

NPSTC

Full NPSTC Meeting | Orlando, FL

Friday, March 9, 2018

Conference Line: (510) 227-1018 | Conference ID: 192 7086

Screen Share: https://join.me/NPSTCsupport1

Submit Questions Online

Send email to support@npstc.org

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

“Life is Good with Dunkin’ Donuts.”

Drink a cup of Dunkin’ Donuts coffee to **Tom Sorley** and remember all of his contributions to the public safety community.

He will be greatly missed!

ANDREWSEYBOLD

PUBLIC SAFETY ADVOCATE
ANDREWSEYBOLD.COM

Welcome and Opening

- Doug Aiken, NPSTC Vice Chair
  - Call to Order
  - Pledge of Allegiance
  - Roll Call
- Technical Tips
  - Webinar Access Information: https://join.me/NPSTCsupport1
  - Online participants submit questions to support@npstc.org. Do NOT use the the join.me chat bubble, it will be displayed to all.
  - To mute your phone, press *6, NOT hold.
  - Email attendance to attend@npstc.org.

Pledge of Allegiance

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

4

Role Call
Governing Board Organizations

- American Association of State Highway Transportation Officials (AASHTO)
- American Radio Relay League (ARRL)
- Association of Fish & Wildlife Agencies (AFWA)
- Association of Public-Safety Communications Officials-International (APCO)
- Forestry Conservation Communications Association (FCCA)
- International Association of Chiefs of Police (IACP)
- International Association of Emergency Managers (IAEM)
- International Association of Fire Chiefs (IAFC)
- International Municipal Signal Association (IMSA)
- National Association of State Chief Information Officers (NASCIO)
- National Association of State Emergency Medical Services Officials (NASEMSO)
- National Association of State Foresters (NASF)
- National Association of State Technology Directors (NASTD)
- National Council of Statewide Interoperability Coordinators (NCSWIC)
- National Emergency Number Association (NENA)
- National Sheriff's Association (NSA)

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

5

Welcome

- Associate Organizations
  - Canadian Interoperability Technology Interest Group (CITIG)
  - Utilities Telecom Council (UTC)

- Affiliate Organizations
  - Alliance for Telecommunications Industry Solutions (ATIS)
  - Open Mobile Alliance (OMA)
  - Telecommunications Industry Association (TIA)
  - TETRA Critical Communications Association (TCCA)

Welcome

- Liaison Organizations
  - Federal Communications Commission (FCC)
  - Federal Emergency Management Agency (FEMA)
  - Federal Partnership for Interoperability Communications (FPIC)
  - National Telecommunications and Information Administration (NTIA)
  - Public Safety Communication Europe (PSCE)
  - SAFECOM Program
  - U.S. Department of Homeland Security, Office for Interoperability and Compatibility (OIC)
  - U.S. Department of Homeland Security, Office of Emergency Communications (OEC)
  - U.S. Department of Justice (US DOJ)
  - U.S. Department of the Interior (US DOI)
  - University of Melbourne Center for Disaster Management and Public Safety (CDMPS)

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

7



NPSTC

Federal Partners Update

Department of Homeland Security (DHS), Office for Interoperability and Compatibility (OIC)

John Merrill, Director

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

DHS SCIENCE AND TECHNOLOGY

Briefing for NPSTC

NEXT GENERATION FIRST RESPONDER APEX PROGRAM

March 9, 2018

Homeland Security

Science and Technology

John Merrill

Director

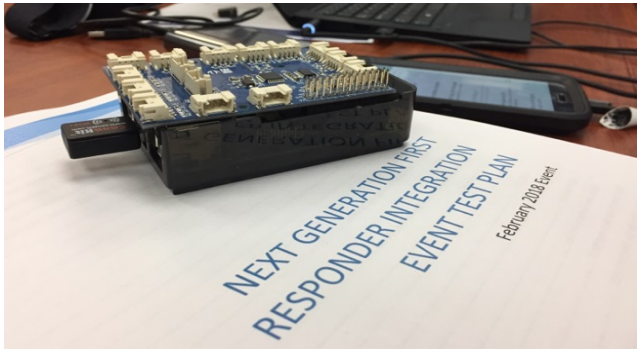
Office for Interoperability and Compatibility

Science and Technology Directorate

Integration Demonstrations

NGFR integration demonstrations have evolved into exercises with partner public safety agencies to produce knowledge products to facilitate technology implementation.

https://edit.dhs.gov/science-and-technology/ngfr



- **Grant County TechEx NGFR Case Study Series**
  - Deployable Communications, Location Services, and Video Services released in 2017.
  - Physiological Monitoring, Situational Awareness and Raspberry Tech Bulletin will be released in March 2018.
- **NASA JPL PlugTest – February 2018**
  - Integrated technologies from performers with a variety of modules which will inform the 2018 NGFR/Harris County, TX Operational Experimentation (OpEx).
  - After Action Report will be released mid-to-late 2018.

NGFR Integration Handbook

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. NGFR is requesting industry feedback.

Part One - Provides an introduction and overview of the NGFR on-body framework and the concepts behind its modular design.

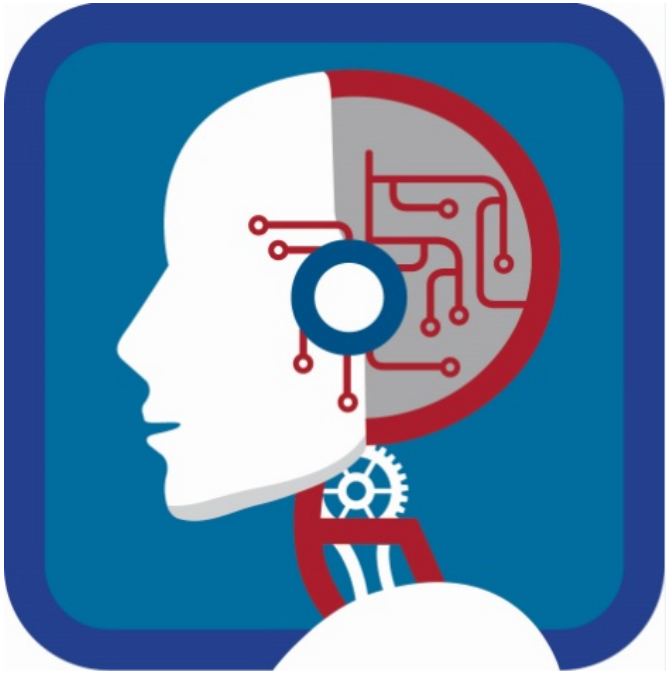
Part Two - Targets engineers and details engineering design for module-to-module communications and data transfer from on-body systems to agency systems, including the interfaces, services and standards.

Part Three - Targets software developers and engineers to guide modular development; provides additional details of the data architecture for modules and their interfaces

AUDREY Pilot Programs

Assistant for Understanding Data through Reasoning, Extraction & sYnthesis

In 2017, NGFR partnered with U.S. and international public safety agencies to begin pilot programs for the AUDREY artificial intelligence solution.

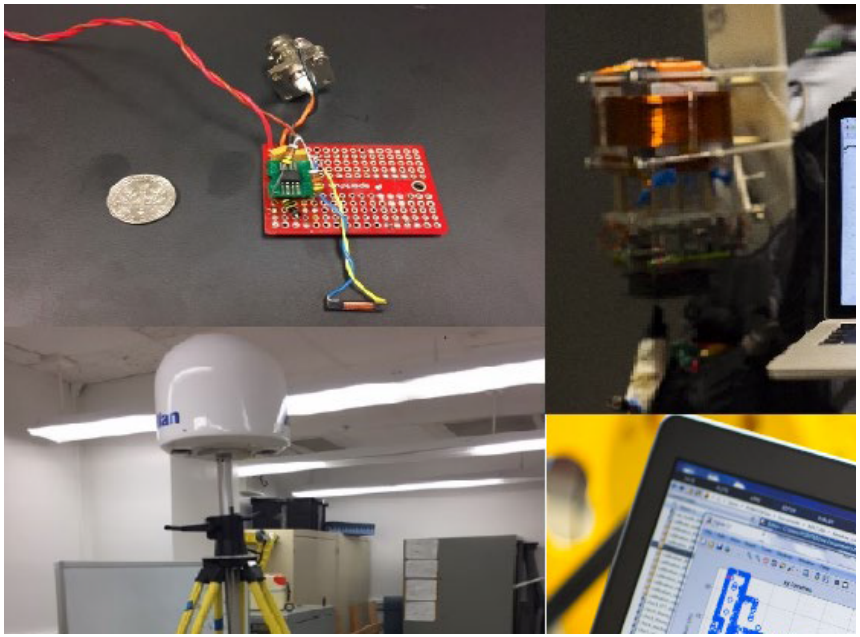


- Continued partnership with Grant County, Washington Multi-Agency Communications Center.
- New partnership with Defence Research and Development Canada and Hastings-Quinte Paramedic Services.
- Discussions with:
  - US Coast Guard
  - Office of Health Affairs
  - Sacramento PSAP

POINTER

Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders

Precision positioning sensor system that locates first responders via low-frequency magnetic fields and can transmit signals through materials, including wood, concrete, brick and rebar.



- Testing of miniaturized receiver, transmitters and UHF wireless communications link will occur May – September 2018.
- Version One will be commercially available mid-to-late 2019.
- First release will target rural homes, warehouses and low-rise buildings.
- Next phase to focus on high-rise buildings, outdoor and underwater environments and tunnels.

Advanced Multi-Purpose Base Ensemble Uniform (AMBER)

Designed and developed as a multi-threat base protective ensemble, the AMBER project's anticipated completion date is mid-to-late 2018.

- Grant County, Washington fire departments to begin testing early 2018.
- International partners interested in testing:
  - Sweden
  - United Kingdom
  - Canada
- Collecting data for transitioning weather April-July, 2018.

Other Programs/Projects

- Tracking of Emergency Patients (TEP)
- CAUSE – Next steps
- CA/US Collaboration
- LA County Sheriff
- UCF AR/VR HUD
- Harris County Spiral III
- Plug Fest
- JAM-X 2019

Engage With Us!

DHS S&T Next Generation First Responder Apex Program

EMAIL
NGFR@hq.dhs.gov

DHS S&T FIRST RESPONDERS GROUP

WEBSITE
www.FirstResponder.gov

TWITTER
@dhsscitech

EMAIL
First.Responder@dhs.gov

FACEBOOK
@FirstRespondersGroup

Homeland Security

Science and Technology



NPSTC

Federal Partners Update *(continued)*

Department of Homeland Security (DHS), Office of Emergency Communications (OEC) – Ron Hewitt, Director

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.



NPSTC

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

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

NPSTC Federal Partners Update

Kevin McGinnis and Dave Buchanan, First Responder Network Authority

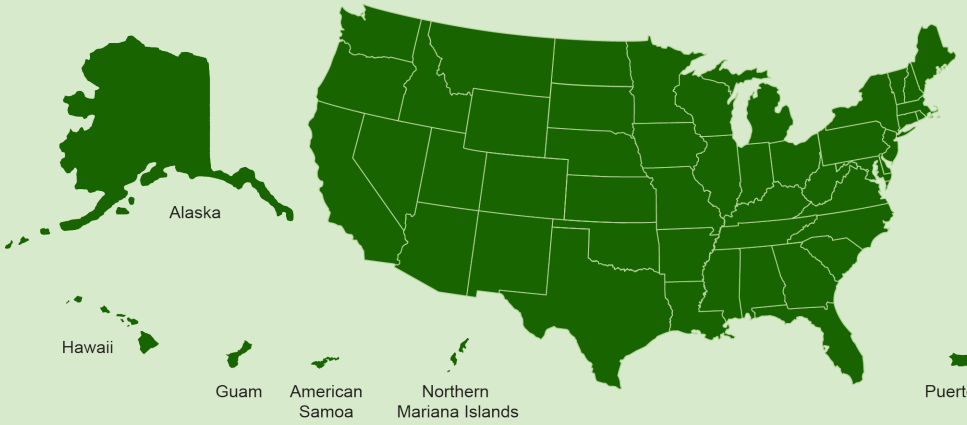
56 U.S. States/Territories are Onboard with FirstNet

Benefits of opt in

FirstNet – the network public safety fought for and needs for its vital mission – is a reality, delivering nationwide interoperability and key features now:

- **Priority & preemption**
- **Better sustainability**
- **Greater security**
- **More efficiencies**
- **Enhanced coverage & capacity**

States/territories on FirstNet



50
States
6
Territories and Washington, D.C.

What's coming in 2018

Expanding FirstNet: The First Responder Network Authority will issue work orders to deploy RANs in opt in states/territories, giving AT&T the green light to expand the network to provide the bandwidth and mission-critical connections for public safety users

Driving innovation: FirstNet will unlock a new technology marketplace for public safety, enabling first responders to benefit from the latest lifesaving technologies and applications

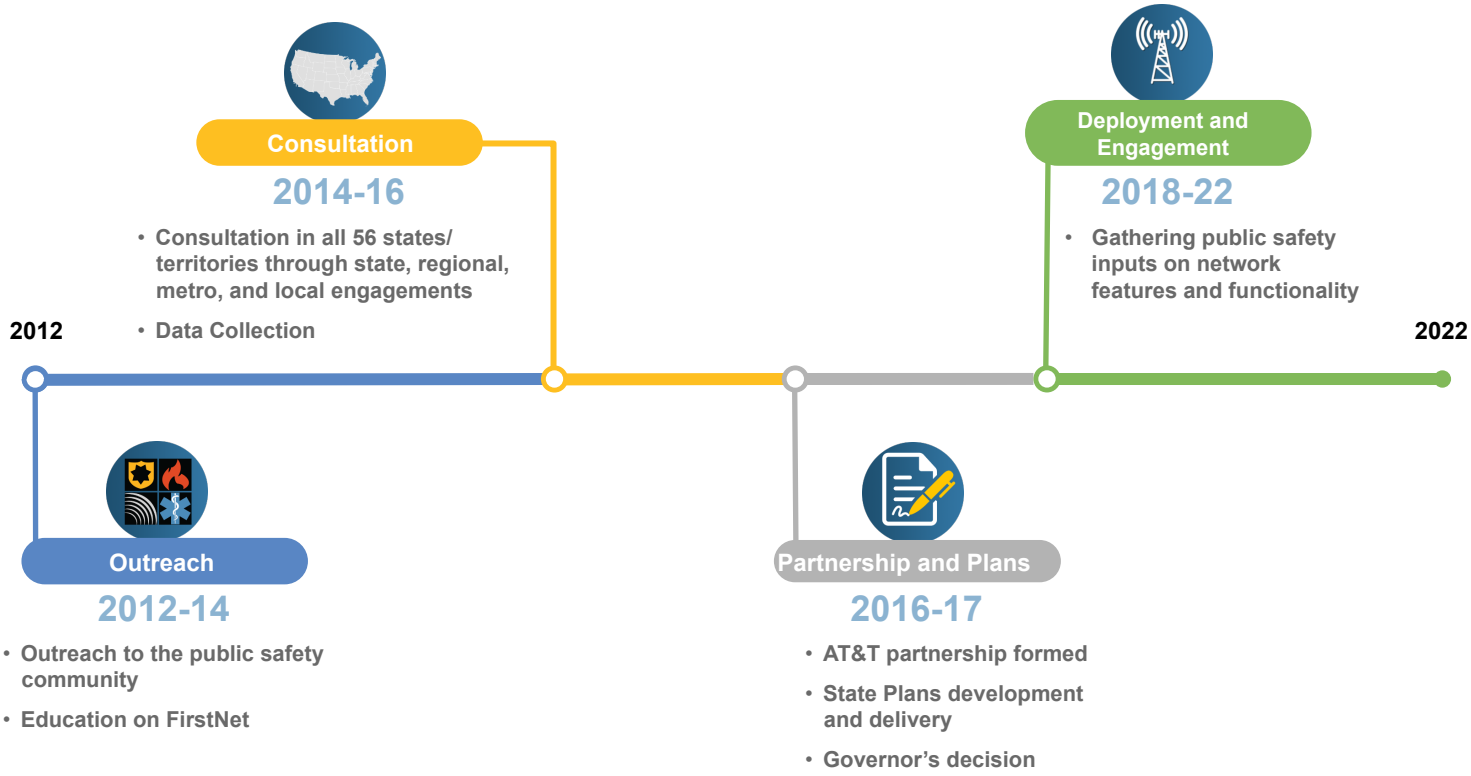
Securing emergency communications: FirstNet's first-of-its-kind core infrastructure will give first responders a dedicated, highly secure network with full encryption and end-to-end cybersecurity

Consultation with public safety: The First Responder Network Authority will continue to engage with public safety, states, territories, federal agencies, and tribal nations to ensure the network meets their needs

FirstNet

FirstNet

FirstNet's Journey



FirstNet®

Public safety priorities

- Public safety always gets priority
- Highly secure network to meet public safety's data requirements
- Controlled access by public safety agencies for their users
- Coverage where public safety operates
- Enhanced user experience

FirstNet®


FirstNet®

FirstNet NPSBN Development

Public Safety Advisory Committee

Paul Patrick, Interim PSAC Chair



NPSTC

Public Safety Communications Research (PSCR)

Dereck Orr, Acting NIST CTL Lab Director, PSCR Division Chief

Via teleconference

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.


PSCR Program Summary
PSCR
NIST
OPEN INNOVATION TO SOLVE PUBLIC SAFETY COMMUNICATIONS
Play clip
0:01 / 1:35
NIST



NPSTC

Technology and Broadband Committee

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

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Technology and Broadband Committee Roadmap

- The Committee and Working Groups are focused on six major areas:
  - 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

Technology and Broadband Committee Roadmap

- The Committee and Working Groups are focused on six major areas (continued):
  - 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

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Public Safety Internet Of Things Use Case Development

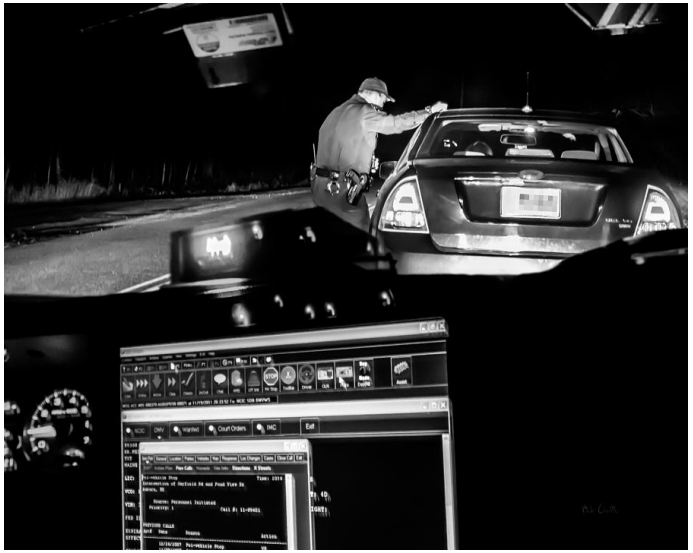
- The PS IoT Working Group has been developing use cases to fully understand the way in which sensors and devices will impact public safety

Public Safety Internet Of Things Use Case Development

- A law enforcement traffic stop use case was discussed on the past two working group calls.
- A wide range of IoT devices were reviewed:
  - Speech to Text CAD/MDT entry and database inquiry,
  - License Plate Reader (LPR) cameras,
  - Body camera and dash camera,
  - Automated database inquiries and alerts,
  - Location Based Services assess officer safety,
  - Safety sensors detect potential threats, a struggle, or an officer down,
  - Equipment sensors alert dispatcher when firearm is removed from holster, or fired; or other gunshots are detected.

Public Safety Internet Of Things Use Case Development

- IoT devices must also successfully operate under a wide range of environmental conditions:
  - Daylight, partial light and nighttime operations,
  - Wind, rain, snow,
  - Cold, hot and humid conditions.



Public Safety Internet Of Things Device, Networks, Identity

- 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 is it coming from a tablet or laptop?

Public Safety Internet Of Things Use Case Development

- Initial impression of 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.
    - First responder must not be distracted by normal interaction with the IoT device, yet must receive urgent alerts immediately.

Public Safety Internet Of Things Use Case Development

- Initial impression of PS IoT devices:
  - Must provide data and analysis that is accurate, credible, and helpful to the first responder's mission.
    - False alerts must be minimized.
    - Latency of data delivery must be minimized to provide mission critical services.
      - Time lag between sensor detection, analysis and alert to the first responder must be assessed.

Public Safety Internet Of Things Use Case Development

- Next Steps:
  - Finish review of use cases
    - 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)
  - Prepare Report for the Governing Board on the PS IoT ecosystem, noting important issues and opportunities.
  - Create outreach documents for public safety that highlight important considerations with IoT usage.

Break



NPSTC

Spectrum Management Committee

Don Root, Chair *via teleconference*

Charlie Sasser, Vice Chair

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Committee Issue Update

- **4.9 GHz** – Don Root
- **6 GHz Spectrum Update** – Don Root
- **Non-Compliant Radios** - Don Root
- **T-Band Update** – Jim Goldstein
- **Federal Communications Commission (FCC) Filings** – Charlie Sasser

4.9 GHz

- A draft 6th FNPRM was placed on 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.
- Next slide provides high level comparison of draft 6th FNPRM with current 4.9 GHz rules and with NPSTC 4.9 GHz National Plan Recommendation.
- 6th FNPRM has additional details and key questions.

4.9 GHz – High Level Summary Comparison

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

4.9 GHz – Going Forward

- Timing
  - FCC Voting on 6th FNPRM March 22.
  - Comments will be due 60 days after publication in the Federal Register, so possibly late May/early June timeframe.
- The Spectrum Committee will reinvigorate its 4.9 GHz Working Group to help draft a NPSTC response.
- Dave Buchanan, chair of the 4.9 GHz WG in the last round, has agreed to continue as Working Group Chair.

6 GHz Spectrum Update

- In August 2017, 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 October 2, 2017
- On January 26, a group of companies filed an Ex Parte and a study by RKF engineering that concludes "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 it is reviewing the study.
- The Committee recommends waiting for those study results before commenting further.

Non-Compliant Radios

- The Land Mobile Communications Council (LMCC) has raised the issue of non-compliant radios with FCC.
- The radios in question:
  - Are sold mostly over the internet for use on Part 90 spectrum;
  - Do not meet Part 90 technical requirements; and
  - Permit front panel programming.
- LMCC met with 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

- 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 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 formation of a T-Band Coalition in December 2017 and meetings with Congressional Members and staff in mid-February.

NPSTC Regulatory Filings for 2018

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.	



NPSTC

Federal Partners Update *(Continued)*

Federal Communications Commission (FCC)

David Furth, Deputy Bureau Chief *via teleconference*

Charles Cooper, Field Director

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.


NPSTC

NPSTC Delegate Update

Communications Security, Reliability and Interoperability Council (CSRIC) Work Group

Charlie Sasser, NPSTC Delegate

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

CSRIC UPDATE - WG1

- **Transition Path to NG911**
  - ***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.
  - ***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.

CSRIC UPDATE - WG1

- CSRIC Working Group One was divided into two Task Teams due to the large volume of research required to accomplish the objective.

Working Group 1 Task 1

- Objective
  - ***911 System Reliability and Resiliency during the NG911 Transition***: 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.

Working Group 1 Task 1 Status

- Working Group Meetings.
  - Weekly meetings established.
  - Sub tasks defined and members assigned to:
    - Identifying Transitional Risks/Demarcation Points,
    - Outage Prevention, Reporting and Notification.
- Draft outline developed.
- Survey of existing service provider detection tools is being drafted.
  - Expect survey to be administered by ATIS/NRSC.
  - Survey to be sent out by end of year.

Working Group 1 Task 2

- Objective
  - ***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.

Working Group 1 Task 2 Status

- Working Group Meetings
  - Weekly meetings established on a regular schedule.
  - Sub tasks defined and membership identified.
- Draft outline developed to initiate discussion on further outline details.
- Organized members around outline framework.



NPSTC

Interoperability Committee

John Lenihan, Interoperability Committee Chair

Jason Matthews, Vice Chair

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Interoperability Committee Roadmap

- 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 *via teleconference*, Chair

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Common Channel Naming Overview

- Examining how Nationwide LTE Interoperable Talkgroups may function and what type of naming standard may be needed.
  - What is the equivalent of 8CALL90 or UCALL40 on FirstNet?
  - What is the equivalent of a nationwide interoperability simplex channel on FirstNet?
- Issues
  - Reviewing barriers and challenges with current use.
    - Does a traveling first responder know if the specific LMR interoperability channel is installed in the area?
    - If the LMR interoperability channel is installed, is it monitored by a dispatch center?

Common Channel Naming

- 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 their device directing them to switch to a specific talkgroup being used for incident; and the talkgroup would have also been pushed to their device.

Common Channel Naming

- LTE Technology Provides New Options:
  - Leverage application features to provide rapid access to an interoperable communications talkgroup.
    - A state trooper traveling through an adjoining state could press a button their device which would automatically locate an appropriate (and authorized) MCPTT talkgroup for the officer to use.
    - The display of talkgroups in the officers 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.

Common Channel Naming

- LTE Technology Provides New Options:
  - 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).

Common Channel Naming

- Next Steps:
  - Complete a series of short use cases that illustrate the different ways that nationwide LMR interoperability channels are used today.
  - Discuss potential features, capabilities and options.
  - Recommend a set of naming sequences that could be used for these talkgroups, which include consideration of:
    - 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.
  - Report for the Governing Board with recommendations.

Emergency Medical Services Working Group

Paul Patrick, Chair

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Emergency Medical Services 2018 Work Plan

- 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.

Emergency Medical Services 2018 Work Plan

- 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.

Emergency Medical Services 2018 Work Plan

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

Emergency Medical Services 2018 Work Plan

- EMS Working Group topics, continued:
  - Organize presentations to monitor emerging technology 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.



NPSTC

Town Hall Outreach

Barry Luke, NPSTC Deputy Executive Director

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Public Safety use of Social Media During Disaster Events

Barry Luke, Deputy Executive Director

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Social Media Town Hall
Public Safety Use in Disasters

- On January 24th, NPSTC held a virtual Town Hall presentation to discuss how public safety agencies use social media in disaster situations.
  - 185 participants joined the 90 minute panel presentation.

Introduction of Panel Members

Daron Wyatt
Public Information Officer,
Anaheim Police Department/Anaheim Fire and Rescue
Incident: California Wildland Fires

Alan Harris,
Emergency Manager,
Seminole County, Florida

Mark Economou,
Public Information Manager,
Boca Raton Police Department
Incident: Hurricane Irma

Introduction of Panel Members

Michael Walter,
Public Information Officer,
Houston Emergency Management
Incident: Hurricane Harvey

Michelle Guido,
Public Information Officer,
Orlando Police Department
Incident: Pulse Nightclub Shooting

Public Safety Use of Social Media Today

- Social media has been transformational for public safety agencies.
  - Creates authoritative source for information.
  - Allow faster distribution of accurate information to the public.
  - Enhance 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 complimentary to use of social media during disaster events.

Public Safety Use of Social Media Today

- Social media has caused some challenges for public safety agencies.
  - Public expects an agency to have a social media presence, even when they don't.
  - 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).

Public Safety Use of Social Media Today

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

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

Public Safety Use of Social Media Today

1. Outbound messaging from public safety agencies.
   - This 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.

Public Safety Use of Social Media Today

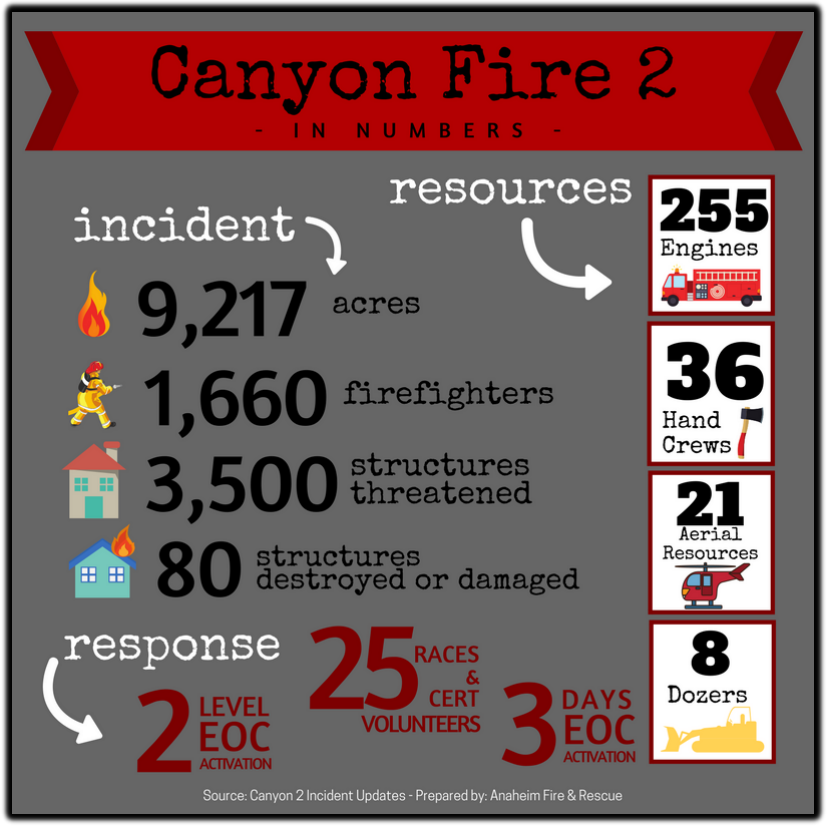
2. Intelligence analysis using crowd sourced social media data.
   - More common in metropolitan areas with UASI Fusion Centers.
   - Information from Twitter and other social media platforms can be collected for analysis of key words and trends.
   - Data may be used to monitor for threats during large 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 include Tweet Deck, Tweet Suite, Digital Sandbox.

Public Safety Use of Social Media Today

3. Inbound messages from citizens to public safety agencies and PSAPs requesting response.
   - This is a relatively new issue.
   - In many disasters, access to 911 is temporarily unavailable (due to infrastructure damage, power failure, or PSAP overloaded).
   - 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 have significant resource implications as well as data privacy and risk management aspects.
   - Citizen groups have established informal processes to monitor social media and, in some cases respond, to emergency requests resulting in confusion.

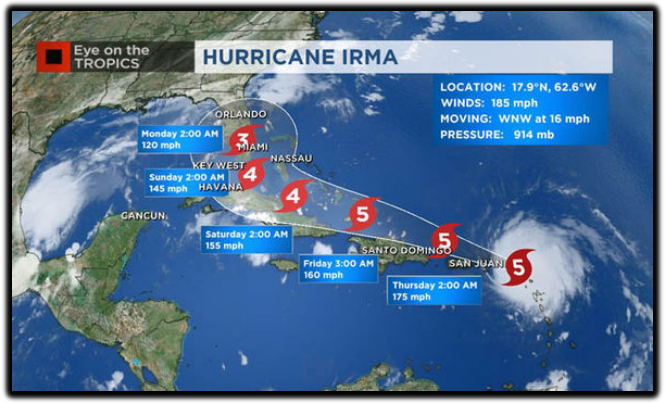
California Wildland Fires

- Canyon Fire 2 started on October 9, 2017.
- Fed by 50 mph Santa Ana winds.



Hurricane Irma

- Category 5 hurricane.
- Strongest storm on record in the open Atlantic region.
- Developed on August 30, 2017.
- Made landfall in Cudjoe Key, Florida on September 10th.
- Caused 134 deaths (across all impacted countries).



Hurricane Harvey

- Struck the Texas coast on August 24, 2017.
- Costliest tropical cyclone on record ~125 billion in damage.
- 40” of rain in a four day period, some areas received 60”.
- Displaced 30K residents, prompting 17K rescues.

Pulse Nightclub Shooting

- June 12, 2016
- Terrorist Attack at the Pulse Nightclub
- Killed 49 people and wounded 58 others
- Was the deadliest attack since September 11th
  - Was surpassed by the Las Vegas shooting in 2017

Panel Discussion

- 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?)
- Did you find any operational gaps in managing social media information between the PIO, the PSAP and Incident Command?
- Who was involved in the creation of your agency (or regional) social media policy?
- What social media challenges do you think public safety agencies will experience in the future, including instances where citizens post messages seeking emergency response?

Social Media Town Hall
Public Safety Use in Disasters

- The Town Hall presentation is available on the NPSTC You Tube Channel (accessible from our main web site).
- Follow up discussions occurred with DHS S&T and with the U.S. Coast Guard, both agencies are studying this issue.
- We are evaluating other topics for future Town Hall presentations.
  - If you have suggestions, please let Marilyn Ward know.



NPSTC

Affiliate Organization Member Update

TETRA Critical Communications Association (TCCA)

Tony Gray, Chief Executive

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.

Presentation to Governing Board

NPSTC
National Public Safety Telecommunications Council

March 2018

Tony Gray
Chief Executive

Critical communications for all professional users

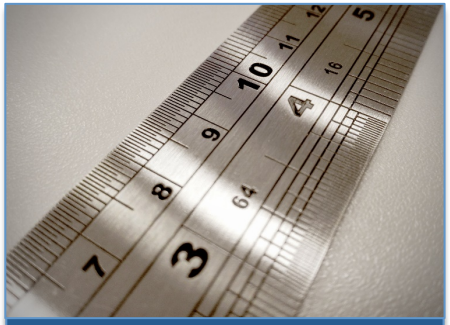
Topics

About us

Recent News

Critical communications for all professional users

Supporting all critical communications professionals



Supporting open and standardised mobile critical communications technologies and complementary applications.

Catalysing competitive multivendor markets worldwide through open standards and harmonised spectrum.

Members are end users, operators, industry and other stakeholders globally sharing knowledge and experience.

Collaborative working across the critical communications ecosystem to develop and drive the most effective solutions for all.

Critical communications for all professional users

Working Groups

The key elements of our work are driven by TCCA Working Groups open to all qualified members, including:

- Applications Working Group
- Broadband Industry Group (BIG)
- Critical Communications Broadband Group (CCBG)
- International Critical Control Rooms Alliance (ICCRA)
- Marketing Group & Events Task Force
- Operator User Association (OUA)
- SCADA, Smart Grid and Telemetry Group
- Security and Fraud Prevention Group (SFPG)
- Technical Forum (TF)
- TETRA Industry Group (TIG)
- Transport Group

How we work

We inform, advise and have a strong influence on the direction of the critical communications sector.

3GPP™ A GLOBAL INITIATIVE

We catalyse and drive the evolution of commercial 4G/5G towards providing truly critical communications grade bearer networks.

We facilitate the maintenance, development and enhancement of relevant ETSI standards, e.g. TETRA, and manage the test & certification processes.

Critical communications for all professional users

Recent news

Successful MCPTT plugtest June ’17

MCPTT plugtest#2
25th – 29th June 2018 with NIST & FirstNet in USA

Consortium with University of Basque Country, Expway & Bittium to develop & publish Open Source platform and APIs for MCPTT apps

Collaboration on work item for testing and certification of Mission Critical User Equipment (UE) devices

Critical communications for all professional users

Thank you

Questions / Comments?

Tony Gray
Chief Executive
Mob: +48 69 228 2883
Email: tony.gray@tcca.info
www.tcca.info

Critical communications for all professional users

Affiliate Organization Member Update

Project 25 Technology Interest Group (PTIG)

Steve Nichols, Director

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

International Wireless and Communications Expo
Orlando, Florida
NPSTC Meeting, March 9, 2018

Project 25 Update for NPSTC

New Standards, Applications, and Interoperability

Presented by:
PTIG - The Project 25 Technology Interest Group

www.project25.org

PTIG P25 Update

- New P25 Security Standards and Updates
  - Link Layer Encryption
  - Encryption Key Fill Device (KFD) Updates
  - P25 Authentication
- P25 Standards Update: TIA TR-8 meetings, Feb 6-8 2018
- What is P25 Compliance????
- PTIG Update
  - New P25 Statewide Systems List
  - New White Papers: P25 Authentication, P25 Trunking Control Channels
  - New P25 Benefits Docs:
    - P25 Top 10 Benefits for non technologist Users
    - P25 Value Proposition for Agency Administrators, procurement managers

Link Layer Encryption (LLE) Problem Statement

- P25 Link Layer Encryption helps ensure the following:
  - Integrity – How can you 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 you 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?

LLE Problem Statement

- 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
  - Initiator of a Call (Typically a User ID)
  - Target of a Call (Typically a Group ID but may be a Supergroup or another User ID)

From: Jeremy
To: Bill
Message: Q@#$
%DFG%^&

LLE Affected Standards

Standard Number (TIA-102.x)	Title	Effect	Status
TBD	Link Layer Encryption Overvie		Ready to move to TR8.3
AABB-B	Trunking	mats for LLE control BKs and MBTs.	Not started
AA		Addition of ISPs and OSPs in support of LLE operations and LLE key management	
	ocedures	Addition of procedures f	
	Conventional Procedures	Addition	
BBAC	Phase 2 Two-Slot TDMA Medi Access Control Layer P		
BAAA-A	FDMA C		
BA		on in nt.	Not started
		aging and procedures for anagement.	Not started
		Addition of messaging and procedures for LLE key management.	In-Progress – Covered Later
AA	tocol	Addition of messaging and procedures for LLE key management.	Not started

LLE standardization is a major effort with many impacts on existing P25 standards.

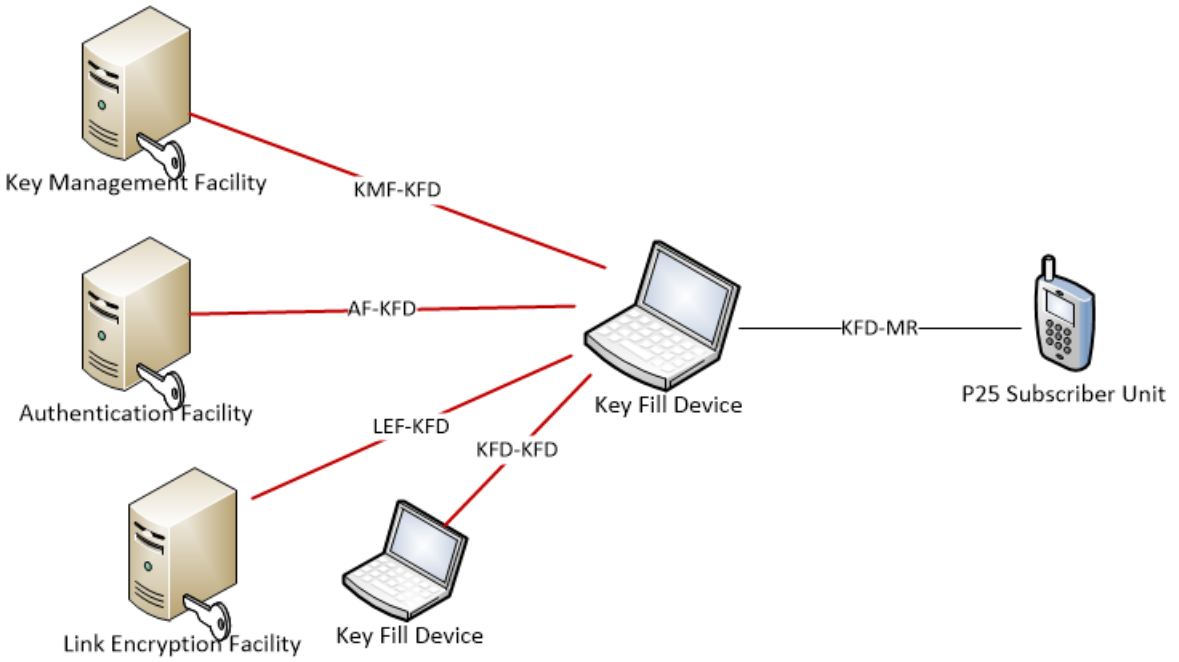
The LLE Overview document establishes the architecture; including the interfaces, published standards, and new standards that are needed.

LLE Important User Considerations

- Update to P25 standards for LLE will have no impact on users that don't require LLE.
- LLE will support interoperability with legacy subscriber units that don't support LLE and subscriber units that support LLE on the same network.
  - For example in P25T, the standards will support a mix of protected & unprotected groups operating on the same site.
- Key management is designed to be as seamless as possible – supporting distribution of future keys before they take affect.
- Protection of the RLEK (& derived CLEK) is very important.
- There is still some time until the standard is published and equipment that conforms to the standard is typically available 12-18 months after publication of a standard.

Key Fill Device (KFD) Addendum Scope

- Enhances interoperability for P25 encryption by providing standards-based interfaces between a Key Fill Device (KFD) and the following:
  - A Key Management Facility (KMF)
  - An Authentication Facility (AF)
  - A Link Encryption Facility (LEF)
  - Another KFD



KFD Addendum User Considerations

- TODAY: Interfaces between KMF, AF, and KFD and the KFD are proprietary. This presents challenges for interoperability between different P25 manufacturers.
- There is no impact on the interface between the KMF and SU with this change. 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 12-18 months after publication of a standard.

P25 Authentication Problem Statement

- P25 Authentication Helps Ensure:
  - Only Authorized Radios Obtain Service on a Trunking System
  - Reduces the Risk to Public Safety Communication Systems Arising From Pirated System Keys or Programming Software
  - Reduces the Possibility of Duplicate Radio IDs
  - Improves Protection From Lost or Stolen Radios

P25 Link Layer Authentication User Considerations

- P25 LLA User Considerations:
  - Multiple Trunking Systems Can Be Supported
    - Unique Authentication Key For Each System and Radio ID
  - Authentication Is Usually Part of Registration, But Can Occur at Anytime
  - Disabling the Key In the Authentication Server Will Prevent an Unaccounted for Radio From Gaining System Access
  - Utilizes 128 Bit AES Encryption
    - 3.4 X 10^{38} Key Values
    - FIPS-140-2 Approved

P25 Standards Update: 2017 Publications

Air Interfaces

- **A revision to the FDMA Common Air Interface Standard** was published.

  This revision addresses errata that have been collected since the last publication.

- **A revision to the FDMA Common Air Interface Reserved Values document** was published.

  This revision addresses errata that have been collected since the last publication.

- **A revision to the Trunking Interoperability Test Standard** was published.

  This revision merges the FDMA and TDMA material and addresses an error in a call pre-emption test procedure.

- **A new Standard for a TDMA Control Channel** Media Access Control (MAC) Layer was published.

  This standard describes the messages and procedures for a single slot (or "dual slot") TDMA control channel. A single slot control channel in combination with a single slot voice traffic channel allows single (12.5 kHz) channel trunking sites.

- **An addendum to the Trunking Control Channel Messages** standard was approved for publication.

  This addendum introduces a "Vehicle Sensed Emergency" flag to the Emergency Alarm message.

- **An addendum to the Trunking Control Channel Messages** standard was approved for ballot.

  This addendum introduces an "Accessory Sensed Emergency" flag to the Emergency Alarm message.

P25 Standards Update: 2017 Publications

Wireline Interfaces

- **A revision to the Fixed Station Interface Standard** was published.

  This revision adds additional capabilities the most significant of which is Packet Data.

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was published.

  This addendum expands the existing emergency alarm request message to indicate that the emergency alarm request has been generated by conditions other than depression of the emergency alarm button

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was approved for ballot.

  This addendum introduces the messages and procedures for Individual Regrouping control across an ISSI/ CSSI.

Data

- **A revision of the Location Services Overview bulletin** was approved for publication.

  This revision aligns the content of the Overview document with the content of the Tier 1 and Tier 2 Location Service Specifications.

Broadband

- **An addendum to TSB-88.3** was published.

  This addendum adds new broadband-to-narrowband interference scenarios.

P25 Standards Update: 2018 Publications

Air Interfaces

- **An addendum to the Trunking Control Channel Messages standard** was approved for publication.

  This addendum introduces an "Accessory Sensed Emergency" flag to the Emergency Alarm message.

Wireline Interfaces

- **An addendum to the ISSI Messages and Procedures for Supplementary Data** was approved for publication.

  This addendum introduces the messages and procedures for Individual Regrouping control across an ISSI/ CSSI.

P25 Standards Update: Work in Progress

Air Interfaces

- **A revision to the Conventional Interoperability Test standard** is in progress

  This revision corrects editorial errors and makes clarifications on various test procedures but does not add, remove or technically alter tests.

- **Creation of a High Signal Strength Intermodulation Rejection Test** is in progress.

  This test will measure the ability of a P25 or analog conventional FM receiver to reject an unwanted broadband base station signal, thereby preventing degradation to the reception of a desired signal. Performance specifications are expected to follow completion of the measurement method.

Wireline Interfaces

- **Group Regrouping for the Trunking ISSI/CSSI Standard** is in progress.

  This work will enable dispatch equipment connected to Trunking Infrastructures via the ISSI/CSSI to control group regrouping services. Note the control channel messaging for these services has already been standardized.

- **A revision of the ISSI Recommended Compliance Assessment Tests bulletin** is in progress.

  This revision will add recommended interoperability tests for Trunking CSSI applications and add recommended interoperability tests of TDMA operation of the Trunking ISSI and CSSI.

- **A new Interoperability test standard for Trunked ISSI Supplementary Data Services** is in progress**.**

  This document will provide a standard set of tests for validating interoperability of Supplementary Data Services (Emergency Alarm, Call Alert, etc) operating across a Trunked ISSI.

P25 Standards Update: Work in Progress

Security

- **Definition of a Link Layer Encryption Security Service** is in progress.

  This is the first big new technology upgrade for improved Security for all air interfaces of P25. It protects control channel control messages, and hides group and individual IDs.

- **An addendum to the Key Fill Interface standard** is in progress.

  This will enable Key Fill Device (KVL) interface to a KMF, an Authentication Facility and another Key Fill Device

Data

- **A revision of the Tier 2 Location Service** is in progress**.**

  This revision corrects editorial errors and makes corrections to EXI Encoding examples.

Broadband

- **Definition of 3GPP Mission Critical standard services interworking with TIA Land Mobile Radio standard services** is in progress.

  This document will describe interworking of features (example; group and individual calls) that are common between 3GPP LTE standards and P25 Trunking, P25 Conventional and Analog Conventional FM LMR standards.

What is P25 Compliance ???

"P25 COMPLIANCE" is not strictly defined but most consider "compliance" to mean:

- Adherence to published documentation

P25 SoR drives P25 Standard creation/content

P25 Standards enable interoperability

P25 Standard tests describe consistent methods for testing implementations against a published standard (Performance, Conformance and Interoperability)

Levels of "P25 Compliance"

1. Compliance in the context of the P25 SoR

- 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
- 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
  - P25 SoR contains high level descriptions of functionality that does not enable interoperability
  - Most SoR items trace to published P25 standards, however some do not

Levels of “P25 Compliance”

2. Compliance in the context of the P25 Standards

- 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

P25 Capabilities Guide
Background and Purpose

PTIG's P25 Capabilities Guide was created and is maintained by a Working Group within PTIG

- Manufacturer and User Agency representatives active in P25/ TIA-102 Standards

Intended to be an aid to identify what P25 Interfaces, Services, and Functionality are covered by published P25/TIA-102 Standards

- Assist customers in writing RFP's that meet the P25 standards
- Compare neighboring system functionality for interoperability planning
- Available for Download at **www.project25.org**

Levels of “P25 Compliance”

3. 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

Levels of "P25 Compliance"

4. Compliance in the context of the DHS OIC CAP

- Compliance statements at this level mean:

  The functionality has been implemented per the P25 Standard document(s) and will pass the associated P25 Standard Test(s) covered by published CABs and 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 that produce and maintain the P25 Standard documents and P25 Standard Test documents and 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

DHS OIC CAP Testing Resources

One-stop shop website:
www.dhs.gov/science-and-technology/p25-cap

- Lists of P25 CAP compliant equipment along with supporting documentation
  - Summary Test Reports (STR) and Suppliers' Declaration of Compliance (SDOC)
- Participating P25 CAP recognized labs
- Latest Compliance Assessment Bulletins
- P25 CAP Advisory Panel

PTIG Update

New P25 Statewide Systems List

- 38 P25 State-wide Systems

New White Papers

- P25 Authentication,
- P25 Trunking Control Channels

New P25 Benefits Docs:

- P25 Top 10 Benefits for non technologist Users
- P25 Value Proposition for Agency Administrators, procurement managers

New P25 State-wide Systems List

P25 Statewide Systems (38)	
Alabama 1st Responders	Phase 2 700/800
Alaska ALMR	Phase 1 VHF/700
Arkansas AWIN	Phase 1 700/800
Colorado DTRS	Ph 1 to Ph 2 700/800
Connecticut CSP	Ph 1 800 CERN Ph1 700
Delaware DPS	Phase 1 800
Florida SLERS	Phase 1 700
Hawaii HIR	Phase 1 700
Idaho ICAWIN	Phase 1 700
Illinois STARCOM	Phase 2 700/800
Indiana SAFE-T	Phase 1 800
Iowa ISICS	Phase 2 700
Kansas KSICS	Phase 1 700/800
Louisiana LWIN	Phase 1 700
Maine MSCS	Phase 1 VHF
Maryland FRIRS	Phase 2 700
Massachusetts CMS	Phase 2 700/800
Michigan MPSCS	Phase 1 700/800
Minnesota ARMER	Phase 1 800
Mississippi MWIN	Phase 2 700/800
Missouri MSWIN	Phase 2 VHF/700/800
Montana MSIRS	Phase 1 VHF
Nebraska NSRS	Phase 1 VHF
New Hampshire	Phase 1 VHF
New Jersey NJICS	Phase 2 700
North Carolina VIPER	Phase 1 700/800
Ohio MARCS-IP	Phase 2 800
Oklahoma OWIN	Phase 1 800
Oregon SRP	Phase 2 700
Rhode Island SCN	Phase 1 800
South Carolina PALMETTO	Phase 1 700/800
South Dakota SRS	Phase 1 VHF
Tennessee ACN	Phase 2 700/800
Virginia STARS	Phase 1 VHF/800
Washington State Police	Phase 2 700
West Virginia SIRN	Phase 1 UHF Lo
Wisconsin WIS	Phase 1 VHF/800
Wyoming WYOLINK	Phase 1 VHF/800

Project 25: Top 10 Benefits

Public Safety Grade Reliability and Performance

Mature, well defined, Air and Wireline Standardized Interfaces

Superior Security using 256 bit AES with OTAR

A User-Driven Technology with support at numerous frequency bands

A Large Installed Base of over 2250 Systems

The reliable, de-facto, choice for mission critical communications during Natural Disasters and critical events

A vibrant market-place with more than 3 dozen suppliers and the preferred technology for Federal Grants

Superior Audio volume and clarity combined with high performance radio designs for Public Safety environments

A live, active, technology that continues to evolve with new capabilities, upgrades, and test standards

Independent testing for performance and interoperability

WWW.Project25.org

International Wireless and Communications Expo
Orlando, Florida
NPSTC Meeting March 9, 2018

PTIG P25 Update

New Standards, Applications, and Interoperability

Affiliate Organization Member Update

University of Melbourne Centre for Disaster and Public Safety (CDMPS) – Geoff Spring

NPSTC Meeting

9 March

Orlando

- CDMPS has completed its 3 Year Review
- A CDMPS 2014 – 2017 Report has been produced
- A new CDMPS research strategy has been launched

THE UNIVERSITY OF MELBOURNE

CDMPS
CENTRE FOR DISASTER MANAGEMENT AND PUBLIC SAFETY

2025 & BEYOND

World-class interdisciplinary research & innovation to improve the whole-system response & resilience of infrastructure, institutions & communities against extreme events and critical incidents, and advance the UN sustainable development goals

By 2018

- Base level funding secured & future funding planned
- Strategic plan being implemented
- New governance & management plan in place
- Enhanced communications & marketing plan being implemented
- Priority research agenda developed
- Education & recruitment program developed

- Number & diversity of UoM faculty/discipline participation
- Amount/level & diversity of funding and support (from UoM and external sources)
- Number & diversity of collaboration & partnerships
- Number & diversity of training programs & graduates
- Satisfaction levels of partners, "alumni" & other stakeholders
- Number & diversity of awards or recognitions & publications
- Media mentions & metrics

Towards 2025

Valued & supported:
- within UoM
- by external stakeholders

Recognised to be making an impact or difference in its:
- RD&D, and
- education and training programs

- Establish appropriate governance & management
- Identify grand challenges and focus areas in DRRM and PS
- Strengthen high-impact inter- & trans-disciplinary RD&D Program
- Establish effective & diverse education & training program
- Develop multi-modal engagement & communication plan

Research Priority Areas

1. Understanding and Mitigating Extreme Events and Critical Incidents

2. Enabling Technology, Informatics and Analytics

3. Improving Whole-Life Infrastructure System Performance and Resilience

4. Strengthening Organisational, Institutional and Community Resilience

5. Enhancing Policy and Decision Making

CDMPS Engagement and Collaboration

- **NPSTC-CDMPS**
- MOU executed March 2015
- Internet of Public Safety Things

- **P25 Steering Committee**
- **P25 Technology Interest Group**

- **Research Roadmapping**
- Location Based Services
- Data Analytics
- User Interface/Experience

- **Conference participation**
- Emergency Services Network
- Public safety apps
- NG999
- eCall

- **Conference participation**
- NG911
- P25

- **Connected vehicles**

www.arcia.org.au

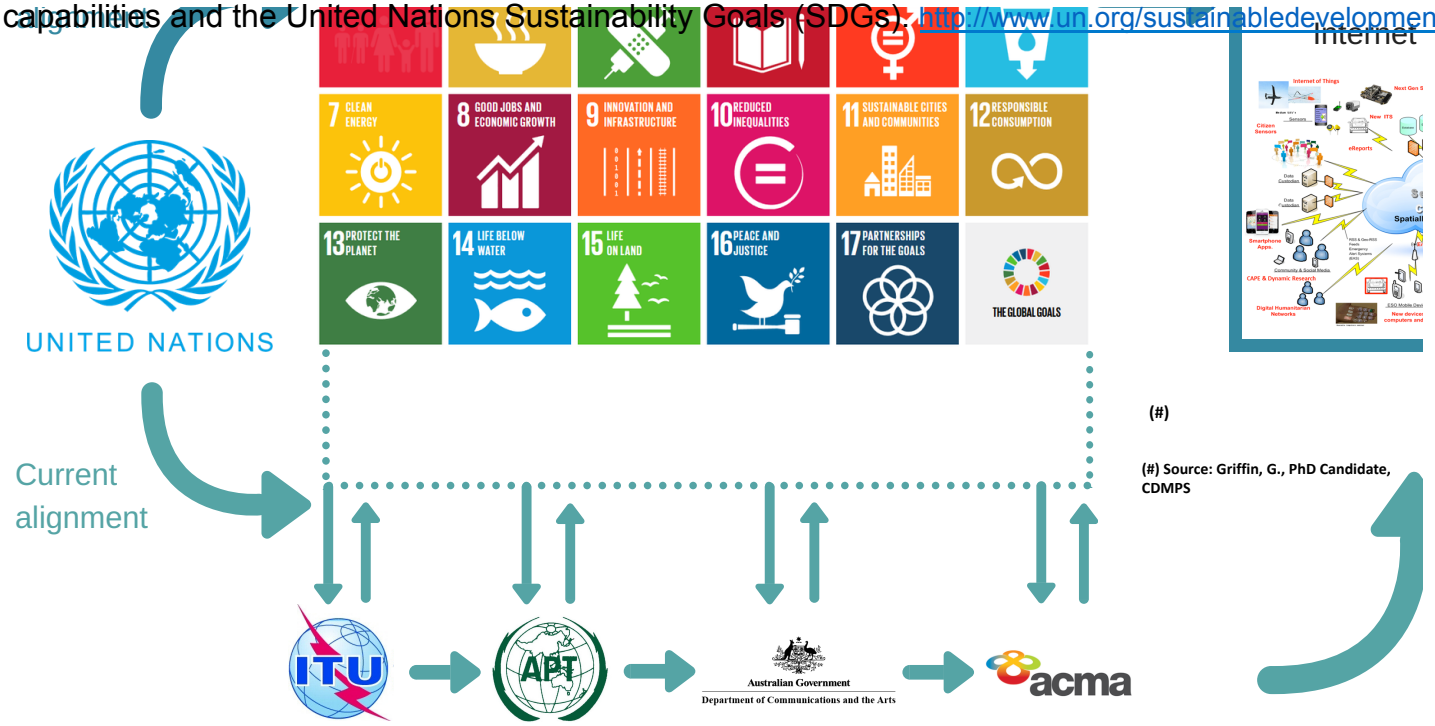
Australian Radio Industry Communications Association

CommsConnect Conference Organiser

Centre for Spatial Data Infrastructure and Land Administration

United Nations Sustainable Development Goals:
How will they influence critical communications?

The movement of mission critical public safety communications into mainstream ICT through PSMB Projects and Next Generation Emergency Call Services will enable the investigation of the relationship between these new capabilities and the United Nations Sustainability Goals (SDGs). http://www.un.org/sustainabledevelopment/



The University of Melbourne CDMPS has commenced initial research into this relationship.

International Performance Measurement and Monitoring
Against UN SDGs

The International Telecommunications Union (ITU) as special purpose agency of the United Nations is participating in the UN SDGs by proposing indicators related to the contribution of ICT (including use of mobile phone networks and the internet) towards achieving the SDGs by 2030.

https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/sdgs/default.aspx

Quixoticity https://www.quixoticity.com/

The number of PSMB Projects now under way internationally offers the opportunity to compare the different approaches being taken to providing a PSMB capability. One such approach has been the publication of an index by Quixotcity launched at the CommsConnect Conference in Melbourne in November 2017.

This Index aims at identifying and promoting best practice in the world of public safety and critical communications and also references the United Nations Sustainable Development Goals (SDGs).

Thank you for your attention

http://research.unimelb.edu.au/cdmps

geoff.spring@unimelb.edu.au

Ph: +61 411 130 184

THE UNIVERSITY OF MELBOURNE

CDMPS
CENTRE FOR DISASTER MANAGEMENT AND PUBLIC SAFETY

Administrative Discussion – Future Meetings

Tuesday, May 15, 2018 | Teleconference

Wednesday, September 6 & Thursday, September 7, 2018 | Washington, DC at OCTO

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Executive Session Level IV

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Executive Level IV Session

- LEVEL IV
  - NPSTC Chair
  - NPSTC Vice Chairs
  - NPSTC Executive Director
  - NPSTC Deputy Executive Director
  - Committee Chairs
  - Committee Vice Chairs
  - Voting Organization Representatives and Alternates
  - Associate Representatives
  - Invited Guests


NPSTC

Adjourn

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (OEC) Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.