates on the activities at the FCC. Before Hurricane Harvey had made landfall, the Commission began to make preparations for needs during the storm and after for recovery. The Commission provided daily updates on communication throughout the storm. Every time there is a storm, the Commission initiates an after action analysis of what was done and what could be done better through the best information the agency can provide.

Regarding FirstNet, Mr. Furth said the Commission has the responsibility under the statute to develop criteria and the process the Commission would use to review an opt-out plan. An item addressing an interoperability compliance matrix submitted by FirstNet has been circulated to FCC Commissioners. The statutory process focuses on interoperability as the goal is a nationwide interoperable public safety network. FirstNet has added its own requirements and desires to the interoperability component. The Bureau was directed to issue a Public Notice to communicate the final piece of the process regarding the added interoperability component. The Commission has imposed on itself an "aspirational shot clock" to expedite any opt-out request.

On next Monday, September 11, the FCC will hold a workshop on 911 outages. The workshop also will focus on situational awareness, particularly in the PSAP. On September 27, the Commission will host the third nationwide test of the alerting system. The Commission has convened a new CSRIC, which is chartered for a fixed time. There are several working groups, including NG911, dealing with reliability issues and next generation alerting.

The Commission is continuing to work on 4.9 GHz and 700 MHz narrowband. With the Office of Engineering and Technology, the PSHSB will host a workshop related to an order on the 800 MHz band to allow wireless carriers to carry LTE on that band and to ensure no interference results.
Mr. Tilles asked if there is an "aspirational shot clock" on the T-Band issue. Mr. Furth said the Commission is working internally on T-Band issues. Mr. Tilles also asked for the status of 800 MHz rebanding on the Mexican border. Mr. Furth said Mexico is beginning to move incumbents. AT&T now owns what used to be Nextel Mexico. The Commission is working with these stakeholders to facilitate the rebanding.

Mr. Downes asked for a status update on the FCC work related to the NTIA MOU to support interoperability between federal and local users. Mr. Furth said it will be in the form of a Bureau Order, not a Public Notice.

FCC, Charles Cooper, Field Director. Mr. Cooper reported on behalf of the new Enforcement Bureau Chief, Rosemary Herald. The Bureau has spent the last three quarters of the year on the field modernization effort. The Bureau is very busy, particularly in light of the hurricane. It is spending resources on investigations of pirate stations. Public safety continues to be the biggest customer with the Bureau running 70 public safety interference investigations, which are equally spread among the three regions. Unlit towers continue to be an issue, particularly in the case of abandoned towers. The Bureau is implementing sanctions on unlicensed operations and violations that are now posted on the FCC Daily Digest. The Enforcement Bureau and the PSHSB partnered to do spectrum surveys in the recent hurricane.

Award Presentation and Break

Participant's Award, Sponsored by NASEMSO. The *NPSTC Participant's Award* was created to recognize individuals and/or organizations that have supported NPSTC and the public safety community on critical objectives such as achieving interoperability. The winners are Paul Kirby, TRDaily; Sandra Wendelken, Mission Critical Communications; Donny Jackson, Urgent Communications; and Andrew Seybold, Public Safety Advocate.

Leadership Award, Sponsored by NASEMSO. The *NPSTC Leadership Award* was created to recognize individuals and/or organizations that have demonstrated exceptional personal and professional conduct. The winner is Tom Sorley.

DJ Atkinson Technical Award, Sponsored by Jeff Bratcher. The *DJ Atkinson Technical Award*, created in 2012 to honor DJ Atkinson's work, recognizes individuals and/or organizations that have demonstrated

exceptional technical support to NPSTC and the public safety communications community. The winner is Dean Skidmore.

Hertz Award, Sponsored by APCO International. The *NPSTC Hertz Award* was created to recognize the exceptional work of one or more individuals, who have demonstrated extraordinary leadership. The Hertz award, named in honor of Heinrich Hertz, whose name denotes the scientific unit of frequency – cycles per second, is not an annual award, but one that is only awarded when exceptional performance warrants it. The winner is Claudio Lucente.

Lifetime Achievement Award, Sponsored by NENA. The *NPSTC Lifetime Achievement Award* reflects the many years the recipient has worked for the interests of public safety communications, nationwide. The recipient shall have positively influenced nationwide policy in many ways over his/her lifetime, which as a result, has demonstrably improved public safety communications. This award is not given annually, but rather as determined by the NPSTC Governing Board. The winner is John Powell.

Chairman's Award, Sponsored by Ralph Haller. The *NPSTC Chairman's Award* was created to recognize one individual, who has demonstrated extraordinary leadership. The winner is David Furth.

Richard DeMello, Award Sponsored by IMSA. The *Richard DeMello Award* is presented to one individual in public safety communications, who has demonstrated the highest levels of personal and professional conduct and performance in the local, state, and national public safety communications arena. The winner is Kevin McGinnis.

Administrative Discussion. NPSTC will hold a full meeting by teleconference in January 2018. There will be an in-person meeting at IWCE in Orlando, FL, on Friday, March 9, 2018.

Adjournment and Executive Level IV Session. Mr. Szoc moved to adjourn the meeting. Mr. Reyes seconded. Approved. Mr. Haller adjourned the meeting at 3:55 p.m. EDT. The Governing Board reconvened in Executive Session at 4:10 p.m. EDT.