National Public Safety Telecommunications Council (NPSTC)
International Wireless Communications Expo (IWCE)
Meeting Minutes
March 9, 2018 | 8:30 a.m. – 5:00 p.m. ET
Call In: (510) 227-1018 | Conference ID: 1927086#
Webinar Access Information: **https://join.me/npstcsupport1**

Welcome and Opening, Doug Aiken, NPSTC Vice Chair. Mr. Aiken called the meeting to order at 8:30 a.m. ET. Participants on the phone were asked to send a record of their attendance to Attend@npstc.org. Mr. Aiken asked for a moment of silence to honor the passing of Tom Sorley and of Ron Haraseth. He thanked Andy Seybold for arranging the delivery of *Dunkin' Donuts* coffee and donuts, a favorite of Tom's; Stacy Orlick, IWCE, for facilitating that; and Mike Corey, American Radio Relay League (ARRL), for shipping AV equipment to the meeting.

Federal Partners Update

Department of Homeland Security (DHS), Office for Interoperability and Compatibility (OIC), John Merrill, Director. Mr. Merrill discussed recent initiatives at OIC. The Next Generation First Responder (NFGR) integration demonstration was sponsored by OIC in Grant County, WA. The TechEx NGFR Case Study Series on deployable communications, location services, and video services was released in 2017. A Tech Bulletin on physiological monitoring and situational awareness will be released in March 2018. The NASA JPL Plug Test, in February 2018, integrated technologies from performers with a variety of modules that will inform the 2018 NGFR/Harris County, TX, Operational Experimentation (OpEx). An After Action Report will be released mid-to-late 2018.

Also released in February 2018, the *Next Generation First Responder Integration Handbook* provides recommendations from NGFR, which detail technical specifications that are needed to develop interoperable solutions to the first responder market.

AUDREY [Assistant for Understanding Data through Reason, Extraction, and sYnthesis]. OIC is sponsoring pilot programs in artificial intelligence, working with the multi-county communications center in Grant County, WA. AUDREY operates in a similar manner to Siri or Alexa and will respond with information on an incident and its location. OIC has initiated a new partnership with the Defence Research and Development Canada and the U.S. Coast Guard.

POINTER [Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders]. Miniaturization of POINTER's receiver should be finalized by the end of March. The receiver will be approximately two-thirds the size of an IPhone 6 and weigh ounces. OIC is anticipating 70 plus meters of range and less than a 1-meter of error accuracy on all three coordinates (x, y, and z). The first release of POINTER will target rural homes, warehouses, and low-rise buildings. OIC anticipates version one of POINTER being commercially available in mid-to-late 2019.

A visual display for POINTER is being developed by the NASA Jet Propulsion Laboratory (JPL). Piloting of the display will begin later this year. Recent testing of POINTER in a large (over 5,000 square feet) 3-story

rural home showed very good success. Testing of the miniaturized receiver, transmitters, and a UHF wireless communications link (400 MHz to 433 MHz frequency) is scheduled for May through September. Three test environments will be included (rural home, warehouse, and low-rise building). The next phase of R&D for POINTER will focus on use cases in high-rise buildings, outdoor environments, tunnels, and under water environments.

AMBER [Advanced Multi-Purpose Base Ensemble Uniform]. Grant County, WA, fire departments will begin testing in the near future. Designed and developed as a multi-threat base protective ensemble, the AMBER project's anticipated completion date is mid-to-late 2018. International partners interested in testing include Sweden, the United Kingdom, and Canada.

Continuing programs from OIC include:

- TEP [Tracking of Emergency Patients].
- CAUSE and CA/US collaboration: OIC completed CAUSE V this year and will work with Canada to continue this valuable exercise.
- LA County Sheriff: OIC is dealing with deputy attrition in this 10,000 person department.
- UCF AR/VR HUD: OIC started discussions to assist firefighters.
- Harris County Spiral III: OIC is sponsoring testing of capabilities described earlier with law enforcement, fire, and EMS.
- Plug Fest.
- JAM-X 2019.

Department of Homeland Security (DHS), Office of Emergency Communications (OEC), Ron Hewitt, Director. Admiral Hewitt (ret.) reported on OEC activities, including hiring seven new coordinators and four new positions for Communications Unit Training (COMU) and providing funding to support state technical assistance. The key goal this year is sustaining LMR through spectrum and infrastructure sharing, with some significant progress toward that goal. OEC has worked with the National Telecommunications and Information Administration (NTIA) to allow sharing of federal channels. The Statewide Interoperability Coordinator (SWIC) for an individual state can sign an MOU with NTIA to grant that spectrum to its users. Seven states have already signed, and OEC hopes to sign 20 states this year. OEC has also been focused on Puerto Rico, working with the Emergency Communication Preparedness Center, a governance center of federal agencies that have tactical radio systems, to assist in bringing communications back and to provide replacement radios and TA to support territorial and local governments. OEC believes there is good momentum to integrate those systems.

In accordance with the National Emergency Communications Plan (NECP) 2014, OEC needs to move into the integrated world of NG911 and wireless alerting and the need to seamlessly transfer information between those systems. The Statewide Communications Interoperability Plan (SCIP) needs to reflect those changes and that integration. With the National Governors' Association (NGA), SAFECOM held a governance workshop on that integration in New Orleans, LA, which was attended by nine states. Admiral Hewett thanked those who helped to advise on the preparation of the 2018 SAFECOM grant guidance. The notice on the requirement and importance of emergency communications interoperability will be in the Notice of Funding upfront.

He noted integration at the state level is important, but integration at the incident level is the most important. To address that, OEC will focus on the COMU, now geared to LMR. SAFECOM put together a task force, the COMU working group, to examine integrating LMR to LTE capability and interoperability. He thanked NPSTC for issuing recommendations on that issue. The COMU has evolved–Joint operational planning for the COMU must address the need for a communications person and IT systems person to manage incidents. He again thanked NPSTC for its work. What NPSTC and OEC do is aligned in the desire to support first responders to be able to communicate.

FirstNet NPSBN Development

FirstNet, Kevin McGinnis, FirstNet, Public Safety Board Member; Chris Sambar, AT&T FirstNet, Senior Vice President; David Buchanan, FirstNet, Director of Consultation. Mr. McGinnis called the week at IWCE remarkable. He said the public safety broadband discussions were formerly one or two sessions, which was very different from the focus of IWCE 2018. He also noted NG911 is a large concern in public safety response and that IWCE did a good job of balancing those components.

The evolution of technology in EMS and the availability of things once just discussed as "someday" has been rewarding. Twelve years ago he attended a discussion with wireless providers, who said public safety would never have priority and preemption. Public safety took that answer and decided to build its own broadband network. The Public Safety Alliance lobbied the Hill and won. Public safety needed and wanted its own network with priority and preemption, and it is coming.

Mr. Sambar said other wireless providers continue to take shots at FirstNet, calling it an AT&T monopoly. He said it is what public safety asked for–a public safety broadband network that AT&T has been asked to build. He provided an update on the status of the network. The task order for network buildout has been finalized, but AT&T had already begun its work with the states. Over 10,000 sites will have Band 14. There is buildout in areas where there is poor or no coverage, and AT&T is adding thousands of sites to the network. The core network is a dedicated *physically separate* network for public safety. There is a security operations center with a main and backup center. The staff monitor only the FirstNet network and are different people from those who monitor AT&T's network.

There are 350 agencies across the nation, and 40 states are now FirstNet subscribers with 30,000 devices. AT&T is bringing new subscribers onto the network daily, but it has to happen in an orderly fashion; and therefore, it can take some time for agencies that want to get on more quickly. Mr. Sambar noted that device manufacturers have been adding Band 14 to their devices.

Jim Goldstein, International Association of Fire Chiefs (IAFC), asked about enhanced location timing. NPSTC recommended it be effective by June 2019. Mr. Sambar said he considers this a very important issue and has discussed it with a number of companies. There are major challenges with the z-axis in just about all of the technologies, including its ability to be effective when the power in a building goes out. AT&T/FirstNet is in discussion with NextNav on its location device, but its solution needs to be tested in a building when it is on fire because its device uses pressure, and the pressure changes in a building when it is on fire.

Some manufacturers do not like to insert GPS to provide location into a device because they feel it discloses proprietary information. Regarding a question about latency, Mr. Sambar said the standard for

MCPTT does not address latency. There will be redundant core nodes across the country, which reduce latency as well.

Mr. Buchanan echoed Mr. McGinnis's comments on the strong interest in FirstNet at IWCE. He discussed how FirstNet will engage public safety going forward, saying it is important to recognize that only 49 weeks ago the contract was signed with AT&T, and only 71 days ago FirstNet received network certainty with 56 opt-ins. FirstNet celebrated its sixth anniversary last month. FirstNet is now focused on the next 3 to 5 years and how to support public safety. The goals have been clear over the last 6 years: Public safety always gets priority; that the NPSBN is a highly secure network that meets public safety data requirements; and that it offers controlled access by public safety agencies for its users, coverage where public safety operates, and an enhanced user experience.

FirstNet will host a webinar next month. Recognizing that many first responders are not familiar with FirstNet, it will continue to educate public safety and decision makers about FirstNet. This will include collaboration campaigns with all levels of public safety, disciplines, and agency size. FirstNet will try to use these meetings to "unpack" communications issues agencies have today, describe use cases that will help agencies understand how to use FirstNet, and learn how to integrate FirstNet use into public safety operations. He thanked NPSTC for its recommendations and partnership.

Public Safety Advisory Committee (PSAC), Paul Patrick, Interim PSAC Chair. Mr. Patrick said he was honored to serve as the interim Chair of the PSAC. With the guidance of FirstNet, the PSAC is sunsetting its Early Builders Working Group, which did a great job and has provided excellent lessons learned since 2013. The PSAC will be hosting webinars, with the first focused on location based services. A month ago, the PSAC hosted a Tribal Working Group, where there were discussions on LTE Broadband 101 and procurement for tribal governments. Other webinars are planned, one for MCPTT, and others on FirstNet applications, subscriber paid offerings, quality of service, priority and preemption, and local control. The next PSAC meeting will be June 4 in San Diego, CA.

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

Committee Roadmap, Kim Coleman Madsen, Chair, by teleconference. Ms. Coleman Madsen said the Committee and Working Groups are focused on six major areas in upcoming months:

- Monitoring emerging technology trends that will impact public safety agencies, including the emergence of new devices, applications, and systems.
- Continuing to study how Mission Critical Push to Talk (MCPTT) will be used by first responders, including unique issues involving encryption, off network communications, and identity structures.
- Assessing the Public Safety Internet of Things (PS IoT) ecosystem.
- Updating the PAM Tool to provide translation of disparate data fields in various radio programming software.
- Finalizing a review of UAS and robotics issues impacting public safety.
- Monitoring the evolution of public safety video system capabilities, including the use of video analytics.

Public Safety Internet of Things (IoT) Working Group, Barry Fraser, Chair. Mr. Fraser thanked staff for their assistance and support of the Working Group. It has focused on use cases for police, fire, and EMS. During its last two calls, the Working Group discussed a law enforcement traffic stop use case and reviewed a wide range of IoT devices, including:

- Speech-to-Text CAD/MDT entry and database inquiry.
- License Plate Reader (LPR) cameras.
- Body and dash cameras.
- Automated database inquiries and alerts.
- Location based services to assess officer safety.
- Safety sensors that can detect potential threats, a struggle, or an officer down.
- Equipment sensors that can alert dispatchers when a firearm is removed from a holster or fired, or other gunshots are detected.

PS IoT devices may operate on many different networks: Does the IoT sensor communicate to the officer's LTE device, which connects it to the NPSBN, or does the device communicate directly to the NPSBN? The network connection between multiple IoT devices on the officer's body must be reliable. Each device must have an established identity and that data must be provided when the device sends data. If an IoT device sends an "Emergency Alert" to the dispatcher, is the alert coming from a device on the officer's body, or is it coming from the patrol car or from a tablet or laptop?

The Working Group concluded that PS IoT devices:

- Must work as advertised under all environmental conditions. Many devices will likely come to market that will not meet the needs of public safety in spite of the vendor's claims.
- Must be cost effective to purchase/lease, operate, and maintain. Agencies are increasing looking at subscription services vs. agency purchase and ownership.
- Must have an easy to understand user interface when alerting the first responder or providing information. The first responder must not be distracted by normal interaction with the IoT device, yet must receive urgent alerts immediately.
- Must provide data and analysis that is accurate, credible, and helpful to the first responder's mission. Must minimize false alerts. Latency of data delivery must be minimized to provide mission critical services.

The Working Group will finish its review of the use cases below, prepare a report for the Governing Board on the PS IoT ecosystem, noting important issues and opportunities, and create some two-to-five page outreach documents that are discipline specific for public safety, including these scenarios:

- Law enforcement traffic stop.
- House fire.
- Medical emergency response.
- Multi-Agency response (vehicle crash with hazmat and injuries).
- Response to a Smart Building (interaction with other sensors).
- Response to a Smart Home (interaction with home devices).

Public Safety Communications Research (PSCR), Dereck Orr, Acting NIST CTL Lab Director, PSCR Division Chief. Mr. Orr presented an update on key milestones at PSCR. The June conference on Mission Critical Voice worked to identify key performance indicators (KPIs) that would describe user experience

and allow researchers to assign a measureable assessment to compare LMR to LTE. The first measurement on mouth to ear latency has been released with methodologies and datasets available. The next KPI is access time.

The current grant program on location based services is available and has been extended to April 30. Called Point Cloud City, PSCR has doubled that award to $1 million. The task is to use Lidar based technology to map a grantee city and make maps available for research on in building location and navigation.

PSCR received more applications than expected to develop a Virtual Reality (VR) prototype. The grant is for $5 million with a goal for academia to create prototypes and to enhance understanding and the application of lessons learned from VR for real world usage. PSCR hopes to make an award by the June conference. PSCR has a current prize challenge on VR using a heads-up navigation tool. The applicants will navigate from point A to point B in a complex first floor of a building. PSCR will demonstrate that activity at the June conference and award $125,000 to the winner.

PSCR has received 30 submissions for a drone challenge, which is in process. The types and sizes of drones were limited in this challenge, which was initiated to see whether public safety can use inexpensive, simple drones that can carry a 25-pound payload. PSCR selected and funded ten applicants to build drones based on their white paper descriptions.

The June meeting celebrates PSCR's tenth anniversary and will last 4 days. There will be tracks based on subject matter. Each grantee will have a 50-minute session to present and demonstrate their technology. PSCR will support invitational travel to NPSTC's Governing Board and the PSAC. There are only 40 rooms at the government rate left out of the initial 150.

Mr. Orr presented a video, which was created as a result of a prize challenge offered by PSCR to entice developers to work on innovative projects to solve problems for public safety. The video ran at the PSCR booth, which caught people's attention and encouraged them to ask questions and interact with PSCR.

Spectrum Management Committee – Don Root, Chair via teleconference; Charlie Sasser, Vice Chair

4.9 GHz, Don Root. Mr. Root reported a draft 6th Further Notice of Proposed Rulemaking (FNPRM) was placed on the FCC website March 1, with Commissioner voting scheduled for March 22. The draft is comprehensive and endorses much of the input from the NPSTC 4.9 GHz National Plan Recommendation. Below is a high-level comparison of the draft 6th FNPRM with current 4.9 GHz rules and with NPSTC's 4.9 GHz National Plan Recommendation.

Issue	Current Rule	NPSTC Plan	6th FNPRM
Frequency Coord.	Minimal	More Rigorous	More Rigorous
Licensing	Blanket License	Site Based	Site Based

NB traffic	Secondary	Primary on 1 MHz Channels for Backhaul	Primary on 1 MHz Channels for PTP, PTMP
Airborne Use	Prohibited	5 MHz for Airborne & Robotics	5 MHz for Manned Airborne & Robotic
Channel Aggregation	20 MHz max	20 MHz max	40 MHz max; RPC can limit to 20 MHz
Eligibility	Public Safety	Expand to CII Oppose Commercial	Questions re CII, Private, Commercial and Leasing
RPC 4.9 Plans	Optional [10 of 55 filed plans]	Nat'l Plan w RPC option on some issues	Regional flexibility on some issues; window to file plan

The 6th FNPRM has additional details and key questions. Comments will be due 60 days after publication in the Federal Register. The Spectrum Committee will reactivate its 4.9 GHz Working Group to help draft a NPSTC response. Dave Buchanan, former Chair of the 4.9 GHz Working Group in the last round, has agreed to resume his role as Working Group Chair.

6 GHz Spectrum Update, Don Root. In August 2017, the FCC issued a Notice of Inquiry on possible spectrum sharing in bands between 3.7 GHz and 24 GHz, including the 6 GHz microwave band. NPSTC filed comments on October 2, 2017. On January 26, a group of companies filed an Ex Parte and a study by RKF engineering that concluded, "unlicensed services can successfully coexist with the primary services in the 6 GHz band." NPSTC has been advised by a major carrier with 6 GHz fixed operations that it is reviewing the study. The Committee recommends waiting for those study results before commenting further.

Non-Compliant Radios, Don Root. The Land Mobile Communications Council (LMCC) has raised the issue of non-compliant radios with the FCC. The radios in question are sold mostly over the Internet for use on Part 90 spectrum. They do not meet Part 90 technical requirements, and they permit front panel programming. The LMCC met with the FCC Enforcement Bureau on March 1, to raise awareness of the issue. To the extent these radios present a risk to public safety, NPSTC also may want to consider additional action.

T-Band Update, Jim Goldstein. On February 26, Representatives Eliot Engel (D-NY16), Lee Zeldin (R-NY1), and Peter King (R-NY2) introduced the "Don't Break up the T-Band Act" (H.R. 5085). This

legislation, if enacted, would repeal the requirement that the FCC auction the public safety T-Band spectrum and that public safety move out of the band. NPSTC members have issued statements of support. This legislation is a follow up to the formation of a T-Band Coalition in December 2017 and meetings with Congressional Members and staff in mid-February. Mr. Goldstein said there will be a Senate companion bill and hopes this will occur quickly.

Mr. Root said two more members have signed the bill, Al Green, Houston, and Karen Bass, Los Angeles.

Federal Communications Commission (FCC) Filings, Charlie Sasser

Date Filed	Topic	Type of Filing
TBD	**4.9 GHz 6th FNPRM**	**Comments (tentative)**
TBD	**New Technology/Services NPRM**	**Comments (tentative)**
3/12/18	**Medical Device Waiver Request**	**Comments (in-process)**
1/31/18	**TAC Spectrum Policy Rec.**	**Comments**
	13 Filings were made in 2017.	

Federal Communications Commission (FCC), David Furth, Deputy Bureau Chief; Public Safety and Homeland Security Bureau; and Charles Cooper, Field Director, Enforcement Bureau. Mr. Cooper reported on updates at the Enforcement Bureau. The Field Office worked 1,300 investigations, mostly interference related, with one quarter related to public safety. There were no specific trends in interference identified that were mostly caused by jammers, unintentional devices causing interference, and the occasional intruder. Regarding the issue of non-compliant radios, he said, the Bureau met with the LMCC and the Spectrum Enforcement Division. The complaint asserts that uncertified devices are proliferating, including radios sold in this country that do not have proper authorization and those that can be modified or used improperly. If end users make modifications to the equipment, the Bureau must take enforcement action against the user, not the manufacturers. There have been several enforcement actions. The Bureau will work with LMCC to address this problem.

Jason Matthews, Vice Chair, Interoperability Committee, said his agency sees these radios everywhere. Mr. Haller said LMCC would like to acquire case studies of interference to forward to the Enforcement Bureau. Mr. Matthews said he would send Mr. Haller cases. Mr. Sasser complimented Mr. Cooper and his staff on the quick response he has always observed when he had had interference in his jurisdiction.

Mr. Furth reported on a significant development in the 4.9 GHz proceeding, with a FNPRM scheduled for the March 22 agenda. The draft of the FN is on the FCC website. Key elements include the plan to upgrade and revise the technical plan [drawn from NPSTC's plan]; to expand channel aggregation bandwidth limits to 40 MHz; to allow aeronautical and robotic use on 5 MHz of the band; and to require frequency coordination through the FCC's Universal Licensing System (ULS). Incumbents that have point-to-point already will need to register in the ULS, so they will have protection. Existing licensees will be grandfathered, but they also will need to register. There will be a comment period of 60 days.

Because of universal opt-ins to FirstNet, the FCC will not have to deal with any opt-outs. The Bureau adopted a Report and Order (R&O) in the 700 MHz narrowband proceeding, which added updates, dealt with the vehicular repeaters exemption, and identified interoperability features that would need testing to ensure compliance with interoperability rules. To meet the interoperability requirement in the band, radios have to be programmed to those channels out of the box. The Bureau needs to establish a uniform date by which all rules must be followed in response to a Motorola request. Mr. Furth said work on 800 MHz interstitials and Mexico rebanding is ongoing.

Mr. Haller thanked the Bureau for issuing the 4.9 GHz proceeding for comment and for including so many of NPSTC's recommendations.

NPSTC Delegate Update

Communications Security, Reliability and Interoperability Council (CSRIC) Work Group, Charlie Sasser, NPSTC Delegate. Mr. Sasser discussed the FCC CSRIC. The CSRIC pulls together experts in 911 technology to address issues in the transition from 911 to NG 911 and the complexities that will be created by adding texting to the different processes across PSAPs, including funding and staffing. Mr. Sasser serves as a volunteer on Working Group 1. The group holds weekly meetings and has identified subtasks. A survey of existing service provider detection tools is being drafted to be sent out by the end of year.

CSRIC Working Group 1was divided into two Task Teams due to the large volume of research required to accomplish the objective. One task team is focused on *911 System Reliability and Resiliency during the NG911 Transition*. The Working Group will review existing best practices and develop additional guidance regarding overall monitoring, reliability, notifications, and accountability in preventing 911 outages in transitional NG911 environments. The second task team is looking at *Small Carrier NG911 Transition* considerations. The Working Group will study and develop recommendations for the CSRIC's consideration on small carrier best practices for managing the transition to NG911.

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

Committee Roadmap, John Lenihan, Chair. Chief Lenihan reported the Committee and Working Groups are focused on the following issues:

- Monitoring use of non-P25 technologies by public safety agencies.
- Examining what nationwide interoperability communications will look like on FirstNet.
- Working with the DHS, FCC, and Canada on issues impacting cross border voice and data emergency communications.
- Studying emerging trends in healthcare and technology that will impact EMS.

Common Channel Naming Working Group, Don Root, Chair, via teleconference. Mr. Root said the Working Group is examining how Nationwide LTE Interoperable Talkgroups may function, what type of naming standard may be needed, and associated issues. What is the equivalent of 8CALL90 or UCALL40 on FirstNet? And what is the equivalent of a nationwide interoperability simplex channel on FirstNet?

The group is reviewing barriers and challenges with current use. Does a traveling first responder know if the specific LMR interoperability channel is installed in the area? And if the LMR interoperability channel is installed, is it monitored by a dispatch center?

LTE technology provides new options:

- Creation of "just in time" interoperable tactical talkgroups that service a specific geographic area around an incident. *A dispatcher could create four tactical talkgroups to support law enforcement and fire operations at the scene of a large fire and "push" those talkgroups to the designated first responder radios.*

- Use of Location Based Services data to alert a first responder of the availability of a designated MCPTT talkgroup for a specific incident. *A mutual aid engine company or EMS unit would receive an alert pushed to its device, directing them to switch to a specific talkgroup being used for an incident, and the talkgroup would have also been pushed to its device.*

- Leverage application features to provide rapid access to an interoperable communications talkgroup. *A state trooper traveling through an adjoining state could press a button on the device, which would automatically locate an appropriate (and authorized) MCPTT talkgroup for the officer to use. The display of talkgroups in the officer's device could be color coded to note which talkgroups are monitored by the PSAP and which talkgroups are reserved for tactical use, allowing the officer to select the best talkgroup to call for assistance.*

These potential new capabilities may change the landscape for interoperable communications. Local, regional, statewide, and nationwide interoperability talkgroups may be managed in a completely different way. For example, a set of local interoperability talkgroups could be established for day to day operations and also made available for out of area responders, negating the need for statewide and nationwide assignments. First responders may find it easier to access interoperability resources and may no longer have to hunt through several zones on the radio trying to find the correct channel or talkgroup.

The Working Group plans to complete a series of short use cases that illustrate the different ways that nationwide LMR interoperability channels are used today and that will discuss potential features, capabilities, and options. The group will recommend a set of naming sequences that could be used for these talkgroups, which include consideration of the items identified below and development of a report for the Governing Board with recommendations.

- MCPTT talkgroups and MCPTT off-network talkgroups.
- Specialized naming requirements for temporary tactical talkgroups created for a specific incident.
- Separate naming conventions for local, regional, statewide, and nationwide interoperability talkgroups if deemed necessary.

Emergency Medical Services Working Group, Paul Patrick, Chair. The EMS Working Group is planning to study a number of important topics this year:

- Finalize review of EMS Broadband Application List from 2014.
- Create outreach document on Prehospital Notification for Time Sensitive Emergencies.
- Assist the PS IoT Working Group with assessment of use cases involving EMS.
- Study the impact of NG911 on EMS response.

NG911 Impact to EMS may include:

- Automatic receipt of data alerts from citizen devices (e.g., heart rhythm monitoring watch).

- Automatic receipt of vehicle crash data and telemetry.
- Ability for the PSAP to visually interact with the caller (allowing for more comprehensive patient assessment, leading to additional pre-arrival medical care instructions).
- Ability for the PSAP to transfer patient data to the responding EMS unit.
- Ability for the PSAP to transfer incident data to a hospital trauma center.
- Ability for the PSAP to transfer patients to other EMS's related call centers, including those that may provide video telemedicine services.

The group will conduct literature reviews of emerging technology solutions:

- Google software that does an eye scan to assess heart attack and diabetic risk.
- Specialized Alexa software that helps homebound patients manage their diabetes and other medical conditions.
- Analytics that interpret CT body scan results for doctors in rural hospitals, who do not have immediate access to radiologists.
- Increasing use of robot type devices in hospitals to support the virtual presence of a specialist.

The group will organize presentations to monitor emerging technologies in the healthcare field that may impact EMS:

- PulsePoint citizen alerting system for cardiac arrest.
- Mobile telemedicine field solutions for first responders.
- Mobile specialty response pilot projects, including hospital-sponsored units that scan patients for stroke detection at the scene of the incident.
- Monitor UAS pilots, which support EMS response.
- Study EMS response to recent mass casualty incidents to identify voice and data communications system issues.
- Repeat the IWCE 2018 Presentation on EMS technologies for the Working Group later this month.

Town Hall Outreach, Barry Luke, NPSTC Deputy Executive Director

NPSTC's Town Hall: Public Safety Use of Social Media during Disaster Events. On January 24, NPSTC held a virtual Town Hall, a 90-minute panel presentation to discuss how public safety agencies use social media in disaster situations. There were 185 participants, who learned how social media was used in the Pulse Nightclub Shooting from Michelle Guido, Public Information Officer, Orlando Police Department; during Hurricane Harvey from Michael Walter, Public Information Officer, Houston Emergency Management; in Hurricane Irma from Alan Harris, Emergency Manager, Seminole County, Florida; and Mark Economou, Public Information Manager, Boca Raton Police Department; and during the California Wildland Fires from Daron Wyatt, Public Information Officer, Anaheim Police Department & Anaheim Fire & Rescue.

Social media has been transformational for public safety agencies.

- Creates an authoritative source for information.
- Allows faster distribution of accurate information to the public.

- Enhances the efficiency of information transfer to the media.
- Social media has diminished the need for Citizen Information Hotlines and other notification methods.
- Daily use of social media tools by public safety agencies is complementary to use of social media during disaster events.

Social media has caused some challenges for public safety agencies.

- The public expects an agency to have a social media presence, even when they do not.
- Managing social media and maintaining up-to-date, relevant information takes dedicated staff resources.
- It can be challenging to have a "two-way" conversation between the public safety agency and the citizen on social media.
- Citizens have used social media during recent disasters to call for help (both when 911 service is available and when it is not).

There are three types of social media usage by public safety agencies today:

- Outbound messaging from public safety agencies to citizens.
- Intelligence analysis, using crowd sourced social media data.
- Inbound messages from citizens to public safety agencies and PSAPs.

Outbound messaging coming from the public safety agency is the most common form of social media engagement. Agency-based websites were early examples of social media use. Facebook and Twitter are the most popular social media applications as well as commercial social media platforms like Next Door. Some public safety agencies are starting to use Facebook Live to broadcast from the incident scene.

Intelligence analysis using crowd-sourced social media data is more common in metropolitan areas with fusion centers. Information from Twitter and other social media platforms can be collected for analysis of key words and trends. Data may be used to monitor for threats during large-scale events or can help provide an early assessment of damage following a major storm. Data monitoring includes tracking of hash tags on Twitter to follow certain topics and conversations as well as information posted to public pages on Facebook. Commercial products available include Tweet Deck, Tweet Suite, and Digital Sandbox.

Inbound messages from citizens to public safety agencies and PSAPs requesting response is a relatively new issue. In many disasters, access to 911 is temporarily unavailable (due to infrastructure damage, power failure, or PSAP overload). Cellular networks are frequently impacted, limiting the public's access to social media messaging. Few public safety agencies have technology and associated policy to manage response requests from citizens, which has significant resource implications as well as data privacy and

risk management aspects. In some cases, citizen groups have established informal processes to monitor social media, and in some cases, respond to emergency requests, resulting in confusion.

Some of the lessons learned include the comment from a panel participant that while social media is extremely effective, it is important not to put the entire outreach plan on social media to assist older citizens or those who do not have access to social media. During Hurricane Harvey, citizens experienced a 2-to 3-hour wait for 911 to be answered. Most people relied instead on social media to ask for help, a scenario that had not previously occurred. The Pulse Nightclub shooting was completely different with no warning that the incident would occur. PIOs had to respond on the fly.

Mr. Luke asked the panel participants the following questions:

- Are the existing software tools that you use to manage social media sufficient for public safety use? (Is there a technology gap between what is available and what is needed?) *Most answered they are not. Some of the tools and software require specialized training.*
- Did you find any operational gaps in managing social media information between the PIO, the PSAP, and Incident Command? *Agencies that were collaborative or worked on a regional level had better results.*
- What social media challenges do you think public safety agencies will experience in the future, including instances where citizens post messages seeking emergency response*? Agencies believe citizens will call for help on social media, and they will need to develop procedures to manage that. NG911 that will allow text or imaging to a PSAP may be an answer when it is implemented.*

The Town Hall presentation is available on the NPSTC YouTube Channel (accessible from the home page on the NPSTC website). Follow-up discussions have occurred with DHS S&T and with the U.S. Coast Guard. Both agencies are studying this issue. NPSTC is evaluating other topics for future Town Hall presentations.

Ms. Ward said NPSTC received an excellent response to the Town Hall, asking the Board if there was interest in hosting similar forums and what topics members would like to see examined. John Contestabile, Chair, VTAG, suggested public safety applications for the broadband environment would be a good topic.

Affiliate Organization Member Update

TETRA Critical Communications Association (TCCA), Tony Gray, Chief Executive Officer. Mr. Gray reported on TCCA and its recent activities. He said the organization is now known solely as TCCA to reflect its focus on critical communications. Members are end users, operators, industry, and other stakeholders globally sharing knowledge and experience. TCCA catalyzes and drives the evolution of commercial 4G/5G towards providing truly critical communications grade bearer networks; facilitates the maintenance, development, and enhancement of relevant ETSI standards, e.g., TETRA; and manages the test and certification processes. TCCA supports open standards for mobile communications. Its working groups cover similar areas to NPSTC's and include applications, broadband industry, transport, and a technical group.

TCCA held a successful MCPTT plug test in June 2017; the MCPTT plug test#2 will occur on June 25-29 with the National Institute of Standards and Technology (NIST) and FirstNet in the United States. Through a grant from PSCR, TCCA is part of a consortium with the University of Basque Country, Expway, and Bittium to develop and publish and an open source platform and APIs for MCPTT apps. With GCF [Global Certification Forum], TCCA is collaborating on a work item for testing and certification of Mission Critical User Equipment (UE) devices.

Project 25 Technology Interest Group (PTIG), Steve Nichols, Director. Mr. Nichols briefed the Board on the activities of the PTIG. The biggest, new change in P25 technology is link layer encryption. P25 end-to-end-encryption for voice calls and packet data protects the contents of the transmission. End-to-end encryption by itself does not protect against intercepting the identities of the parties involved in a call. P25 link layer encryption helps ensure the following:

- Integrity: How can a user know the message has not been altered in some way?
- Specifically Replay Protection ensures that a message cannot be resent later by an untrusted source.
- Confidentiality: How can the user be sure that the message is only received by the intended parties?
- Key Distribution: Do the initiating and receiving parties have the means to securely communicate?

Today, interfaces between the Key Management Facility (KMF), Authentication Facility (AF), and Key Fill Device (KFD) are proprietary. This presents challenges for interoperability between different P25 manufacturers. There is no impact on the interface between the KMF and Subscriber Unit (SU) with this change. It should allow support for legacy devices with new/updated KFDs. There is still some time until the standard is published, and equipment that conforms to the standard is typically available 12 to 18 months after publication of a standard. Mr. Nichols provided a list of updated documents available on the PTIG website.

P25 Compliance. He discussed what P25 compliance means, saying while it is not strictly defined, most consider "compliance" to mean adherence to published documentation. The P25 SoR [Statement of Requirements] is created by the users and drives P25 standard creation/content. The P25 standards enable interoperability. P25 standard tests describe consistent methods for testing implementations against a published standard (Performance, Conformance, and Interoperability).

Compliance in the context of the P25 SoR includes the following:

- P25 SoR is created and maintained by P25 Steering Committee's User Needs Subcommittee (UNS).
- UNS' view of what interfaces, services, features, etc., that should be addressed by P25 standards and/or implemented in P25 systems/equipment and includes importance ranking (Mandatory, Standard Option, Standard Option-Required).
- P25 SoR is not part of the P25 Standard. Compliance statements at this level mean the functionality described in the SoR has been implemented.
- The P25 SoR contains high-level descriptions of functionality that do not enable interoperability.

- Most SoR items trace to published P25 standards; however, some do not.

Compliance in the context of the P25 Standards means:

- Manufacturers selectively implement standard functionality based on the customers they serve: P25 Interfaces (Air, Wireline, etc.); P25 Services (Data, Security, etc.); P25 Features (Group call, Ind call, etc.)
- Compliance statements at this level mean some set of functionality covered by the P25 Standard documents has been implemented per the document and is expected to interoperate.

Compliance in the context of the P25 Standard Tests. Compliance statements at this level mean the implemented functionality produces the specified results under the specified conditions for:

- Performance: Standard measurement methods with associated specifications (primarily applies to RF).
- Conformance: Standard feature operation with proper message sequence and message content.
- Interoperability: Standard feature operation between equipment of different manufacturers.

Compliance in the context of the DHS OIC CAP means the functionality has been implemented per the P25 Standard document(s) and will pass the associated P25 Standard Test(s) covered by published CABs, testing has been done in CAP recognized labs, and reports have been approved by DHS OIC.

- Recommended Compliance Assessment Test Telecommunication Systems Bulletins (RCAT TSBs).
    - Created by the industry and user community TIA members, who produce and maintain the P25 Standard documents and P25 Standard Test documents, and are endorsed by the P25 Steering Committee.
    - Provided to the DHS OIC CAP Advisory Panel for consideration when drafting or revising Compliance Assessment Bulletins (CABs).
    - RCATs are P25 recommendations for P25 tests appropriate for use when assessing P25 standard compliance of a product.
    - CABs define testing and test result reporting for the DHS OIC Compliance Assessment Program.

University of Melbourne Centre for Disaster and Public Safety (CDMPS), Geoff Spring. Mr. Spring provided a briefing on CDMPS, which has completed its 3-year review and has published a *CDMPS 2014-2017 Report*. CDMPS has launched a new research strategy with the following research priorities.

- Understanding and mitigating extreme events and critical incidents.
- Enabling technology, informatics, and analytics.
- Improving whole life infrastructure system performance and resilience.
- Strengthening organizational, institutional, and community resilience.
- Enhancing policy and decisionmaking.

CDMPS partners on various initiatives with NPSTC, PSCR, P25, APCO [Association of Public-Safety Communications Officials] Canada , British APCO, CommsConnect Conference Organiser, the United Nations, Centre for Spatial Data Infrastructure and Land Administration, On [Connected Vehicles], and the Australian Radio Industry Communications Association.

Mr. Spring complimented NPSTC on its work, saying Australia is pleased to work with this group. Mr. Haller and Mr. Spring signed a new 2-year MOU between NPSTC and the University of Melbourne through the CDMPS.

Upcoming Meetings. NPSTC will meet by teleconference on Tuesday, May 15, 2018; and in Washington, D.C., at OCTO on Wednesday, September 5, and Thursday, September 6, 2018. Mr. Goldstein said the May date may conflict with a SAFECOM meeting. Ms. Ward said staff will research alternative dates.

Adjournment. Mr. Goldstein moved to adjourn the meeting. Paul Szoc, International Municipal Signal Association (IMSA), seconded. The meeting adjourned at 12:10 p.m. ET.