

# Full NPSTC Meeting | Washington, DC

**Wednesday, September 28**

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

Webinar Access Information : <https://join.me/NPSTCsupport1>

Submit Questions Online

Send email to [support@npstc.org](mailto: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.

# Welcome and Opening



- Ralph Haller, NPSTC Chair
  - Call to Order
  - Pledge of Allegiance
- Technical Tips
  - Webinar Access Information: <https://join.me/NPSTCsupport1>
  - Online participants submit questions to [support@npstc.org](mailto: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](mailto: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.*

# 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)



# Welcome

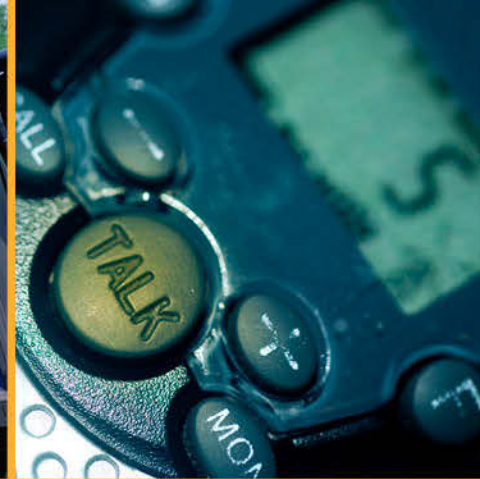


- Associate Organizations
  - Canadian Interoperability Technology Interest Group (CITIG)
  - Utilities Telecom Council (UTC)
  
- Affiliate Organizations
  - Alliance for Telecommunications Industry Solutions (ATIS)
  - Open Mobile Alliance (OMA)
  - Telecommunications Industry Association (TIA)
  - 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)



## Federal Partners Update

**Department of Homeland Security (DHS), Office of Emergency Communications (OEC) – Chris Essid, Deputy Director**

**Department of Homeland Security (DHS), Office for Interoperability and Compatibility (OIC) – Sridhar Kowdley, Program Manager**

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.



Homeland  
Security

# Update from the Office of Emergency Communications

National Public Safety Telecommunications  
Council (NPSTC) In-Person Meeting

September 28, 2016

Chris Essid  
Deputy Director  
Office of Emergency Communications

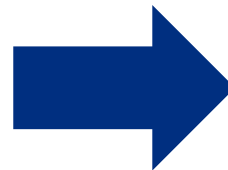


# National Governors Association Policy Academy

2016 Focus:  
Enhancing Emergency  
Communications  
Interoperability

Alaska, Hawaii,  
Illinois, Utah, and  
West Virginia

2006 NGA Policy  
Academy on  
Interoperability



- DHS OEC
- 2008 NECP
- SWICs, SIGBs, SCIPs
- IECGP Funding





# Interoperability Communications Capabilities Analysis Program (ICCAP)

This summer, as part of the ICCAP program, OEC has been conducting pilot observations during planned events in urban areas:



Date	Location	Event
9/1	Honolulu, HI	Honolulu World Conservation Congress
9/9	Carmel, IN	BMW Golf Championship Tournament
9/18	Los Angeles, CA	Return of the Los Angeles Rams
9/24	Washington, DC	Opening of the African American Museum
10/22	Austin, TX	United States Grand Prix Formula One

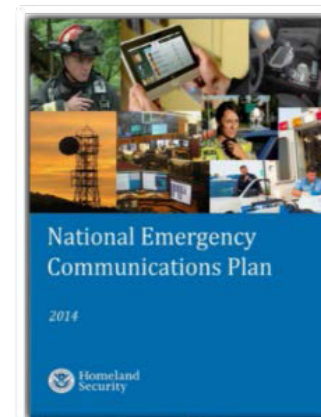




# Governance and Planning IPT

OEC recently launch a new Statewide Governance and Planning IPT to enhance support for states and territories through strategic planning and technical assistance.

- Leveraging feedback from SWICs and other state-based leaders
- New approach will be presented at SAFECOM/NCSSWIC in-person meetings in October



Homeland  
Security

Office of Emergency Communications

# A New Look for GETS

## 2016 Government Emergency Telecommunications Service (GETS) Card

### Card Front



**Government Emergency  
Telecommunications Service**  
Office of Emergency Communications

**John Smith**  
**Department of Defense**

Dial Access Number: **1-710-627-4387**

After Tone, Enter PIN: \* \* \* \* \*

When Prompted, Dial: **Area Code + Number**

### Card Back

**GETS**  
If you cannot complete your GETS call using 1-710-627-4387, try using one of these alternate access numbers:

<b>1-888-288-4387</b>	AT&T
<b>1-877-646-4387</b>	AT&T VoIP
<b>1-855-333-4387<sup>1</sup></b>	Sprint VoIP
<b>1-800-900-4387</b>	Verizon
<b>1-855-400-4387</b>	Verizon VoIP

<sup>1</sup> Can be used for toll-free destinations (e.g., 800, 855)

**WIRELESS PRIORITY SERVICE (WPS)**  
**\*272 + Area Code + Number + SEND**  
From a WPS-Enabled Phone

[www.dhs.gov/gets](http://www.dhs.gov/gets) | [www.dhs.gov/wps](http://www.dhs.gov/wps)  
**Warning: For Official Use Only by Authorized Personnel**

**24 Hour Assistance**  
For help or to report trouble:  
**1-800-818-4387**  
or **703-818-4387**

**Familiarization Calls**  
Make periodic GETS and WPS test calls to:  
**703-818-3924**

**U.S. Government Property**  
If found, return to:  
DHS (Attn: NPPD/CS&C/OEC)  
245 Murray Lane SW  
Bldg. 410, MS 0615  
Washington, DC 20598

Distribution beginning November 1, 2016 – November 1, 2017



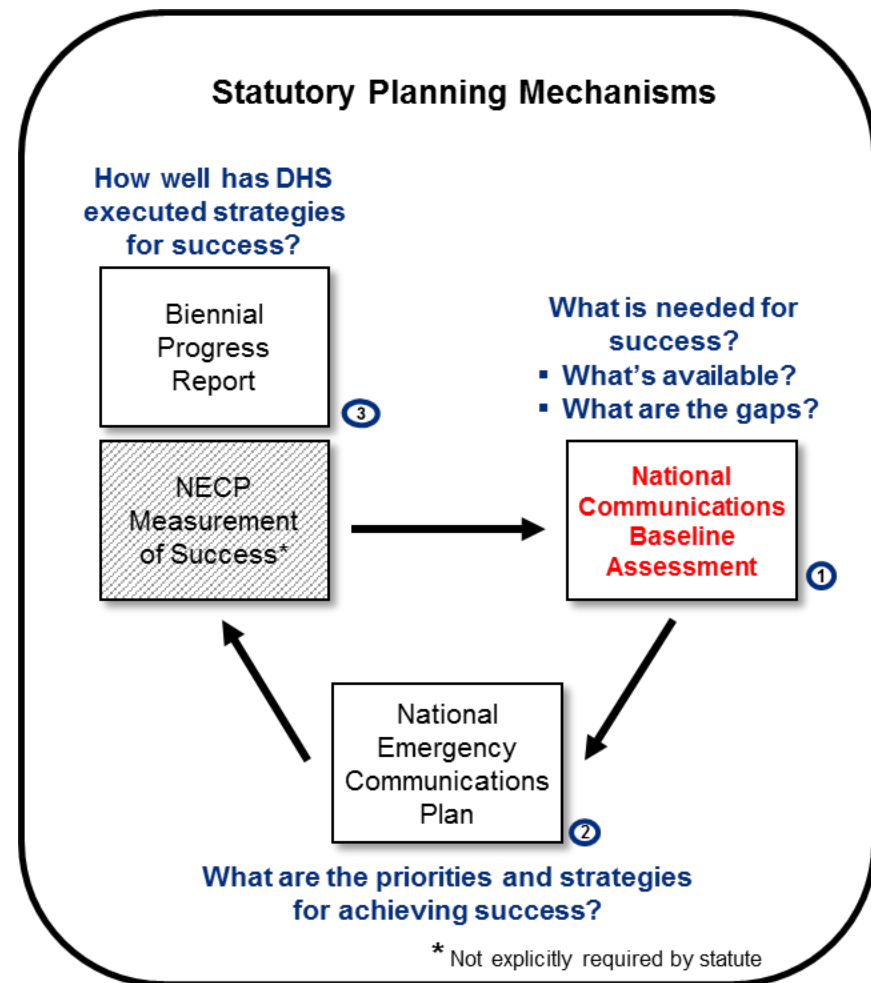
**Homeland  
Security**

Office of Emergency Communications



# National Communications Baseline Assessment

- **Goal:** Conduct a national baseline assessment of the current ecosystem of communications capabilities needed and in use by emergency response providers
- **Objectives:**
  - Address “Title XVIII – Emergency Communications” requirements
  - Develop an improved assessment framework that allows OEC to determine the *available vs. needed* communications capabilities
  - Establish a consistent, repeatable, and effective baseline assessment process to help standardize OECs national planning lifecycle

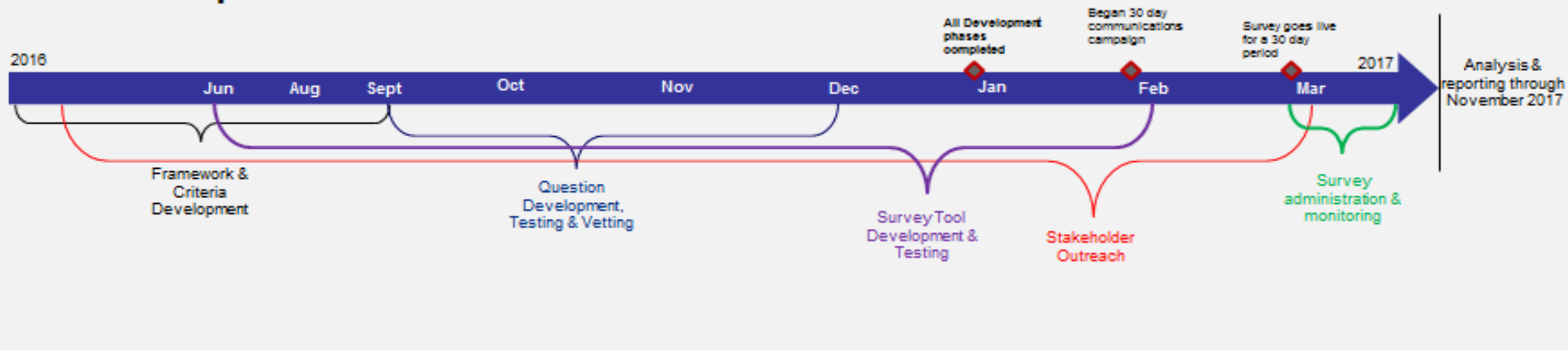




# NCBA Timeline

- OEC will conduct an extensive analysis on the data collected beginning March 2017
- OEC will utilize the data and analysis from this effort to:
  - Identify areas where OEC can target resources via TA, SCIPs, SAFECOM Guidance
  - Identify capability levels and capability gaps
  - Report to Congress on what is needed

## NCBA Development Timeline







# NCBA Champions Working Group

- OEC is engaging external and internal stakeholders extensively, and continues expanding its efforts:
  - OEC stood up the “NCBA Champions Working Group” to elicit stakeholder feedback and expertise on all aspects of the project
  - The NCBA Champions Working Group is comprised of POC’s from the following stakeholder groups:
    - Major public safety partnerships & associations (e.g., SAFECOM, NCSWIC, Tribal Nations\*, CIPAC/ ESSCC, State of Washington SIEC)
- **Ask:** We need NPSTC Members to participate
  - Interested? Please email us at: [OEC@hq.dhs.gov](mailto:OEC@hq.dhs.gov)





# Homeland Security



Homeland Security

Office of Emergency Communications



# DHS S&T

## First Responder Electronic Jamming Exercise

---

Briefing for NPSTC

**September 28, 2016**

**Sridhar Kowdley**

Program Manager  
First Responders Group  
Science and Technology Directorate



**Homeland  
Security**

Science and Technology

# Exercise Overview

- **Purpose:** Conduct live testing and demonstrations of first responder communications in a electronic jamming threat environment provided by White Sands Missile Range (WSMR)
- **Outcomes:** Understand the impact of electronic threats on first responder communications and mission operations; identify training gaps and mitigation strategies; and share lessons learned and best practices with first responders nationwide




Homeland  
Security


Science and Technology

# Electronic Jamming Threat

- First responders across the country face increased electronic jamming threats, notably jamming of GPS, radio and wireless systems
- Proliferation of electronic jammers can delay emergency response times, escalate hazardous situations, result in loss of life or facilitate illicit activities
- In addition to first responder threats, this exercise will address additional threats to homeland security, including:
  - Global War on Terror**
  - Southern Border Protection**
  - Infrastructure Protection and Security**



## Cellular, GPS, Wi-Fi, and Other Signal Jammers



Signal jammers are illegal and can interfere with operational channels commonly used by first responders, disrupting vital communications or affecting emergency operations. There have been documented incidents of the loss of first responder radio communications near areas where cell and GPS jammers were being used. Loss of cellular coverage was also observed in these areas which prevented 9-1-1 and other emergency calls from being made. Jammers can target cellular, GPS, Wi-Fi, and other radio signals, individually or in combination.

Indicators of Jamming:

Disruption or failure of wireless communications or mapping equipment, including cellular or GPS devices, for unknown reasons could indicate interference by a jammer.

Specific indicators might include:

- Inability to transmit or receive on two-way radios outside of known "dead zones."
- Unusual sounds on designated frequencies, such as white noise, intermittent electronic chirping, or tones.
- Lack of normal sounds heard on designated frequencies or presence of "dead air."
- Technical difficulties that appear and disappear intermittently.
- Lack of audible click when keying microphone.
- Abrupt loss of communications, especially if stationary.
- Loss of lock, intermittent disruption, or general failure of a GPS receiver or GPS-enabled device.

Actions:

Incidents where a suspect operating a jammer is identified should be reported to the FCC at [www.fcc.gov/complaints](http://www.fcc.gov/complaints) or 1-888-CALL-FCC (1-888-225-5322). The FCC will investigate and take follow-up administrative enforcement action against the subject where applicable.

Reports should include the following:

For an ongoing incident or if a suspect is identified, provide:


- Identification details of suspect using illegal equipment (Name, DOB, vehicle tag, etc.).
- Description or identification of suspected jamming device (including photo if available).

For all incidents, provide:

- Reporting party's name/contact information/agency, date, time, duration, location, & stated mission or operations.
- Nature of the disruption (such as single occurrence, recurring, intermittent, or loss of signal indication).
- Equipment affected (type, model, application).
- Environmental conditions (weather, topography, terrain, time of day).
- Steps taken to improve or regain ability to use equipment.
- Other wireless devices not affected by the suspected jamming or anomaly.

The FCC can assist with legal and technical questions when jammers are encountered or suspected. Contact points are through [jammers@fcc.gov](mailto:jammers@fcc.gov) or the FCC's Spectrum Enforcement Division at (202) 418-1160 (9 AM - 5 PM ET) or 1-888-CALL-FCC. Additional public information is available at: <http://www.fcc.gov/jammers>.

Jammer Examples (including disguised devices)



Applicable Laws:

Federal laws prohibit any person from willfully or maliciously interfering with authorized radio communications and prohibit the manufacture, sale, marketing, importation, distribution, or shipment of jamming equipment.

State laws may also prohibit the possession or certain uses of jammers (e.g., interference to police communications) and thus provide a basis for local seizure and prosecution. Law enforcement agencies should develop a strategy in advance with their office of legal counsel.

The Communications Act of 1934

Section 301 - requires persons operating or using radio transmitters to be licensed or authorized under the Commission's rules (47 U.S.C. § 301).

Section 302(b) - prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 U.S.C. § 302a(b)).

Section 333 - prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government (47 U.S.C. § 333).

Section 503 - allows the FCC to impose forfeitures for willful or repeated violations of the Communications Act, the Commission's rules, regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other Commission authorization, among other things (47 U.S.C. § 503).

Section 510 - allows for seizure of equipment used, possessed, advertised, or sold with knowing intent to violate Sections 301 or 302 (47 U.S.C. § 510).

FCC Rules

Section 2.803 - prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States (47 C.F.R. § 2.803).

Section 2.807 - provides for certain limited exceptions, such as the sale to U.S. government for authorized, official use (47 C.F.R. § 2.807).

The Criminal Code (Enforced by the Department of Justice)

Title 18, Section 1362 - prohibits willful or malicious interference to U.S. government communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1362).

Title 18, Section 1367(a) - prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both (18 U.S.C. § 1367(a)).



**Homeland Security**

Science and Technology

In 2015, DHS issued a joint bulletin with the FCC capturing the impact of jamming on First Responder Communication and emergency communications.



# So What did We Do?

- Coordinated with DHS OEC and DHS components to identify participants
- Worked with FCC/NIST and DHS to obtain jammers
- Contracted with AF 746 TS to conduct testing and operate jammers
- Conducted detailed planning sessions (spectrum/scenario)
- Obtained and characterized jammers
- Obtained invitational travel for state and local first responders

## Exercise Resources

- Over 225 personnel participated on-site
- Over 500 personnel supported planning
- 61 organizations supported exercises
- 16 mobile command and first responder vehicles
- 70 first responder scenarios conducted
- 53 commercial and DOD jammers
- Operated over 500 square miles of desert – more than 7 times the size of Washington, D.C.



**Homeland  
Security**

Science and Technology



U.S. Immigration and Customs Enforcement



FEMA



U.S. Customs and Border Protection

DIGITAL GLOBAL SYSTEMS



# Homeland Security



MITRE



SwRI



Science and Technology



GD



LOCKHEED MARTIN

U.S. AIR FORCE

HARRIS



# First Responder Vehicles



**Homeland Security**

Science and Technology

# Day 1: Jamming Critical Infrastructure

- Participants included the Department of Defense, Federal Communications Commission, Federally-Funded Research and Development Centers, and industry partners
- Tested GPS and anti-jamming GPS systems against a variety of GPS jamming threats



**Homeland  
Security**

Science and Technology

# Day 2: Jamming UAS

- Participants included Lockheed Martin Aerospace, Stark Aerospace, AeroVironment, Air Robot, and Stanford University (not part of RAPS)
- Tested fixed and rotary wing unmanned aircraft systems (UAS) against GPS and broadband jamming to examine the effect on navigations and communications capabilities
- Stanford University tested a UAS platform that autonomously locates GPS jammers by honing in on the jammer's signal – and it was successful!
- The other four vendors tested their UAS's to locate suspects during drug smuggling and illegal immigration scenarios, assessed by officers from the U.S. Border Patrol







# Day 3-5: Jamming First Responders

- Participants included Los Angeles County Sheriff's Department, the Harris County (TX) Fire Marshall's Office, the Mesa (AZ) Police Department, New Mexico Department of Homeland Security and Emergency Management, FEMA, ICE, CBP, USCG, and industry
- Tested first responder communications systems, including land mobile radio systems (multiple bands), Cellular, Wi-Fi, Satellite, GPS, Bluetooth, and other wireless devices (i.e. thermal imaging)
- Assessed not only how the equipment was impacted by GPS and broadband jamming, but also how well responders were able to work around the jamming to still accomplish their mission

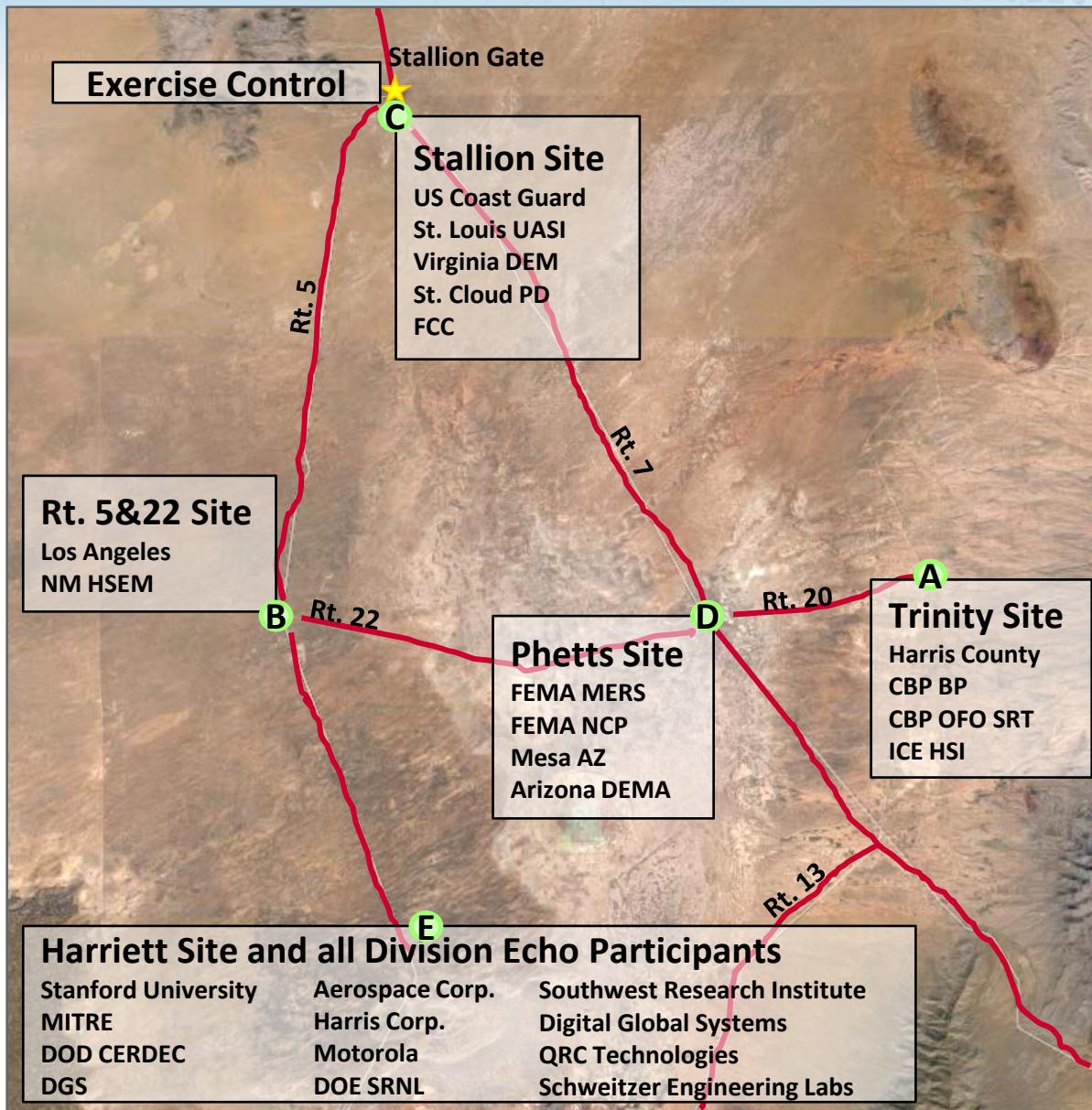


**Homeland  
Security**

Science and Technology



# Day 3-5: Exercise Layout At WSMR



## Organization

By splitting up into four first responder divisions and one industry division, we were able to run 5 simultaneous scenarios with different jammers – **more than 70 scenarios over three days**

## Industry Testing

Industry participants at Division Echo tested a variety of receivers, spectrum analyzers, and communications devices against the full range of jammers, and have shared their data with DHS S&T for analysis



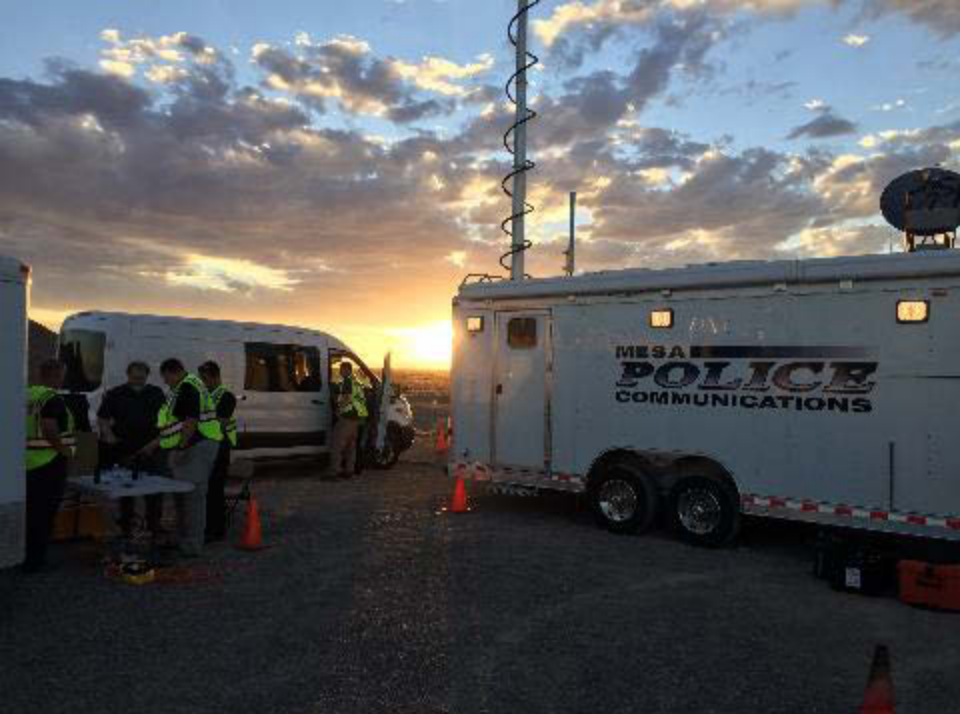


























# Initial Observations and Findings

- First Responders were all surprised at how these commercial jammers worked
- First Responders recognized that they have gaps in training, and stated they would “have to rethink their communications plans” and identify mitigation strategies
  - A representative from FLETC witnessed test and we will be discussing anti-jamming training.
  - A responder from the Arizona Department of Emergency Management and Military Affairs said that he is now “ten times more likely to recognize intentional jamming” than before the exercise
- Detailed reports and test results will be compiled from data provided by all organizations and data collected in the field
  - Reports containing vulnerabilities appropriately classified, including FOUO/LES planned for October 2016
- Responders used creative problem-solving to accomplish their mission in jamming environments



# Acknowledgements

- This exercise would not have been possible without significant contributions from:
  - **DHS Office of Emergency Communications** for coordinating with State and Local participants and assisting with exercise execution
  - **New Mexico Department of Homeland Security and Emergency Management** for providing assets and supporting exercise execution
  - **FCC and FAA** for assisting in spectrum authorization and coordinating with DOD to characterize jammers
  - **Air Force 746 Test Squadron and White Sands Missile Range** for supporting exercise planning, providing the test environment, and supporting exercise execution including operating commercial and DOD jammers and facilitating logistics



**Homeland  
Security**

Science and Technology



# Follow-On Exercise in 2017

- Objectives:
  - Test anti-jamming mitigation technologies in a field setting
  - Evaluate first responder jamming mitigation techniques, tactics and procedures (TTPs)
- Details:
  - Location and Date TBD
    - Looking at August-December 2017, depending on facility availability
    - Evaluating DOD and non-DOD facilities
  - Similar scope in size– 200-300 participants
  - Split into two parts – a T&E event to technically evaluate the mitigation technologies and a full-scale exercise to evaluate the first responder TTPs
    - Each part will have different requirements for planning and execution
    - NUSTL will lead the T&E event with the industry participants
    - OEC and FEMA will help lead the exercise portion with first responders



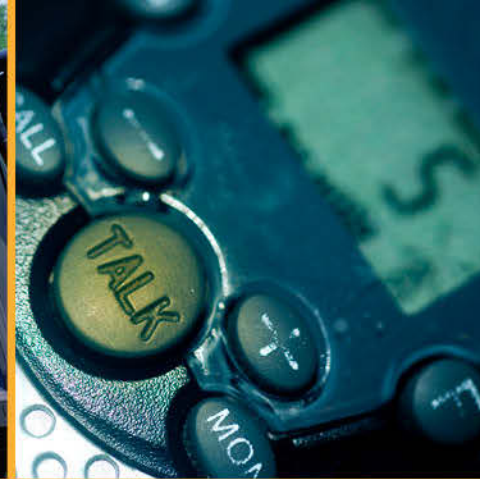




# Homeland Security

---

Science and Technology



# Technology and Broadband Committee

**Tom Sorley, Chair**

**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.



# Broadband Emerging Technologies Working Group

**Kim Coleman-Madsen, Chair**

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



# Broadband Emerging Technologies Working Group



- Hosted several presentations on current topics.
  - NIST overview of sensors and connected systems
  - NIST Smart Cities Project
  - State Alternative Planning Approaches Panel Discussion
  - NG911 and Broadband Data



# Broadband Emerging Technologies Working Group

---



- Upcoming Presentations
  - Public Safety LTE deployment in the United Kingdom (October)



# Broadband Emerging Technologies Working Group

---



- FirstNet Agency Status Page
  - Finalizing a report that discusses public safety requirements for the NPSBN Agency Status Page.
  - High Level Features include rapid access to:
    - FirstNet network status.
    - Agency designated information and resources.
    - Incident information on active emergency events.



# Broadband Emerging Technologies Working Group

---



- What do we mean by Agency Status Page?
  - NPSTC SOR speaks to a web status page for first responder access to **network status** and **incident information**. The FirstNet RFP speaks to a home agency status page providing the same functionality.
  - The PSAC is discussing **local control** issues which may involve a web portal.
  - There are also a variety of other **web portals** (related to the provision of applications and other services).

# Broadband Emerging Technologies Working Group

---



- FirstNet Agency Status Page
  - Completed review of previous NPSTC requirements for a local agency controlled “landing page” for first responders:
    - 2009 NPSTC Report, “700 MHz Broadband Task Force Report”
    - 2012 NPSTC Report, “SOR for High Level Launch”
  - Reviewed the FirstNet Final RFP
    - Multiple references to “Agency Information Homepage”

# Broadband Emerging Technologies Working Group

---



- Public Safety uses for Status Page:
  - A police officer can view a list of high priority emergencies among all agencies in the area (his city, adjacent city, sheriff, and state patrol).
    - This would allow a state patrol trooper to maintain situational awareness on major incidents occurring in all jurisdictions





# Broadband Emerging Technologies Working Group

---



- Public Safety uses for Status Page:
  - A Fire engine responding mutual aid to an incident in an adjoining city (or county) can access incident information to assist their response.
    - This would include the ability to display the incident location, radio channels assigned, staging location for mutual aid units to report to, and a list of units assigned/on-scene.



# Broadband Emerging Technologies Working Group

---



- Public Safety uses for Status Page:
  - A public safety user is alerted to the presence of a major incident occurring nearby based on their GPS proximity to the event.
    - For example, a sheriff's deputy traveling through a city may pull into a gas station for coffee and be unaware that a robbery in progress has been reported at that location.



# Broadband Emerging Technologies Working Group

---



- Web Status Page:
  - The Working Group is finalizing a list of Functional Details that provide context on the operation of the status page:
    - Access based on user authentication
    - Provision of real time incident data via agency interface
    - Default landing page issues for home vs. itinerant users
    - Use of a common status page template for consistency
    - Capability for various audible and visual alerts based on message severity
    - Local control influence on what information is shared



# Broadband Emerging Technologies Working Group

---



- Web Status Page:
  - The Working Group has identified a number of issues that should be considered by FirstNet
    - Status page design to support all device types (laptop, tablet, smart phone)
    - Use by devices without keyboards
    - Translation of agency incident codes when displayed on the status page (what is a “Signal 24”?)
    - Navigation between regional and local status pages and navigation between agency specific local pages (law enforcement vs. fire)

# Broadband Emerging Technologies Working Group

---



- Web Status Page:
  - The core material in the report is consistent with prior NPSTC recommendations and with the FirstNet RFP.
  - The goal of the report is to provide additional context on the use of the status pages.
  - The report should be completed for Governing Board review in November.



# LMR to LTE Migration Working Group

**Chris Kindelspire, Chair**

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

# LMR to LTE Migration Working Group



- Studying interoperability of public safety LMR with FirstNet LTE mission critical voice.
- Created five use cases to validate existing NPSTC PTT requirements.
- Working with PSCR to better understand the technical complexity of direct mode/off network communications.
- Have identified a number of key issues.



# LMR to LTE Migration Working Group



- Unit ID and Alias

- Reviewing LMR Unit ID and LTE Talker ID features
- What should LTE Talker ID include?
  - Agency Name, Officer Name, CAD Unit #
  - Differentiate users accessing multiple devices (vehicle, tablet, handheld radio device)
  - Default ID for a device when a user is not signed in



# LMR to LTE Migration Working Group

---

- Unit ID and Alias
  - Need for nationwide standardized Unit ID structure?
    - First Responders can be out of area but need meaningful translation.
    - A state trooper radioing for local assistance.
    - Mutual aid units arriving from another state.
  - How does an LTE Unit ID appear on an LMR device?
    - LTE provides more capability than P25 ID



# LMR to LTE Migration Working Group

---

- Emergency Button
  - How can Emergency Button alerts travel across both networks?
    - LMR user to LTE user/console
    - LTE user to LMR user/console



# LMR to LTE Migration Working Group

---



- SCAN
  - Examining differences in the LTE scan function.
  - LMR radios have sequential audio scan.
  - LTE has multi-audio monitor
    - “Scanning” three talk groups could result in three simultaneous audio streams coming to the device speaker.





# LMR to LTE Migration Working Group (

---



- Off Network Communications
  - Examining differences in LTE “Direct Mode” communications.
  - 3GPP standards continue to evolve in this area.
  - Many options based on configuration of the network and configuration of user devices.

# LMR to LTE Migration Working Group

---



- Off Network Communications
  - Loss of FirstNet coverage
  - 3GPP standard states that a user should “automatically” move to ProSe (Direct Mode) communications.
    - Goal is to provide the first responder with continuous communications.
    - Responder can communicate with other responders who are also in Direct Mode or with responders who are still on the main FirstNet network.

# LMR to LTE Migration Working Group

---



- Off Network Communications
  - What is the threshold setting that detects loss of coverage?
    - Moving through a building that has poor coverage, you may be “in” and “out” of coverage every few steps.
  - Where the radio switches to direct mode, what channel is selected?
    - To a default interoperable talk-group? (common to everyone)
    - To a discipline specific talk-group? (Fire vs. Law Enforcement)
    - To an agency specific talk-group? (Orange County Fire?)

# LMR to LTE Migration Working Group

---



- Off Network Communications
  - When operating in direct mode, should your radio automatically switch back when network coverage is detected?
  - Can you lock your device into a specific mode?
    - A group of firefighters may be assigned direct mode for their mission, even though they are in FirstNet coverage.



# LMR to LTE Migration Working Group



- Off Network Communications
  - 3GPP Standards allow a user in direct mode to “discover” other nearby users.
    - This mode will let them know who they can communicate with.
  - Nearby users will be displayed in a list
    - similar to the list of Wi-Fi hotspots that appear on your phone.
  - Who should appear on the first responders list?
    - Everyone who is in range (public safety and CII users?)
    - Just users of the same discipline (firefighters vs. police officers)
    - Just users from the same agency (Orlando PD officers only)
  - What should appear on the list?
    - Users agency, name, CAD Unit ID
  - How is the list organized/sorted?

# LMR to LTE Migration Working Group

---



- Off Network Communications
  - 3GPP Standards speak to the ability of a first responder to communicate with public safety units on the FirstNet macro network and with off-network users in direct mode.
    - There is some level of uncertainty in how this will work.
  - Can a first responder receive a message from a user in direct mode while they are transmitting on the macro network? Or, can a first responder only hear messages from either network when they are not transmitting.

# LMR to LTE Migration Working Group

---



- Off Network Communications
  - The Working Group would like to thank Jeb Benson and the whole PSCR team for their assistance in navigating all of these issues.

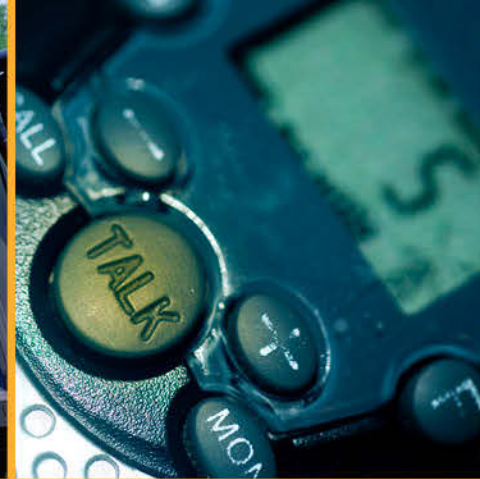
# LMR to LTE Migration Working Group

---



- Working Group Name Change
  - The focus of the WG has been on interoperability issues between LMR and LTE systems, with a specific focus on voice operations.
  - There is a need for consistent messaging that LMR systems are important and need sustainment.
  - The use of the word “migration” may be viewed as indicating that public safety is moving from LMR to LTE.
  - Recommendation: Change Working Group name to “LMR LTE Integration and Interoperability”.
  - Governing Board Vote needed to implement this change.





# Break

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.



# Broadband Deployable Systems

**Barry Luke, NPSTC Deputy Executive Director**

# Broadband Deployable Systems

---

- This is a joint U.S./Canadian working group created by NPSTC at the request of DHS S&T and Canada's Centre for Security Science.
  - Broadband deployable systems will likely be a key component in both the US FirstNet buildout and with Canada's public safety broadband network.
  - Strategies for network interoperability between the two countries are important.
- LTE Broadband Deployable Network issues for public safety, including backpack, vehicular, towed and airborne solutions.

# Broadband Deployable Systems

- Broadband Deployable device form factors include:
  - Backpack deployable units
  - Vehicle based deployable systems
  - Towed/Trailer solutions
  - Airborne platform systems





# Broadband Deployable Systems

---

- Created a series of use cases and identified needed operational capabilities and technical challenges.
  - Wildland fire is an isolated area (no network coverage)
  - Large sporting event (adding capacity)
  - Mass casualty event
  - Search and Rescue incident
  - Disaster response
  - Service continuity transition (exterior to interior)
  - Bring Your Own Coverage

# Broadband Deployable Systems

---

- Discussed different deployable system configurations:
  - When using backhaul and connected to the macro network.
  - When disconnected from the main network.
  - When operating with more than one deployable at the scene.

# Broadband Deployable Systems

---

- Created an Incident Commander/COML Decision Matrix.
  - Helps match the correct deployable system to the needs of the public safety mission.
  - Will a vehicle based solution be sufficient or should a COW/SOW be requested?

# Broadband Deployable Systems

- Created an Incident Commander/COML Decision Matrix

**Broadband Deployable Systems**  
**Incident Command/COML Decision Matrix**  
**Version: 10/7/2015**

This document is designed to assist an incident command or COML in selecting the proper deployable system resource. The answers to the matrix questions below would be coupled with additional information on the incident location, type of terrain, and other factors that would impact the use of a backpack, vehicular, towed-trailer COW/SOW, or aerial solution.

The DS needs to support PS User Group Size "A"  
(to be defined, large number of users) N= \_\_\_\_\_

The DS needs to support PS User Group Size "B"  
(to be defined, medium number) N = \_\_\_\_\_

The DS needs to support PS User Group Size "C"  
(to be defined, small group) N = \_\_\_\_\_

**Expected Coverage Area:**

The DS needs to support Geographic Coverage Mode "A"  
(a large sized outdoor area to be defined)

The DS needs to support Geographic Coverage Mode "B"  
(a medium sized out door area to be defined)

The DS needs to support Geographic Coverage Mode "C"  
(a small sized outdoor area, to be defined)

The DS needs to support Geographic Coverage Mode "D"  
(coverage to include in building)

# Broadband Deployable Systems

---

- Incident Commander/COML Decision Matrix:
  - What applications are needed.
  - What type of voice communications are needed.
  - Site access restrictions.
  - Availability of power.
  - Backhaul.



# Broadband Deployable Systems *(continued)*

---



- Finalizing list of public safety requirements for broadband deployable systems.
  - Approximately 50 requirements have been identified in the following categories:
    - Administration
    - Backhaul
    - Deployment
    - Functionality
    - Handover
    - Interface
    - Security
    - Disconnected Operations

# Broadband Deployable Systems

---

- Cross Border use of broadband deployable systems
  - Also examining feasibility of seamless operation along the U.S./Canadian border.
    - Can a U.S. wildland firefighter continue communicating if they leave FirstNet coverage and enter the coverage “bubble” of a Canadian deployable system?
- Technical and operational challenges are also being examined:
  - Are their gaps in existing 3GPP standards?
  - What security credentials are stored on a deployable system operating in disconnected mode?

# Broadband Deployable Systems

- Final Report should be completed in November for Governing Board review.

## Executive Summary

Chapter 1:	Introduction
	1.1 Purpose of the Report
	1.2 Methodology
Chapter 2:	Public Safety Use of Deployable Systems
Chapter 3:	Types of Deployable Systems
Chapter 4:	Deployment Considerations
	4.1 Cross Border Considerations
Chapter 5:	Role of Back Haul
Chapter 6:	Role of Applications
Chapter 7:	Voice Considerations
Chapter 8:	Operations and Maintenance
Chapter 9:	Deployable Systems Security and Assurance
Chapter 10:	Technical Considerations and Challenges
Chapter 11:	Operational Policy and Governance Considerations
Chapter 12:	Conclusions
	12.1 Recommendation




# Radio Programming Compatibility Requirements (Radio PCR)

**Tom Sorley, Technology and Broadband Committee Chair**

# Radio Programming Compatibility Requirements ( Radio PCR)



- Performing a Quality Assurance Check on a new version of the PAM Tool with new 700 MHz channels added.
- Asking industry partners to verify that their subscriber information listed in the PAM Tool is correct.

**Programming and Management (PAM) Tool**  
**Release: NPSTC\_PAM\_Tool\_071714\_V3**  
**NEW: This version includes updated manufacturer information and NIFOG data**

- This form is a tool to be pre-populated with conventional channel and P25 trunked system and talkgroup information to assist in programming multiple manufacturers radios onto a single system for interoperability.
- Users must be familiar with and have access to the specific programming software for each manufacturer.
- The spreadsheet was developed in collaboration with all of the participating manufacturers.
- Information or questions on specific fields should be referred to each specific manufacturer's representative.
- This tool continues to be developed and future versions may have an import/export feature.
- All agencies using this form are responsible for the information entered into the spreadsheet.



# Radio Programming Compatibility Requirements ( Radio PCR)

---



- Face to face meeting held on September 20-21, 2016 in Houston.
  - Reviewed limitations of the current spreadsheet.
  - Discussed gaps in current PAM Tool capabilities.
  - Created a vision for the future PAM Tool technology.

# Radio Programming Compatibility Requirements ( Radio PCR)

---

- Recommendations include:
  - Add Channel Names and full NIFOG channels list to each vendor tab to make use of PAM easier.
  - Deliver working PAM tool to DHS for: (11/1/2016)
    - Posting on WEB (DHS Public Safety Tools or similar site).
    - Operation & Maintenance of the PAM Tool.
    - Quality Assurance of future changes.
  - Develop an request for “Technical Bulletin” to be submitted to TIA.
    - Make mandatory PAM fields into common interchange format (12/1/2016).
  - Develop Collateral to explain/support TIA request.
    - Visual Aid to include Pre-PAM tool, PAM tool now, and future state.
    - Support letters to be submitted with TIA request.
  - Attend January TIA meeting to promote submission.



# Unmanned Aircraft Systems (UAS)/Robotics

**Dr. Michael Britt , Technology and Broadband Committee Chair**

# Unmanned Aircraft Systems (UAS) and Robotics

- Heard presentations on the following topics
  - Larimer County UAS Program (accident scene reconstruction)
  - Use of UAS for SAR Texas A&M University
  - Regulatory guidance on UAS FAA
  - Michigan State Police Aviation UAS program
  - Persistent Close Air Support, of Arizona



# Unmanned Aircraft Systems (UAS) and Robotics

---



- Public Safety
  - Incident Management
  - Situational Awareness
  - Surveillance
  - Search and rescue
  - Firefighting and fire spotting/observation
  - Fire Investigation (aerial and infrared photography)
  - Communications augmentation
- Local Emergency Management
  - Pre and post-disaster photos
  - Search and rescue
  - Inspection of buildings and homes impacted by severe weather/earthquakes



# Unmanned Aircraft Systems (USA) and Robotics

---



- Traffic
  - Accidents and accident recreation
  - Traffic conditions monitoring
- Infrastructure Inspection
  - Radio Tower Inspection
  - Bridges
  - Equipment parked on pipelines

# Unmanned Aircraft Systems (UAS) and Robotics



- Working on three outreach documents
  1. Considerations for public safety agencies when implementing a UAS program – (in progress)
  2. Overview of current operational uses of UAS/Robotics by Public Safety (ongoing)
  3. Public Safety communications aerial platforms via UAS (pending)





# Video Technology Advisory Group (VTAG)

**Paul Patrick, NPSTC Vice Chair**

# Video Technology Advisory Group (VTAG)



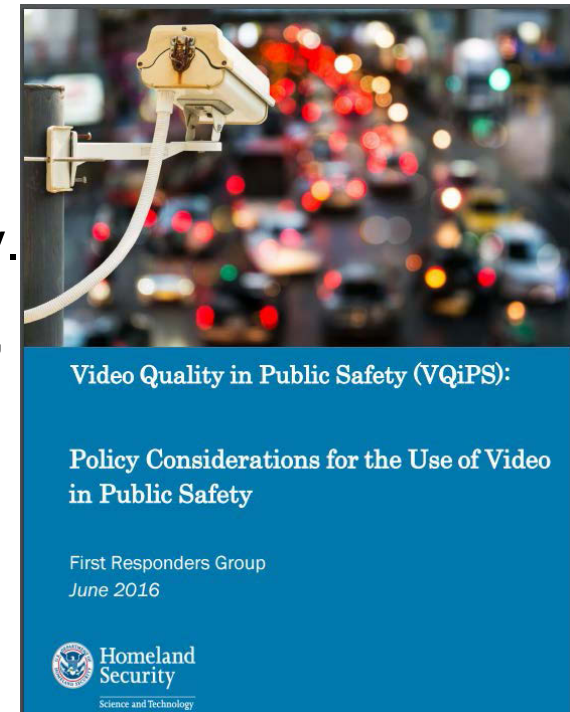
- Support the DHS S&T Video Quality in Public Safety (VQiPS) effort.
- Support the Video Analytics in Public Safety (VAPS) program sponsored by DHS/NIST.
  - New group with focus on public safety agency use of video analytics.

# Video Technology Advisory Group (VTAG)

---



- New resources for public safety agencies:
  - “*Policy Considerations for the use of video in Public Safety*”.
  - Final report released by VQIPS in June.
  - Available on NPSTC website.
  - Provides policy topics that should be addressed by public safety agencies, including privacy, security and transparency.
  - Reviews issues on sighting devices, storage, retention and release of video data.





# Video Technology Advisory Group (VTAG)



- Supported the Video Analytics in Public Safety (VAPS) conference sponsored by NIST.
  - Reviewing public safety agency implementation of video systems and use of analytics.
  - Conference held in June.
  - Analytics can enhance public safety response.



**The First Workshop on Video Analytics in Public Safety (VAPS)  
June 6, 2016, 8:30am – 6:30pm, San Diego, CA**

# Video Technology Advisory Group (VTAG)

---



- VQIPS Annual Workshop, held in Seattle, WA on August 31 and September 1, 2016.
  - Policy round table
  - Agency use case discussions
  - Body worn camera issues
  - The role of video in an active shooter incident
  - Video on UAS platforms
  - Impact of storage, redaction and release
  - Emerging video and analytics technologies
  - Research on human behavioral analysis
- VQIPS Leadership Team developing the 2017 work plan.





# 3<sup>rd</sup> Generation Partnership Project (3GPP)

**Andy Thiessen, Technology and Broadband Committee Vice Chair**

# 3GPP International Standards Update

---

- Update on 3GPP Standards
  - Release 13
  - Release 14
  - Release 15



# Internet of Things (IoT)

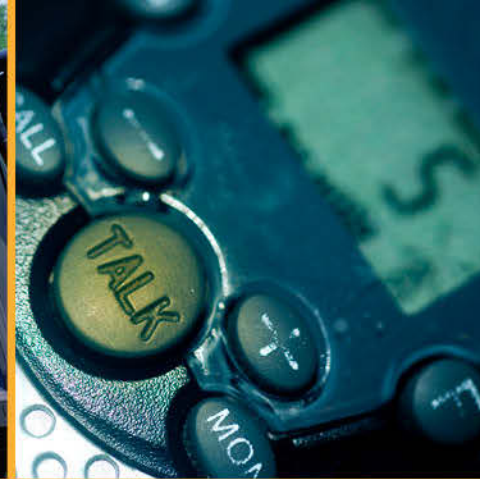
**Tom Sorley**



# Internet of Things (IoT) Task Force

---

- Internet of Things (IoT)
  - In July, the Governing Board approved the creation of a Task Force to assess current IoT issues impacting public safety.
    - The Broadband Emerging Technologies Working Group has been studying various IoT initiatives.
    - The Task Force will examine the IoT ecosystem and will develop a set of recommended issues for the group to focus on.
  - The Governing Board will be asked to approve the Task Forces scope of work once identified.
  - This group will begin its work in January following the completion of Broadband Deployable Systems.



# FirstNet NPSBN Development

**TJ Kennedy, President**  
**Kevin McGinnis, Board Member**

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.



[www.firstnet.gov](http://www.firstnet.gov)

# FirstNet<sup>®</sup>



# Progress Along The Strategic Roadmap

**TJ Kennedy, President**

**September 28, 2016**

# Strategic Program Roadmap





# From: Strategic Program Roadmap Release

# To: RFP Release



Release Strategic Program Roadmap

Public Notices & Comments

Initial State & Territory Consultations

Release Draft RFP Documents

Gather Early Builder Key Lessons

Receive PSAC Findings

Start Expanded Outreach & Consultation

RFP Released

- Initial Consultation meetings in 55 states/territories
- Data Collection in state/territories
- Industry Days with 400+ attendees
- Tribal outreach and consultation
- NEPA/HIPA consultation

## Phases I & II 2014-15

2015-2016



From: RFP Release

To: Complete Draft State Plans

FCC  
opt-out  
NPRM and  
Spectrum  
Relo. Order

NTIA  
opt-out  
Review  
Notice

Focused  
Consultation  
with Expanded  
Outreach

NTIA  
Final Fee  
Review  
Rules

Award RFP  
for Network  
Partnership

Architect  
State Plans  
Process &  
Elements

Final FCC  
Opt-Out  
Rules and  
Further  
NTIA Opt-  
out Grant  
Guidance

Finalize  
Priority  
Network  
Policies

Complete  
Draft State  
Plans

2016}2017

May

- Consultation Task Teams
- Governance Body Mtgs
- Executive Consultations
- In-Person SPOC meetings
- PSAC Findings

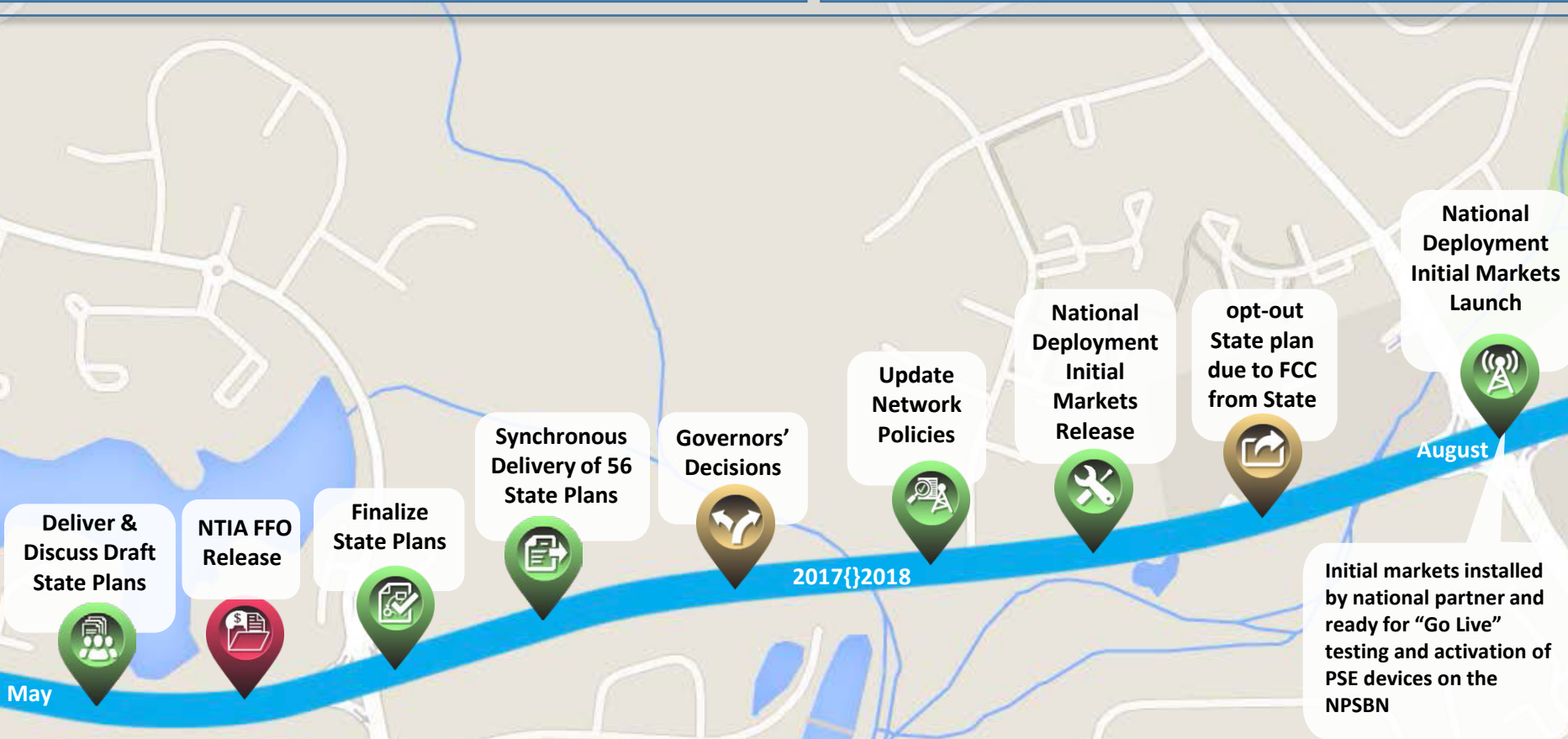
- Culmination of:
- Extensive Q&A Process
  - Pre-proposal Conference
  - Capabilities Statements
  - Proposal Submissions
  - Best Value Determination

# Phase III

\* "These milestone are exclusively controlled by the respective agencies and we have provided target dates based on the best current information available to FirstNet. However, the final timing and outcomes from the relevant proceedings may materially change based on the decisions of the relevant agency."

From: Deliver Draft State Plans

To: Initial Markets Launch






# Phase IV

\* "These milestone are exclusively controlled by the respective agencies and we have provided target dates based on the best current information available to FirstNet. However, the final timing and outcomes from the relevant proceedings may materially change based on the decisions of the relevant agency."

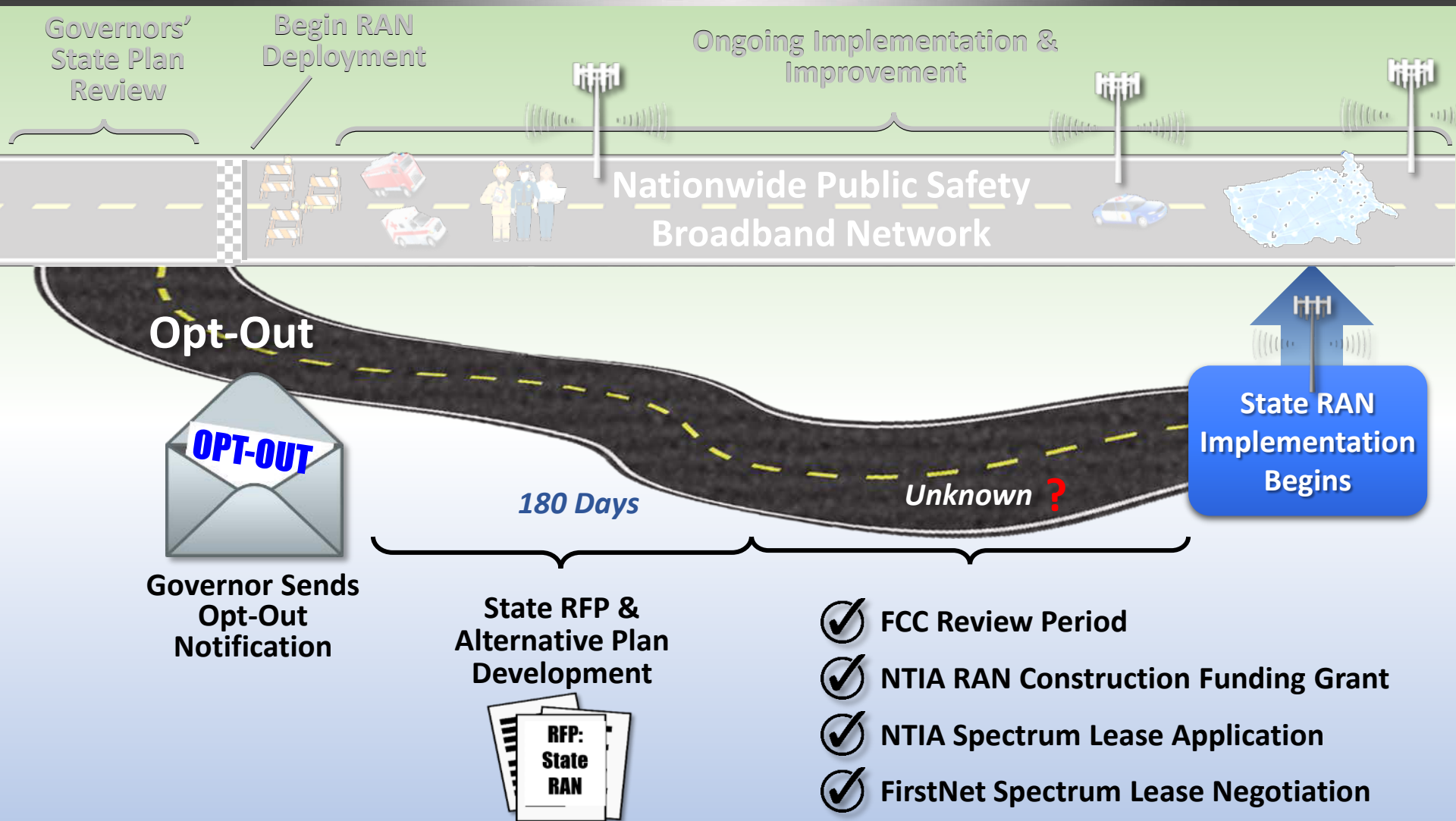
# Responsibilities and Decisions

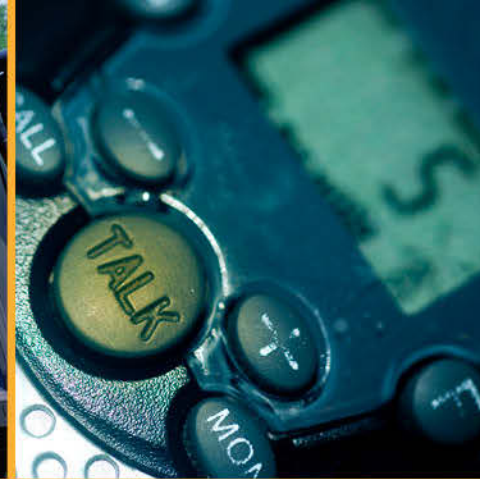


	Decision	Responsibility
 <p><b>BAND-14 CORE</b></p>	N/A	<ul style="list-style-type: none"> <li>✓ FirstNet</li> <li><input type="checkbox"/> QPP</li> <li><input type="checkbox"/> Customer Care</li> <li><input type="checkbox"/> Applications</li> </ul>
 <p><b>RAN DEPLOYMENT</b></p>	<p><b>Governor Decides:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> FirstNet Plan, or</li> <li><input type="checkbox"/> Opt-Out</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> FirstNet, or</li> <li><input type="checkbox"/> Governor</li> </ul>
 <p><b>WIRELESS SERVICES, PRODUCTS &amp; APPLICATIONS</b></p>	<p><b>Public Safety Entities Decide:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Adopt, or</li> <li><input type="checkbox"/> Don't Adopt</li> </ul>	<p><b>Public Safety Entities</b></p> <ul style="list-style-type: none"> <li>✓ Enterprise Users</li> <li>✓ Individual Users</li> </ul>



# Governor's Decision: Timeline

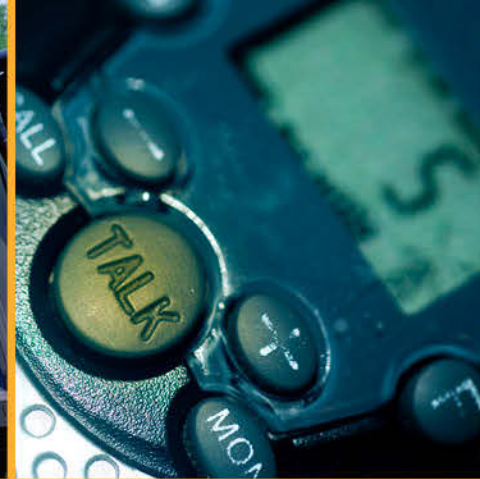




## Lunch *(on your own)*

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.





# Topical Presentation

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.

# Topical Presentation

---

- Compliance Testing, LLC – Michael Schafer, President
- Protecting Public Safety Use of GPS – Greg Buchwald, Chief Technology Office Motorola Solutions, Inc., Engineer

# Issues Providing “P25 Compliant” Radios To First Responders

**Compliance Testing LLC**

**Michael Schafer, President**

[Michaels@ComplianceTesting.com](mailto:Michaels@ComplianceTesting.com)

**Chris Lougee- Director of New Business**

[Chrisl@ComplianceTesting.com](mailto:Chrisl@ComplianceTesting.com)

## NPSTC 2016

# Why are we here? NPSTC:

1. Understands the industry needs and concerns
2. Got FCC to add P25 on 700 MHz Rules
3. Works with TIA developing basic tests
4. Knows the Importance of CAP to its members
5. Interoperability is key

## NPSTC Members would benefit from:

1. More LMR equipment tested sooner
2. More competitive pricing
3. ISSI Tested
4. CSSI Tested





# First Responder Priorities

1. Communication, Communication, Communication with all agencies at a disaster
2. Access to new technologies readily available now
3. User-Friendly Equipment (plug & play)

# Original P25 Objectives- via CAP

1. Interoperability
2. Pricing Competition in Procurements
3. Graceful Migration (Backward & Forward)
4. Spectrum Efficiency

# LMR Manufacturer Priorities

1. Keep testing costs down
2. **52 weeks/yr access to all testing at one location**
3. Opportunity for small radio manufacturers to compete on a level playing field

# Interoperability

1. TIA-102 suite of P25 Test standards
  - 80+ Standards documents completed
  - Interoperable digital Project 25 equipment
2. Compliance Assessment Program
  - Improve confidence in purchasing
  - P25 features and services offered comply with P25 standards
  - Capable of interoperating across manufacturers
  - Ability to communicate with all parties
3. Never more important – Terror Risks

# New Technologies

1. New products trying to come to market...NOW!!!
  - **But - Can't get proper P25 testing done**
  - New P25 features and services added sooner
  - New options to chose from sooner
  - 700 MHz PS spectrum available for P25 compliant radios
2. Plug and Play = Easier to implement!
3. Affordable = Best Value for end users



## P25 CAP is Back

1. New DHS P25 CAP Advisory panel
2. DHS has appointed a new Program Manager
3. New APCO P25 program manager
4. NPSTC asks FCC to require CAP testing (700Mhz)
5. FCC issues R&O (Report & Order)
6. Increased demand for P25 compliance testing by industry and end users

# P25 Issues

1. Radios must be tested to ensure P25 compliance
2. Can't get new technologies CAP tested, timely, affordably
3. Manufacturers can't bring new technologies to market
4. First responders can't deploy enhanced technology
5. How will ISSI – CSSI testing be accomplished?

# Who is best to do CAP Testing?

1. A Competitive Manufacturer?

2. An Independent Lab?

3. Key considerations

- Cost effective, Timely
- Impartiality – Unbiased
- Independent
- Objective
- Credible
- Trustworthy

## Competitor's Lab Issues

1. Can I get in, in time? *So sorry, you missed the RFP date*
2. How comfortable are manufacturers testing at a competitor's lab?
3. Opens IP to the competitor
4. "Product issues" exposed to competitor
5. Can a competitor really be objective / impartial?
6. Could testing delays cause missing a big RFP deadline?

# Independent Lab Issues

1. No logical viable sustainable business model
2. Low volumes of testing cannot support the investment and staffing, maintenance
3. Start up costs too high
4. Ongoing staffing, ISO audits, SME's, support, all very costly
5. Cost of testing prohibitive to LMR manufacturers, especially small ones
6. Loss of Small LMR co's to P25 costs



## Multi-Site Manufacturer Labs vs. One Stop Independent P25Lab

1. P25 Testing must occur at 3 or more labs in 3 different locations at 3 different times
2. CAP ISSI never been done
  - Impractical to Impossible
  - Too difficult logistically
  - Too much cooperation & coordination required between competitors

# US Public Safety Communications Investment **ISSUES**

1. Stated PSCR positions are...
  - “Protect your infrastructure investment through the intersection of the two technologies”
  - “Extend the life of your existing system while beginning to build the new.”
2. New First Responder technology has received over \$100M+ via spectrum sale
3. Current LMR infrastructure in need of financial for appropriate P25 Testing. Est \$20-25mm

## **Solution** - One Stop Independent P25 Lab

1. Independent=UNBIASED-IMPARTIAL
2. All LMR Testing under 1 roof, 1 trip
3. ISSI & CSSI testing available
4. Open all year for testing vs 2 weeks per year
5. Fully equipped & Staffed
6. Accredited to ALL P25 Standards & FCC
7. Expected Start up Costs \$5-10M set up
8. \$2-3M / year operational expenses
9. \$4-5mm / yr to test all company's radios

# Budget for P25 One Stop Independent Lab

	Current Test Volumes	Expected Test Volumes
Description	Low	High
Start up costs	\$ 5,000,000	\$ 10,000,000
Operational costs/yr	\$ 1,000,000	\$ 3,000,000
All testing /yr covered for LMR mfgs	\$ 2,500,000	\$ 5,000,000
5 year total	\$ 22,500,000	\$ 50,000,000
Avg Cost Yr	\$ 4,500,000	\$ 10,000,000

## Current Status P25 - **ISSUES?**

1. New CABS just published 8/10/16
2. Previously “P25 Accredited” test labs ... expire 8-2017
3. Retesting of all radios to new standards by 8-2017
4. Labs must be re-accredited within 1 year to a new DHS Lab requirement ISO17025
5. Previously accredited labs may continue testing thru Deadline

## Field issues force Consideration of Deeper understanding of **Test ISSUES**

1. “Model Class” Test ~ “Test the Parent” and assume “similar-family” models would also pass, *would they really pass?*
2. Firmware changes – Ought they be tested?
3. Theoretical vs Practical application *“This ought to be ok ,so we shouldn’t need to test it” We are motivated (biased) to reduce not increase testing.*
4. Conformance Testing - Not ready, but objective is easier “plug & play” LMR implementations
5. P25 Testing for LMR vendors could become prohibitively expensive to meet “*plug & play*” goal, especially smaller Co’s



# Potential Solution- Federal Funding

Solves all the issues:

1. New P25 Radios & equipment to First Responders sooner
2. Much easier to get through testing for LMR manufacturers
3. No testing fees means, Small LMR manufacturers are not put out of business or out of P25 participation
4. Keeps Equipment Costs down for Cities – Users
5. More testing aids “Plug and Play” objective
6. Both Model Class & Firmware changes get tested

# Requests of NPSTC

1. Send a letter of support to DHS
2. Propose Federal Funding source suggestions

# Questions?

## **Compliance Testing LLC**

**Michael Schafer, President**

[Michaels@ComplianceTesting.com](mailto:Michaels@ComplianceTesting.com)

**Chris Lougee**

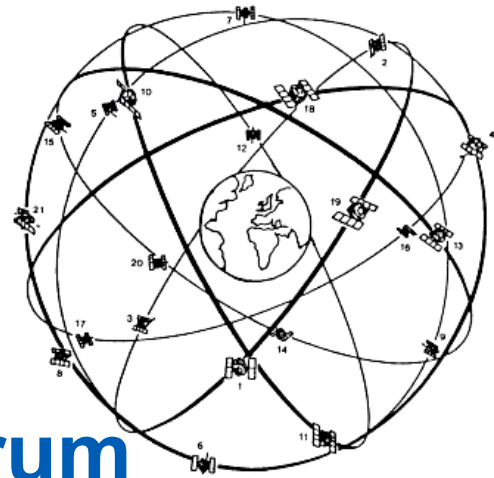
**Director of New Business**

[\*\*Chrisl@ComplianceTesting.com\*\*](mailto:Chrisl@ComplianceTesting.com)



# Protection of GPS Services for Public Safety Needs

## The Genesis of L-Band Spectrum



Discussion, Analysis, and Cooperative Action Steps



Greg Buchwald  
DMTS Engineer  
CTO Organization  
Motorola Solutions, Inc

# History of L-Band Spectrum Allocations

## ■ 1500 / 1600MHz Bands

- Primary Allocation: Mobile Satellite Service (MSS)
  - GPS 1575.42MHz +/- 10MHz; other GNSS systems
  - Radioastronomy ~1610MHz
  - Inmarsat, Iridium; etc.
- **Weak Signal use-cases**

## ■ 2003

- FCC approves the use of Auxiliary Terrestrial Component (ATC) in the MSS spectral allocation bands; satellite component requirement removed
  - Action was essentially ignored by the industry
  - Allowed terrestrial power levels up to +72dBm EIRP / ~16kW
  - Protected 1559 – 1610MHz for GNSS (GPS) services

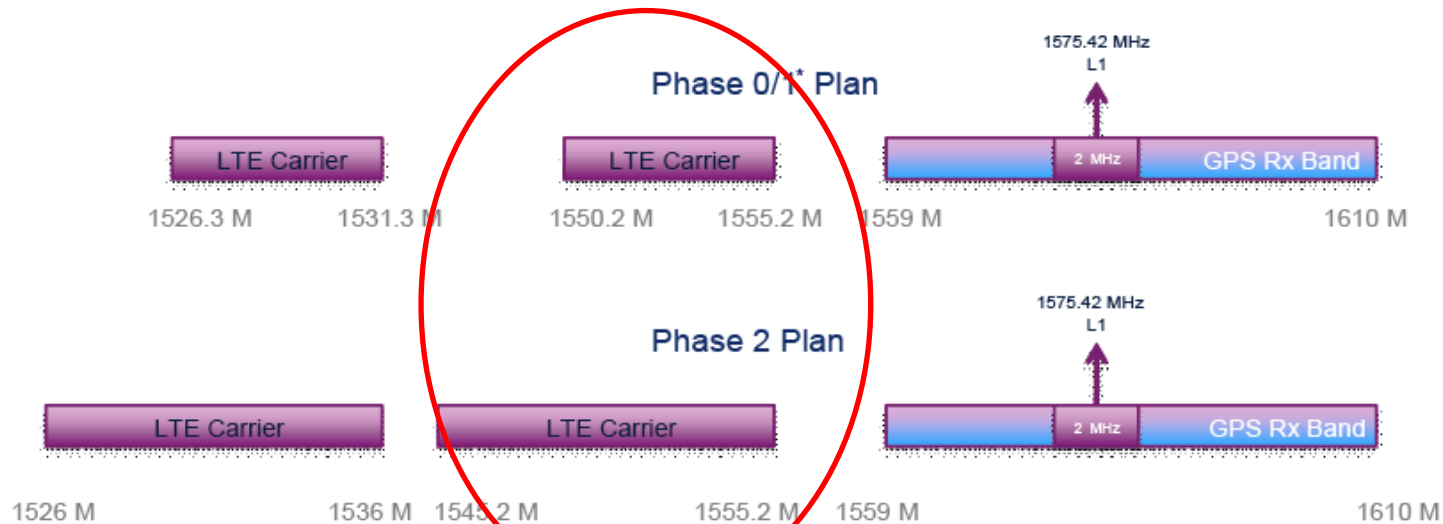
## ■ 2009/2010

- Next-Gen GPS-based aircraft assisted-landing system approved.
- Harbinger request approved (2010)
- GPS Industry awakens; realizes threat to currently-deployed GPS-based systems
- February, 2011: FCC reacts by temporarily withdrawing approval to deploy; orders Working Group formed to assess interference potential.

# LightSquared Terrestrial Service Landscape in 2011

## 2.1. L-band ATC Frequency Plans GPS

Figure 1 describes the LightSquared's present ATC frequency plans by deployment phase. These plans are subject to coordination with other satellite operators and may change in the future. However, a change in the frequency plans would not change LightSquared's obligations to protect other services in adjacent bands, such as GPS.



\* Only upper 5-MHz LTE carrier is used in Phase-0. Both 5-MHz carriers are used in Phase-1

Figure 1: Lightsquared Downlink LTE L-Band and GPS Band



# Round 1 Testing; Industry-wide 2010-2012

- Lab testing of Motorola Solutions Infrastructure Equipment Began December 2010. Initial test results reported to FCC early March, 2011
- Test program expanded to include mobiles, portables, MDTs, PTP, PTMP, accessories and older infrastructure
- FCC Working Group formed
  - Motorola Solutions:
    - Advisor status / participation on the Precision Timing and General Location and Navigation Sub-groups (FCC); daily calls 7 days a week for 6 weeks.
    - **Chaired above-listed sub-groups for NPSTC (National Public Safety Telecommunications Council) including FCC response / filings**
- Live Sky Testing
  - Las Vegas, NV: May, 2011
- Additional WG lab testing
  - Alcatel Lucent: Late May, Early June, 2011
- FCC WG report filed June 30, 2011
  - Comment period ended July 30, 2011
  - Reply Comment period ended August 15, 2011

# Interference Scenarios

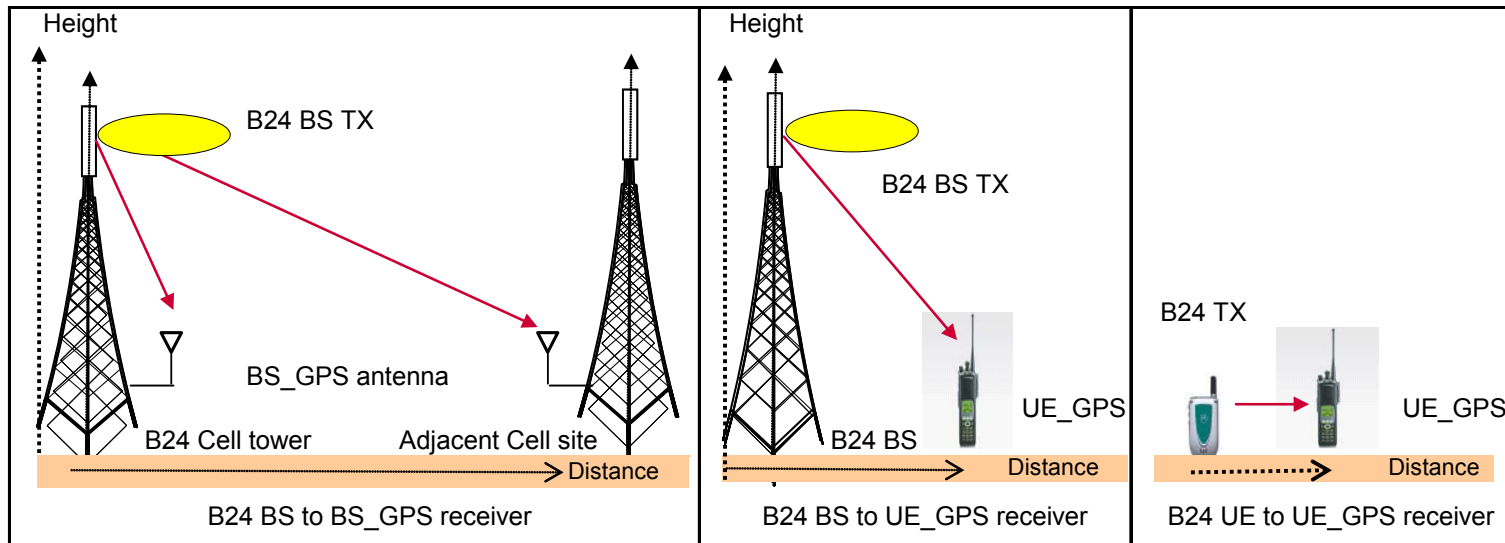
## Two Interference Mechanisms

### 1) OOB into GPS receiver – can only be fixed at L.S. transmitter

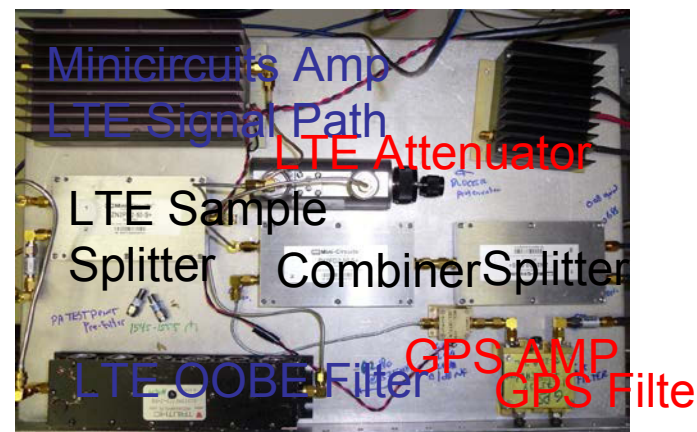
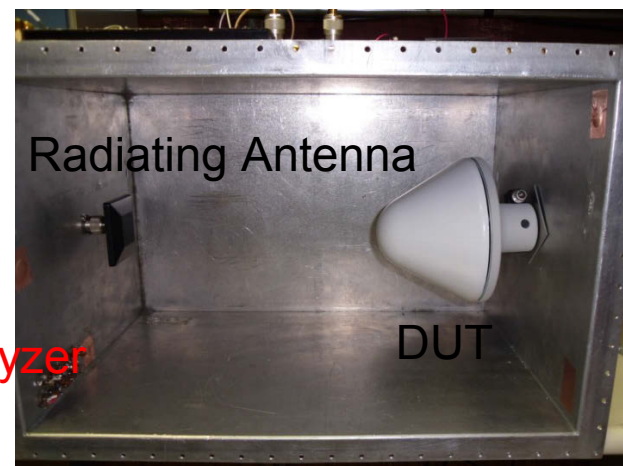
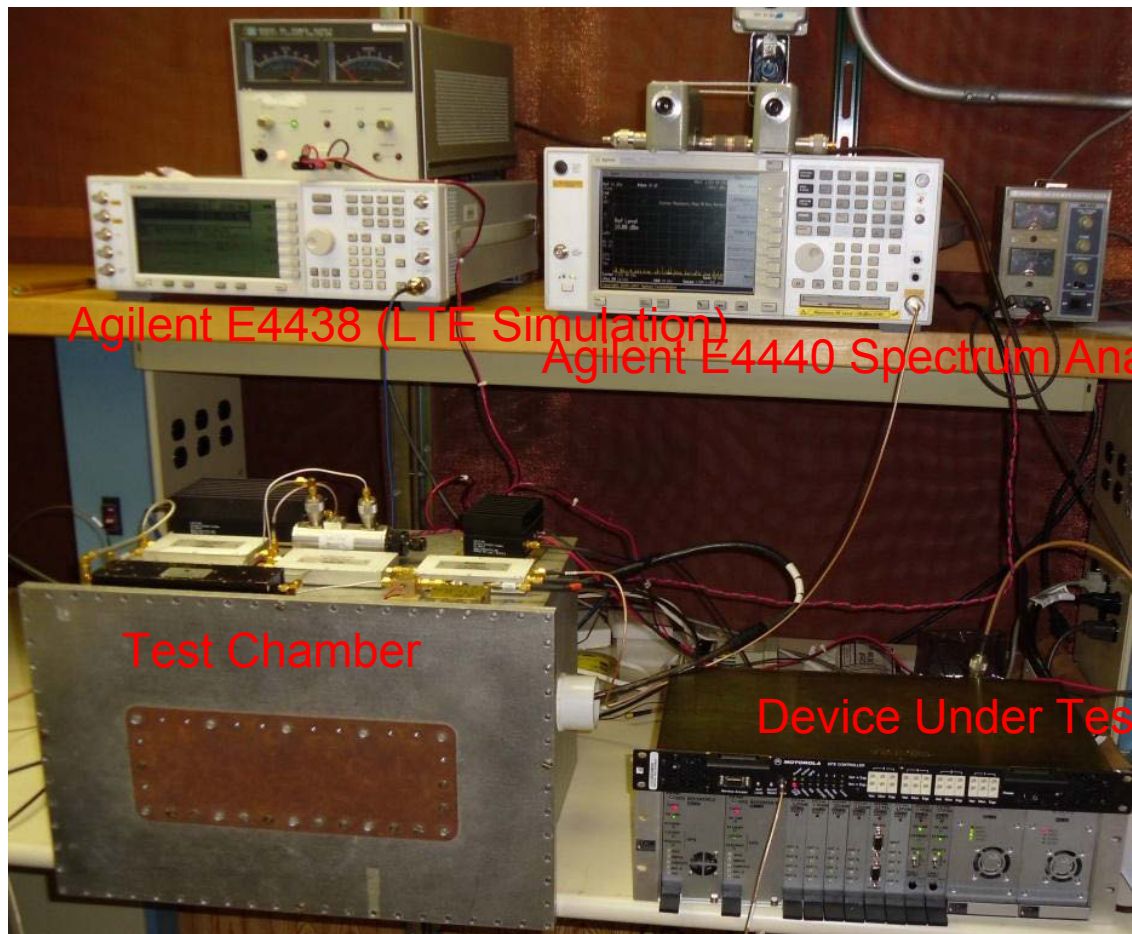
- LightSquared is added filtering to mitigate

### 2) **GPS receiver blocking** – can only be fixed at receiver

- Function of GPS receiver design and,
- Distance between LightSquared Transmitter and Victim Receiver
- **Cross-Modulation Product-caused Interference.**



# L-Band Interference Test Fixture



# Lengthy Test Procedure.....

- Determine proper GPS level: -142dBm/2MHz at the receiver / DUT input.
- Increase interfering LTE signal until lock is lost. Reduce interferer level until lock is regained.
- Increase the interferer level by 10dB so that lock is lost.
- Reduce interferer level by 10dB; check receiver / DUT for reception and lock of at least 4 satellites within 60 seconds.
  - If lock is attained, record level.
  - If lock could not be attained, reduce interferer level by 1dB; recheck lock status.
  - Determines level at which the DUT recovers from a short term 10dB increase in the level
- A total of four measurements are made within a time span of 10 minutes to determine the maximum allowable interference level.
  - The worst case number is noted out and the remaining levels were retained.
- Repeat after 24 hour interval after the initial measurement.
  - Composite tests: composite test signal is fed directly to the DUT.
  - Radiated tests: path loss between the passive, radiating antenna and the DUT antenna is measured.
- The above-listed tests are performed with a 10MHz BW LTE waveform (fc=1550MHz).
- **Calculate Denial of GPS Service Radius based on Free-space Path Loss (PLE = 2)**
  - Denial of GPS Service radius based on 1kW EIRP (+60dBm)

**RIGOROUS;  
TIME CONSUMING**

# Primary Consequences of Interference

## ▪ Base Station

- Simulcast Systems
  - Immediate alarm sent to dispatch or control office if tracked and locked satellites drops below 4
  - In as little as 4 hours or as much as 24 hours, site becomes disabled; taken off-line (lack of timing reference)
    - Lost timing accuracy
      - Alarm, system degradation, potential site deactivation
      - Collision avoidance, spectrum efficiency impacts...self-interference

## ▪ Subscriber Units

- Reduction of location accuracy
  - Officer scenarios
    - Officer-down location: potential response time impact, etc.
    - Traffic stop location: important in escalated situation
  - Potential impact to location stamping of voice and video recording used for evidence
  - NPSTC: 10 – 15 meter accuracy required by most equipment contracts

# Mitigation Methods Employed

- Redesign devices to utilize improved GPS chipsets, and
- Re-design the antenna to incorporate a narrowband filtering
  - Impact to sensitivity of GPS receiver due to additional insertion loss
  - Cost involved
- Infrastructure Timing: Utilize High-rejection Antenna / LNA equipment now offered

Device Number	LTE Level, RX Input	Distance A Bore-sight	Distance B -20dB
1	-20dBm	155 meters	15.5 meters
2	-20.5dBm	160 meters	16 meters
3	-24dBm	240 meters	24 meters
4	-48.5dBm	4.1 km	410 meters
5	-37.5dBm	1.1 km	110 meters
6	-18 dBm	120 meters	12 meters
7	-20dBm	155 meters	16 meters
8	-22dBm	190 meters	19 meters
9	-47dBm	3.8 km	380 meters
10	-35dBm	350 meters	35 meters
11	-38dBm	1.2 km	120 meters
12	-35dBm	350 meters	35 meters
13	-1.8dBm	19 meters	1.9 meters
14	-2.2dBm	20 meters	2.0 meters

APX6000 UHF (w/SAW)

Device Number	LTE Level, RX Input	Distance A Bore-sight	Distance B -20dB
15	-36dBm	950 meters	95 meters
16	-37dBm	1.1 km	110 meters
17	-26.5dBm	325 meters	33 meters
18	-24dBm	245 meters	24.5 meters
19	-28dBm	390 meters	39 meters
20	-18dBm	110 meters	11 meters
21	-29dBm	435 meters	43.5 meters
22	-39dBm	1375 meters	137.5 meters
23	-33dBm	680 meters	68 meters
24	-30dBm	490 meters	49 meters
25	+11.5dBm	<3 meters	<<3 meters
26	+10.5dBm	<3 meters	<<3 meters
27	+5dBm	4.75 meters	<3
28	+4dBm	8 meters	<3 meters

High Rejection Infrastructure

APX7000

Containment of the problem and designing for the anticipated deployment environment is critical to meeting the needs and expectations of public safety and the industry.



# June, 2014 FCC Workshop on GPS... Signals Action on L-Band Spectrum

Home / News & Events / Events /

## Workshop on GPS Protection and Receiver Performance



JUN  
20  
2014

Workshop on GPS Protection and Receiver Performance

9:00 am - 5:00 pm EDT

Commission Meeting Room, FCC Headquarters, 445 12th Street, S.W., Washington, D.C.

Begin to consider the impact to GPS from high power terrestrial signals in L-band spectrum once again; reach out to influence deployment criteria and regulatory environment

## Workshop on GPS Protection and Receiver Performance

Motorola Solutions, Inc.  
*Greg Buchwald*

June 20<sup>th</sup>, 2014

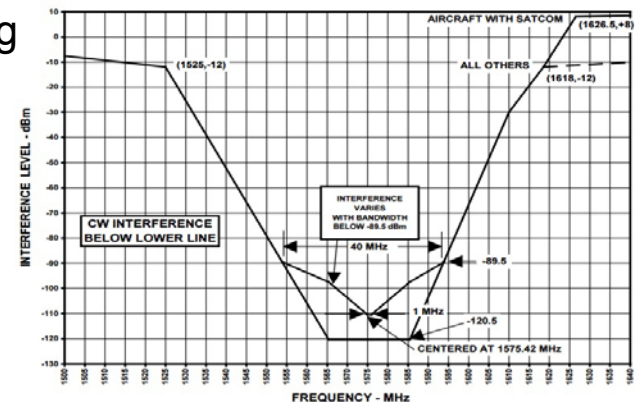


1

# Renewed L-band Emphasis by LightSquared in 2015....

## ■ Revised LightSquared band-plan; Roll-out

- Downlink:
  - The “Upper” band (~1545 – 1555MHz) will not initially be deployed
  - “Lower” band (~1525 – 1535MHz) will be rolled out as a 10MHz LTE downlink channel
- Uplink:
  - 10MHz LTE profile;  $f_c$  between 1628 and 1631MHz; 1670 – 1680MHz
  - Standard LTE uplink power profile: +23dBm
- Mid-band ~1551MHz allocation still in long term plan; doubtful it will ever succeed.
- FAA / DoD and NWS resolution discussions on-going



# Renewed Testing; New Era of Increased Cooperation and Industry Input

- Cooperative approach from Ligado (LightSquared)
  - Roberson and Associates retained to perform all tests
  - R/A reached out to NPSTC for input on test procedures and regulatory perspective
  - Ligado reached agreements with John Deere, other GPS manufacturers – again, extensive cooperation
  - NPSTC met multiple times face-to-face with R/A; inputs always openly taken and acted upon
    - Strongly Influenced Test Procedures
    - Measurement of re-acquisition of GPS signal methods,
    - Power Flux Density (on ground); PSD levels,
    - Several other concerns

# NPSTC Actions and Initial Filing Q2/3/4 2015

Comments re: Ex Parte presentation in IB Docket 12-340; SAT-MOD-2010118-00239, 2012-0928-00160, 20120928-0161, 20121001-00872 filed 25 August, 2015

## GPS Sensitivity Measurement Plan; revised

On August 11, 2015, I met with Roberson and Associates at their Schaumburg office at the request of Stu Query on behalf of NPSTC. Stu Query was present. At that time, we discussed issues identified within the then-current test plan proposed by Roberson and Associates. In the ensuing time since that meeting, a revised test plan was presented to the Commission by LightSquared through their Council, Gerald Waldron of Covington and Burling.

Stu Query asked that I review the revised document and comment on the revised test plan. My comments follow:

In general, the test plan accurately reflects the interests of the Public Safety community including NPSTC and its membership. There remain a small number of issues that require clarification and/or revision. These will be addressed by page number in the revised (25 August, 2015) test plan presented to the Commission.

On Page 4: There remain only two identified public safety devices that will be tested (as opposed to multiple additional items in the 2011 time frame testing): The MSI APX7000 subscriber device and the MW810 Mobile Data Terminal. MSI feels that these two devices sufficiently represent products currently in production and offered for sale to the Public Safety community. It would be better if these devices were called out in a separate category, or at a minimum, a footnote identify these as devices that are utilized for public safety / critical life safety applications. Categorizing them with "general location and navigation devices" suppresses the criticality of accuracy and reliability of such devices: Data recorded by these devices may be utilized for evidentiary purposes, is critical to fast response in the case of officer down and other life / safety issues, and for accurate response of limited resources through dispatch. The importance of GPS data in these use-cases must not be lost or reduced. MSI also notes that certain other law enforcement devices which are not manufactured by MSI but of critical importance to the law enforcement community seem to not be represented in the test plan. These include devices such as "ankle bracelet" tracking devices for those held on house arrest and limited release. Also, vehicular tracking devices, utilized for surveillance purposes, should also be included in the test plan. NPSTC should consider whether these devices should be added to the list for completeness and to insure that proper coverage is included. We also note that timing reference signal devices, such as those manufactured by Trak, are not represented in the Timing portion of the test plan; however, the devices listed adequately



September 9, 2015

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, DC 20554

Re: IB Docket No. 12-340

Dear Ms. Dortch:

The National Public Safety Telecommunications Council (NPSTC) is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. Accordingly, NPSTC provides guidance on issues that can either negatively impact or benefit the operation of public safety communications.

On June 24, 2015 through its legal counsel, LightSquared, LLC submitted notice of an *ex parte* presentation made to Commission officials by its engineering consultant Roberson and Associates. The LightSquared filing addressed "an initial perspective on testing of the compatibility of terrestrial broadband and GPS."<sup>1</sup> LightSquared subsequently submitted a revised test plan on July 15, 2015. The *ex parte* statement that accompanied this revised plan noted "...we hereby renew the request for such comments and critiques and hope to receive feedback within the next week, since testing is anticipated to

## Summary

- **NPSTC has remained vigilant on the issue of GPS protection**

- It remains the industry-wide advocate of GPS protection for the Public Safety Community.

- **Terrestrial use of L-band will most likely occur**

- The spectrum is far too valuable to allow it to lie fallow,
- MSS services have proved to be useful in rural areas while urban areas can best utilize the spectrum for terrestrial use-cases,
- The FCC is under tremendous pressure to open additional spectrum for broadband.

- **Spirit of Cooperation**

- LightSquared was selectively cooperative in the 2011/2012 time frame,
- The re-organized LightSquared, now Ligado, is attempting to cooperate industry-wide this time around: 2015/16,
- Involvement of third party consultants that have interest in opening spectrum yet protection of incumbents and adjacent service users such as Roberson and Associates demonstrate their desire to find a fully workable solution.

**We must all remain vigilant - trust but verify. NPSTC and its partners in this activity have public safety's best interest in mind.**

# Additional Slides for Discussion and Q/A

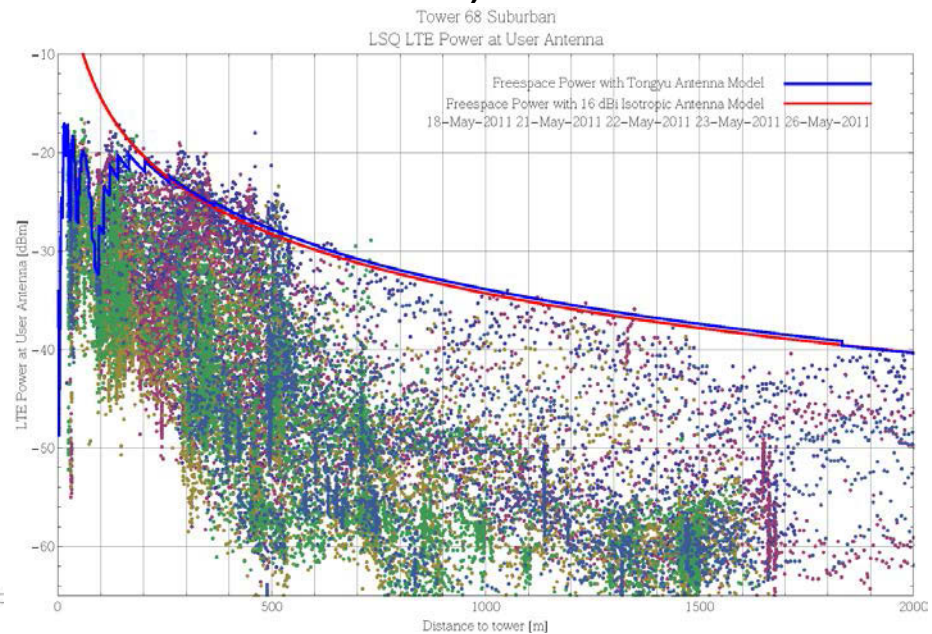
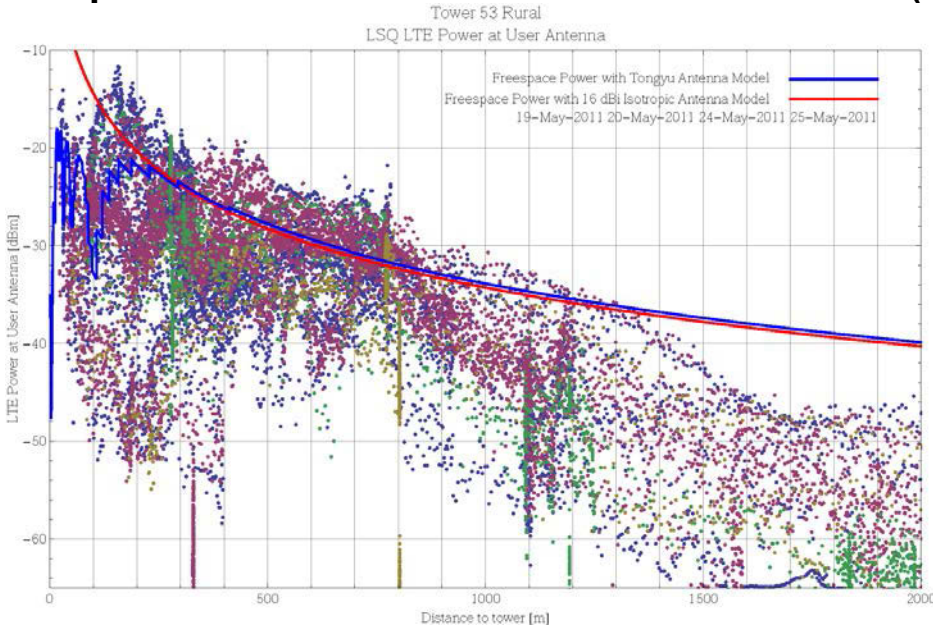


# Live Sky Testing: Las Vegas, NV

Early Subscriber Denial of Service radius ~185 meters

MDT Denial of Service Radius ~610 meters

Improved Denial of Service radius ~25 meters (slant distance ~65 meters)

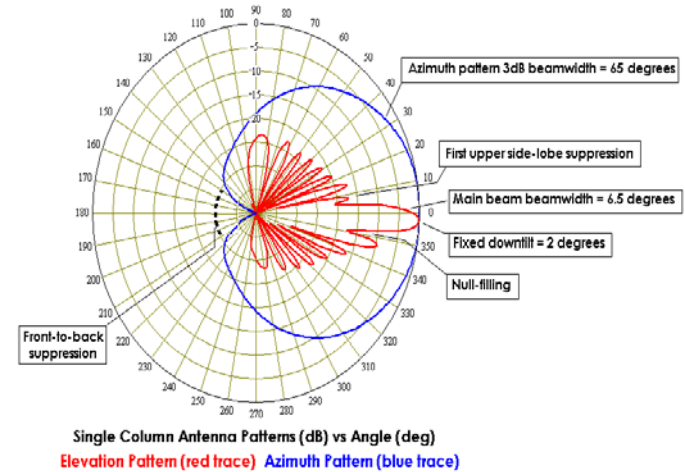


Received signal levels exceeded free space models in conjunction with published antenna power gain and pattern information in many cases. This is primarily due to efficient close-in reflecting objects (building, etc.) and “bounce” off the road causing constructive interference.

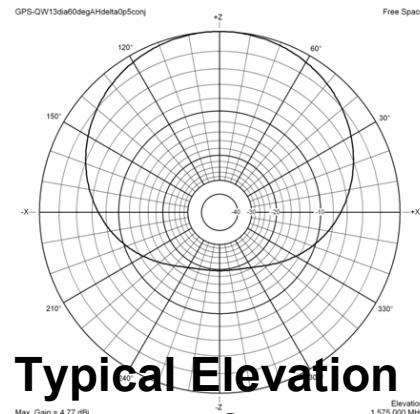
From the Working Group FCC filing June 30, 2011; combined data from 5 companies p

# Interference Distance Calculations

- **Freespace Path Loss, FSPL is defined as:**
  - $FSPL_{(dB)} = 20\log(d) + 20\log(f_{MHz}) - 27.55$ ; where d is in meters
  - $FSPL_{(dB)} = 20\log(d) + 36.25$  @ 1550MHz
- **“Distance A” represents the LOS (Line of Sight) Denial of GPS Service radius assuming FSPL (Path Loss Exponent, PLE=2)**
- **“Distance B” represents the LOS Denial of GPS Service radius assuming an additional 20dB path loss (PLE=2) due to the elevation pattern of the L-Band base station antenna as well as the elevation pattern of GPS antenna**
  - Pattern loss can vary from <12dB to >25dB depending upon deployment; 20dB is a typical value.
- **Non-LOS path loss will be higher (ex: Base station to subscriber unit) in many instances. The PLE can vary from <2.8 to >3.6 for concerned range of separation distance.**
  - Example: A PLE of 3.3 will reduce the denial of service radius from 3600 meters to 145 meters
  - However, many services and deployment scenarios will endure LOS interference conditions



## PCS Antenna Pattern Example



## Typical Elevation Pattern of a Quadrafilar GPS Antenna

## Lead Paragraph of FAA Letter to NTIA From the FAA Introducing Their Report on LightSquared Impact Upon GPS



U.S. Department  
of Transportation  
  
Federal Aviation  
Administration

Office of the Administrator

800 Independence Ave., S.W.  
Washington, D.C. 20591

JAN 27 2012

The Honorable Lawrence E. Strickling  
Administrator  
National Telecommunications and  
Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue, NW.  
Washington, DC 20230

Dear Mr. Strickling:

In June 2011, RTCA completed an assessment of the potential interference to certified aviation receivers resulting from the planned LightSquared long-term evolution (LTE) 4G network (RTCA, Assessment of the LightSquared Ancillary Terrestrial Component Radio Frequency Interference Impact on GNSS L1 Band Airborne Receiver Operation, RTCA/DO-327, June 3, 2011). This report concluded that their planned operation of the upper 10 MHz LightSquared channel would cause significant interference to GPS and should not be allowed. However, this report was inconclusive on the use of only the lower 10 MHz LightSquared channel, and the report recommended further study.

## Section of FAA Report Discussing the Internationally-Harmonized Rejection Requirements for Adjacent Band Emissions Operating Near GPS Spectrum Allocations

The passband for this equipment is from 1565.42 MHz to 1585.42 MHz. Adjacent-band rejection requirements are specified for continuous waveform (CW) RFI below and above the GPS band, and all equipment is designed and tested to ensure that these requirements are met. The complete requirements are defined in Appendix C, RTCA/DO-229, which was first published in 1996. The same requirements are harmonized internationally (ICAO SARPs Annex 10 Volume I, paragraph 3.7.4) since 2001. For convenience, the CW filter rejection curve is shown in Figure 1-1. The adjacent-band rejection is enabled by filtering in the antenna and the receiver. As an example, for a CW signal at 1531 MHz 92.4 dB of rejection is designed into the aviation standards.

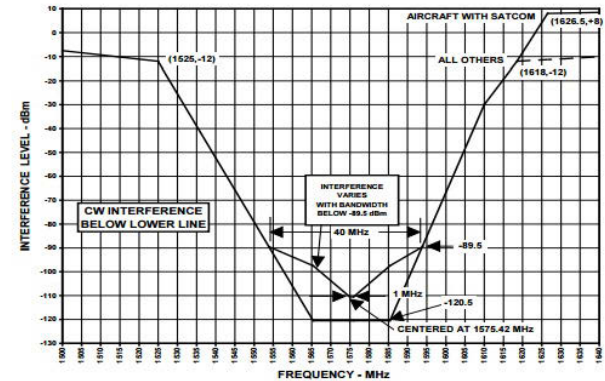
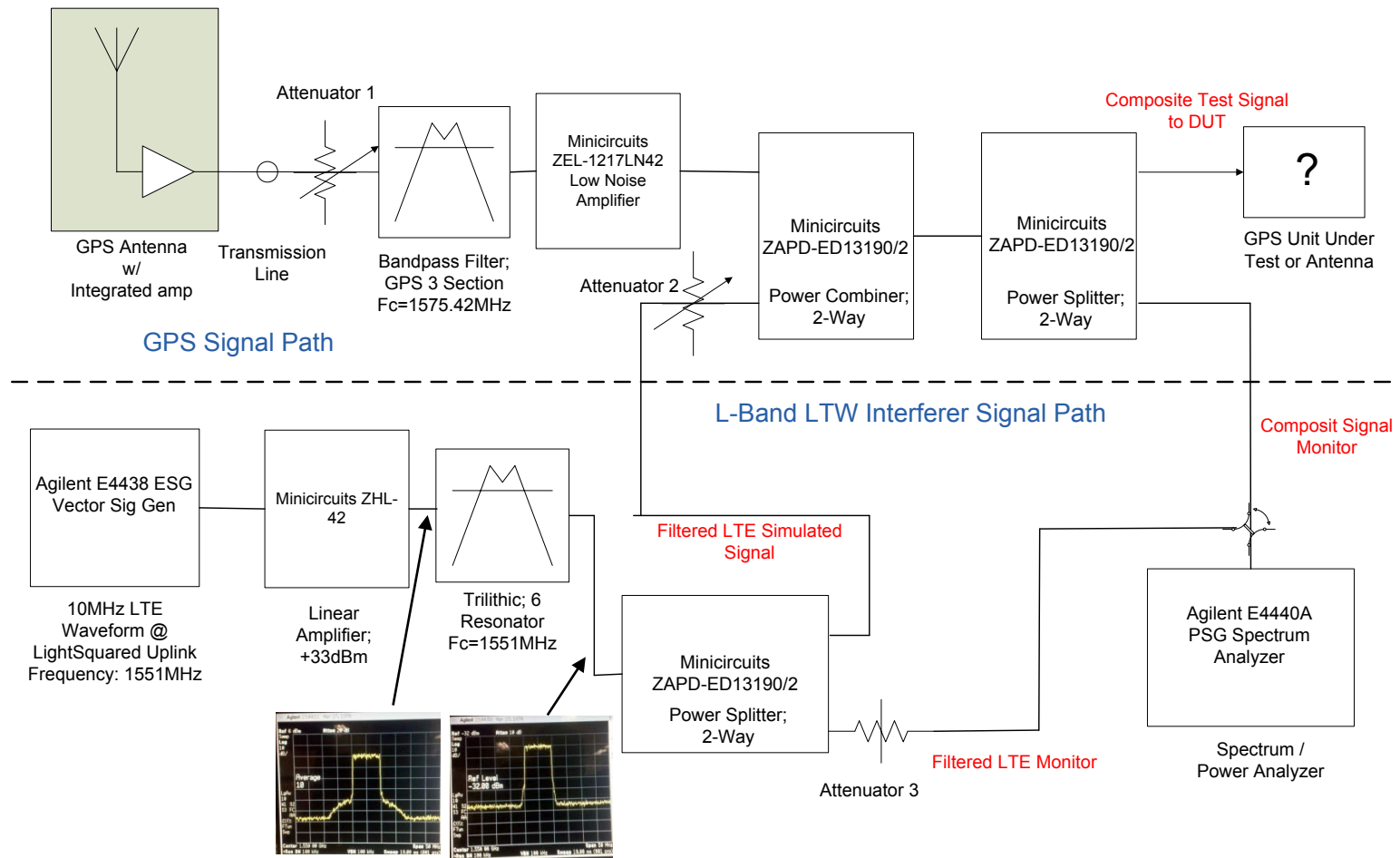


Figure 1-1 Out-of-band CW Interference Rejection Levels

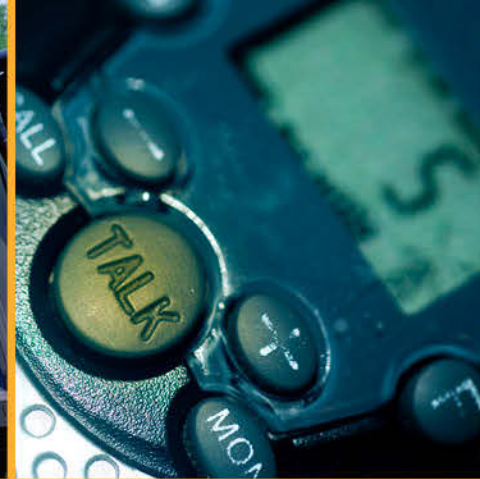
The curve only specifies rejection of CW interference. Results from testing a limited number of certified receivers has indicated that tolerable interference levels are nearly equivalent for CW and a 10 MHz broadband noise signal centered at 1531 MHz. The

# Laboratory Test Configuration



Lab Test Configuration  
GPS Interference / Blocking Susceptibility to  
LightSquared L-Band Transmissions





# Interoperability Committee

**John Lenihan, 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.



# Encryption Task Force

**John Lenihan, Interoperability Chair**



# Encryption Task Force



- FCC rule issued in April mandates use of analog FM for mobiles/portables on FCC-designated interoperability channels in the VHF, UHF and 800 MHz Band.
  - This rule establishes analog as the required method of communication on designated interoperability channels.
  - This rule effectively prohibits use of digital encryption on designated nationwide interoperability (I/O) channels, including Calling and Tactical channels.



# Encryption Task Force



- Encryption:
  - Encryption is allowed on some nationwide channels (ex: VLAW31).
  - Encryption is allowed on all 700 MHz I/O channels (other than the two 700 MHz Calling Channels).
  - Encryption is allowed on all local, regional and statewide I/O channels (based on established policy).



# Encryption Task Force

---

- Task Force is finalizing an outreach document which will educate public safety agencies on the analog mandate and the impact to interoperability and encryption.
  - The document will include a listing of FCC approved nationwide interoperability channels that are affected by this rule.
- The outreach document will flow through the Interoperability Committee before reaching the Governing Board for consideration in November.





# Emergency Medical Services

**Paul Patrick, Chair**

# Emergency Medical Services



- Completed outreach document to encourage EMS agencies to join statewide FirstNet planning efforts.
  - Document approved by Governing Board on September 15<sup>th</sup>.
  - Designed for use by SWICs and SPOCs to get more EMS participation.
  - Thanks for Kevin McGinnis and Paul Patrick for organizing the final document based on input from the EMS Working Group.



## Ten Reasons YOU Need to Be Engaged with FirstNet

FirstNet is building a Nationwide Public Safety Broadband Network. EMS stakeholders are necessary to help define prehospital broadband capabilities. *Are you at the table?*

# Emergency Medical Services

- GPS enabled medical alarms
  - Wearable medical alarms which activate while patients are away from home.
  - Devices have a sensor that can detect a fall and will automatically transmit an alert to the company's call center.





# Emergency Medical Services



## Top 10 Best Medical Alert Systems of 2016

With a GPS medical alert system, if you're unable to communicate, the operator automatically assumes that you're in need of medical help and contacts your local emergency personnel with your GPS coordinates. The response time is much faster.

These devices are able to determine when you've experienced a fall and can automatically contact the monitoring center without requiring you to press any buttons. In most cases, fall detection requires an upgrade and isn't included in the base unit.

A+ BBB Rating

For Active & Independent Seniors



- ✓ Wearable mobile (GPS) and fall detection
- ✓ No long-term contracts
- ✓ Free equipment, activation, and shipping
- ✓ Lifetime warranty on equipment

# Emergency Medical Services

---



- GPS enabled medical alarms
  - EMS agencies are getting calls to respond to GPS locations with no patient contact.
  - Other medical sensors are also being created which will impact public safety, including heart and glucose monitors connected with the patient's smart phone.
  - How are medical sensor calls managed when there is no patient contact or verification of an emergency?
    - Does EMS respond?
    - Does law enforcement respond?
    - Is the call treated like a 911 hang up?

# Emergency Medical Services

---



- GPS enabled medical alarms
  - Working Group is gathering information from vendors.
    - Attempting to identify key market areas.
    - Invite a representative to discuss their solution, verification, false alarm rates, etc.
  - Making contact with public safety agencies in the market areas to determine their experience.
  - Create an outreach document educating agencies on the emergence of these devices.

# Emergency Medical Services

---

- Monitoring pre-hospital video by EMS personnel.
  - EMS Telemedicine Report published in 2015.
  - Continue to monitor video use by EMS agencies.
  - Scheduling follow up from agencies with pilot projects.





# Cross Border Working Group

**John Lenihan, IO Committee Chair**

# Cross Border Working Group

---

- Regulatory Update on Cross Border Base Stations
  - FCC and Canada released guidance on cross border base station placement on June 30<sup>th</sup>.
  - NPSTC has conducted outreach activities to educate public safety agencies along the border.
  - CITIG has also been publishing information for Canadian public safety agencies.
  - NPSTC and the FCC are planning a webinar on October 17<sup>th</sup>.





# Cross Border Working Group

- Cross Border 911 data sharing
  - How does a U.S. PSAP access Canadian customer cellular account information?
  - How does a U.S. PSAP obtain GPS coordinates from a Canadian cell phone carrier during a border emergency?
  - Creating outreach report. U.S. component has been completed, Canadian component in progress.
    - Provides guidance to PSAP's on how to access information in an emergency.



# Cross Border Working Group

- Cross Border 911 Call Routing
  - Mexico is currently implementing 911 to replace their “006” emergency line.
  - The State of Texas has identified problems with 911 calls from Mexico being routed to their PSAPs.
    - US Citizens in Mexico are dialing 911 and reaching Texas PSAPs.
    - Mexican citizens in Mexico are dialing 911 and reaching Texas PSAPs.
    - Mexico reports 911 callers in Texas are reaching their PSAPs.
  - Texas is working with US and Mexico wireless carriers to address routing.



# Cross Border Working Group (

---

- Other Working Group activity:
  - Emergency Vehicle Border Crossing Best Practices
    - Report on strategies for expedited border crossings to assist fire and EMS agencies whose units transit the U.S./Canadian border.
  - Working with OEC Regional Coordinators to identify issues and solutions.
  - Monitoring the planning for CAUSE IV experiment scheduled for 2017.
  - Examining the impact of the FCC's railroad police interoperability order and whether Canada has a similar rule.



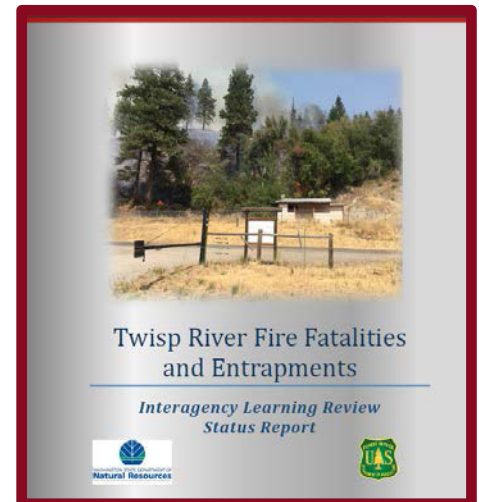
# Radio IO Best Practices Working Group

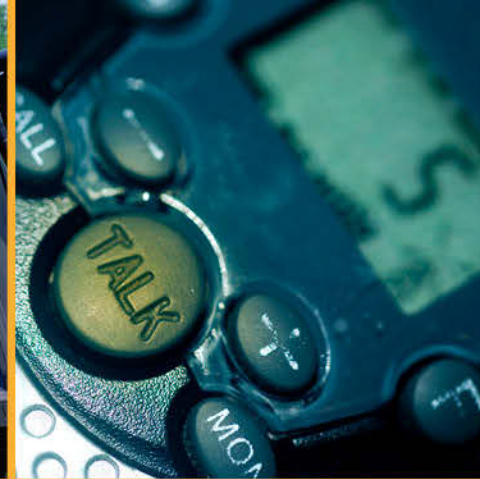
**John Lenihan, IO Committee Chair**

# Radio IO Best Practices Working Group



- This group reviews after-action reports following major incidents and creates best practice recommendations to ensure successful operations.
- The following Best Practice Statements are nearing completion and will be routed to the full I/O Committee for review:
  1. Radio Channel Naming
  2. Training on use of I/O systems and equipment
  3. Change Management Process involving I/O systems
  4. Infrastructure Management for I/O networks





## Award Presentation and Break

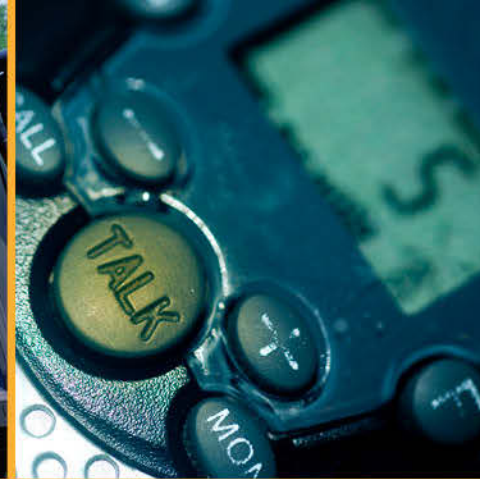
The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (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.



# Award Presentation

---

- Participants Award *Sponsored by NASEMSO*
- Leadership Award *Sponsored by NASEMSO*
- Hertz Award *Sponsored by APCO International*
- Atkinson Technical Award *Sponsored by Jeff Bratcher*
- Life Time Achievement *Sponsored by NENA*
- Chairman's Award *Sponsored by Ralph Haller*
- Richard DeMello Award *Sponsored by IMSA*



# Organizations Update

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.



# TIA Update NPSTC

*Jim Holthaus  
Chair, Private Radio Section (PRS)  
Telecommunications Industry Association*

*Vice President  
RELM Wireless*



# Who is TIA?

- **Trade association**
- **Global information and communications technology (ICT) industry**
  - Standards development
  - Policy initiatives
  - Business opportunities
  - Market intelligence
  - Networking events.
- **Hundreds of member companies**





# TIA “Technology & Standards”

- **Accredited by the American National Standards Institute (ANSI)**
  - Develop voluntary, consensus-based industry standards
- **12 engineering committees**

*TR-8 “Mobile and Personal Private Radio Standards”*

*Formulation of TIA-102 Series standards for Project 25*



# TR-8 Standards Activity

## Completed in 2016:

- **General**  
TIA-102 Documentation Suite Revision C reflects TR8 progress since the last publication (2012), including new TIA publications, improved graphics, and addresses miscellaneous errata identified.

- **Air Interfaces**  
A revision to the FDMA, TDMA and Analog Air Interface Performance Measurement Method Standards *ensure that harmonics present in Class D amplifiers do not interfere with various audio measurements.*

Revisions of the FDMA Conventional Conformance test update the list of reference documents, make general terminology clarifications and provided clarifications on test result expectations without modifying or adding any tests.

- **Broadband**  
A revision of TSB-88.2-E (Wireless Communications Systems – Performance in Noise and Interference Limited Situations – Part 2: Propagation and Noise) adds information associated with Broadband Air Interface Propagation and Noise modeling.





# TR-8 Standards Activity

## Work in Progress:

- **Security**

Link Layer Encryption will provide improved Security for all air interfaces of P25, protects control channel control messages, and hides group and individual IDs.

An addendum to the Key Fill Interface standard will enable Key Fill Device (KVL) interface to a KMF, an Authentication Facility and another Key Fill Device

- **Wireline Interfaces**

An addendum to the ISSI Messages and Procedures Standard corrects several errata that have been noted since the last publication.

A revision to the Fixed Station Interface Standard adds additional capabilities the most significant of which is Packet Data.

Group and Individual Regrouping for the Trunking ISSI/CSSI Standard will enable dispatch equipment connected to Trunking Infrastructures via the ISSI/CSSI to control both group and individual regrouping services.



# TR-8 Standards Activity

## Work in Progress(Continued):

- **Air Interfaces**

A revision to the FDMA Common Air Interface addresses errata that have been collected since the last publication.

A revision to the Trunking Interoperability Test merges the FDMA and TDMA material and address an error in a call pre-emption test procedure.

A new standard for a TDMA Control Channel provides the messages and procedures for operating a 12.5 kHz channel with 2 TDMA slots where either or both may service Control Channel traffic.

An addendum for additional Emergency Alarm 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.

- **Broadband**

Additions to TSB-88 are in progress. These additions will create recommendations for Broadband Data System coverage modeling and verification.



# TIA “Policy”

- **Participate in policy decisions**
  - Impact the communications industry
- **Regulatory issues**
  - Affect member companies
- **Events, Publications and Filings**
- **Committees and Working Groups**

*Wireless Communications Division (WCD)*

*Private Radio Section (PRS)*

# Current Activities

## Policy

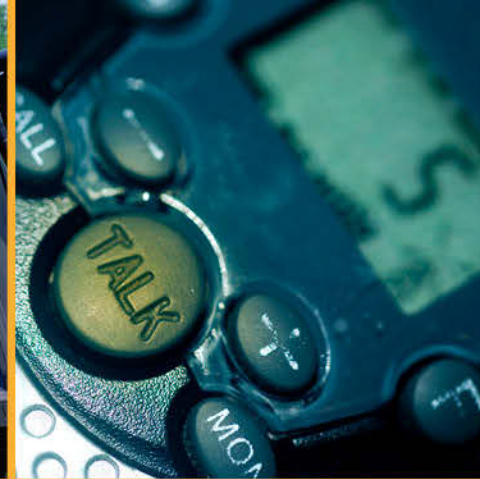
- *Drafting a response to FCC's Order on Reconsideration seeking comments on adoption of the 15 recommended feature sets and capabilities proposed by the P25 CAP AP*
- *Response reinforces TIA's support of P25 CAP and seeks to resolve ambiguities in proposed testing and focus requirements to features necessary for interoperability*
- *TIA Plans to share this response with NPSTC prior to submittal to the Commission.*



# Contact Information

**Jim Holthaus**  
**Chair, Private Radio Section (PRS)**

**Vice President-P25 Solutions**  
**RELM Wireless**  
**[jholthaus@relm.com](mailto:jholthaus@relm.com)**



# NPSTC Strategic Plan

**Lloyd Mitchell, Executive Committee Task Force Chair**  
**Scott Bryant, Scott Bryant and Associates**

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.



# Strategic Plan Discussion

---

- Participant Survey
- Governing Board Member Interviews
- Strategic Planning and Decision Making Session

# Participant Survey

---

- Designed to solicit feedback and input on:
  - Quality of NPSTC products and services
  - Overall satisfaction with NPSTC
  - Willingness to recommend NPSTC to others
  - NPSTC strengths
  - NPSTC challenges or issue areas
  - Changes to improve effectiveness
  - Organizations participating
- Survey will be web-based with email invitations
- Responses will be confidential
- Responses will be compiled and a report developed

# Governing Board Member Perspectives

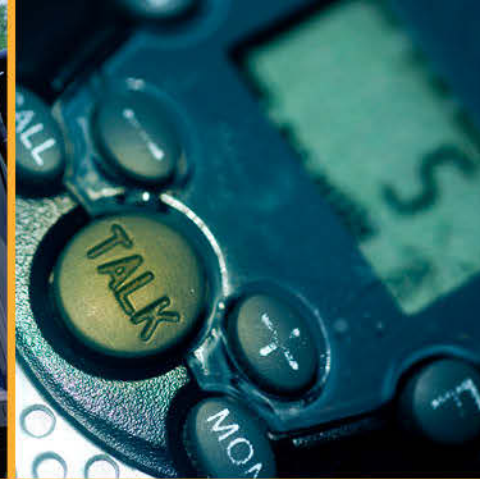
---

- Each Governing Board Member and Alternate will be interviewed over the telephone
- Interview topics include:
  - Key Accomplishments over the past five year
  - Current strengths? (What is working well?)
  - Key challenges (What is not working well?)
  - Future focus (Ideal future visions / future state?)
  - Primary challenges or barriers future visions / future states
  - Most effective strategies / key strategic initiatives
- Results will be compiled and a report developed
- Interviews can include "off the record" information if needed

# Strategic Planning Decision Making

---

- Planned for January Governing Board Meeting
- Review and discuss participant survey results
- Review and discuss Governing Board Member interview results
  - Key NPSTC accomplishments
  - Current NPSTC strengths
  - Current NPSTC challenges
  - Future Focus and Priorities
  - Effective Strategies / Key Strategic Initiatives
- Update NPSTC Strategic Plan roadmap / gameboard



## Executive Level IV Session

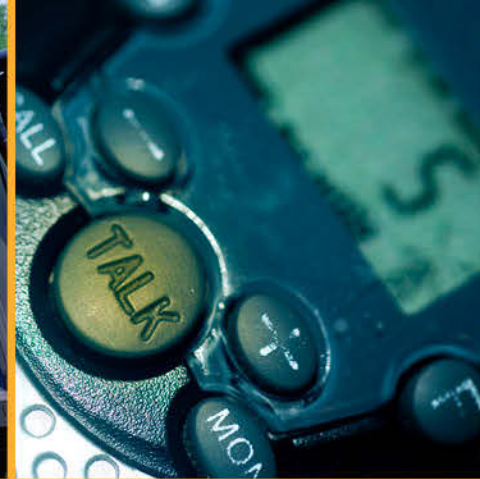
The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC) and the National Protection and Programs Directorate, Office of Emergency Communications (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.

# 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

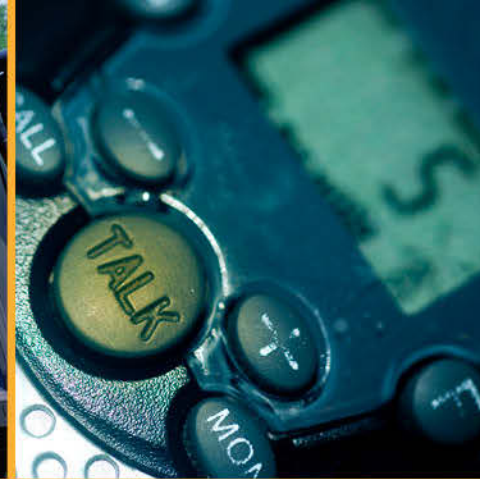




# NPSTC Member Organization Orientation

**Marilyn Ward, Executive Director**  
**September 28, 2016**

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.



# Recess

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.