NPSTC

LMR Encryption | Navigating Recent FCC Rule Changes

Barry H. Luke, Deputy Executive Director

Thursday, April 13, 2017

APCO Western Regional Conference
Ontario, California

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

NPSTC Mission Statement

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

NPSTC

NPSTC Governing Board (Voting Member Organizations)

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
IACP
POLICE
SINCE 1893

NATIONAL SHERIFFS' ASSOCIATION

NATIONAL SHERIFFS' ASSOCIATION

IAFC
INTERNATIONAL FIRE CHIEFS ASSOCIATION
ORG 1873

NASEMSO

APCO International
Leaders in Public Safety Communications

NENA THE 9-1-1 ASSOCIATION
The only organization solely focused on 9-1-1 policy, technology, operations, and education issues.

IAEM
International
Association of
Emergency Managers

IMSA®
Your Partner in PUBLIC SAFETY

ASSOCIATION of
FISH & WILDLIFE
AGENCIES

FCCA

NATIONAL ASSOCIATION OF STATE FORESTERS
FOUNDED 1920

AASHTO

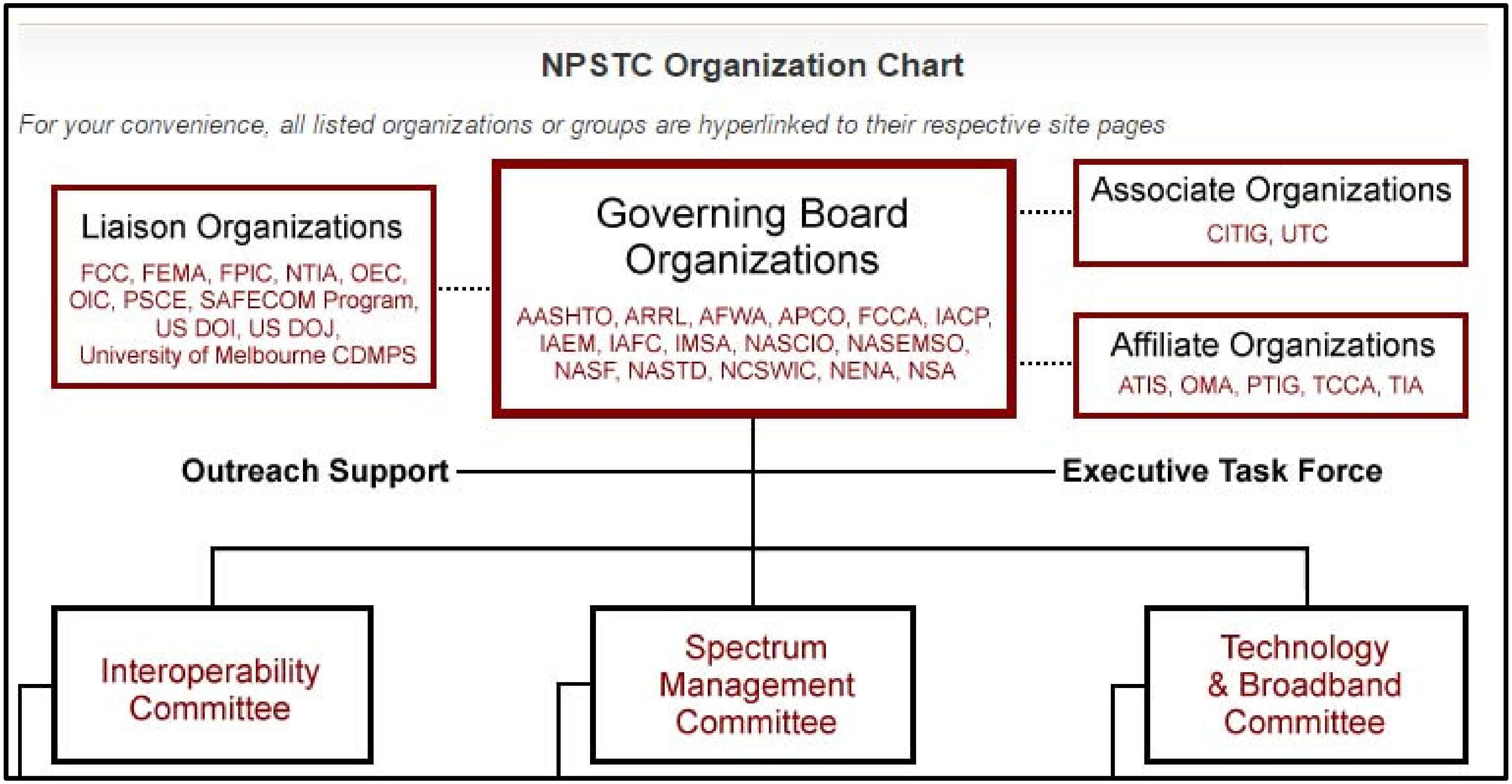
ARRL

NCSWIC

NASTD
National Association of State Technology Directors
Technology Professionals Serving State Government

NASCIO
Representing Chief Information
Officers of the States

NPSTC Organizational Chart



NPSTC Organization Chart

For your convenience, all listed organizations or groups are hyperlinked to their respective site pages

Liaison Organizations
FCC, FEMA, FPIC, NTIA, OEC, OIC, PSCE, SAFECOM Program, US DOI, US DOJ, University of Melbourne CDMPS
Governing Board Organizations
AASHTO, ARRL, AFWA, APCO, FCCA, IACP, IAEM, IAFC, IMSA, NASCIO, NASEMSO, NASF, NASTD, NCSWIC, NENA, NSA
Associate Organizations
CITIG, UTC
Affiliate Organizations
ATIS, OMA, PTIG, TCCA, TIA
Outreach Support
Executive Task Force
Interoperability Committee
Spectrum Management Committee
Technology & Broadband Committee

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

Presentation Overview

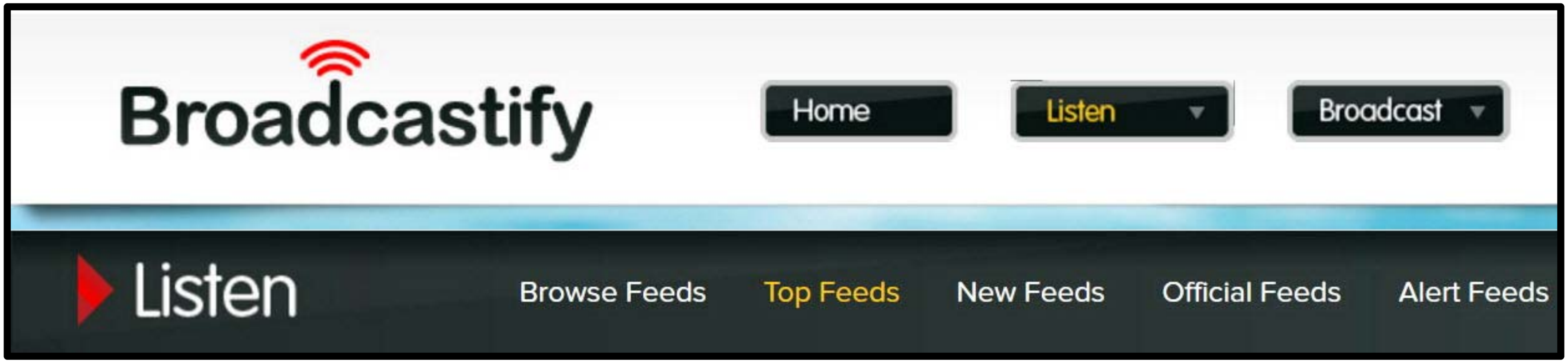
- Why do we use encryption?
- Types of encryption.
- Encryption and Interoperability
- FCC Report and Order #1
- FCC Report and Order #2
- Summary of FCC Impact.
- Options for interoperable encryption.

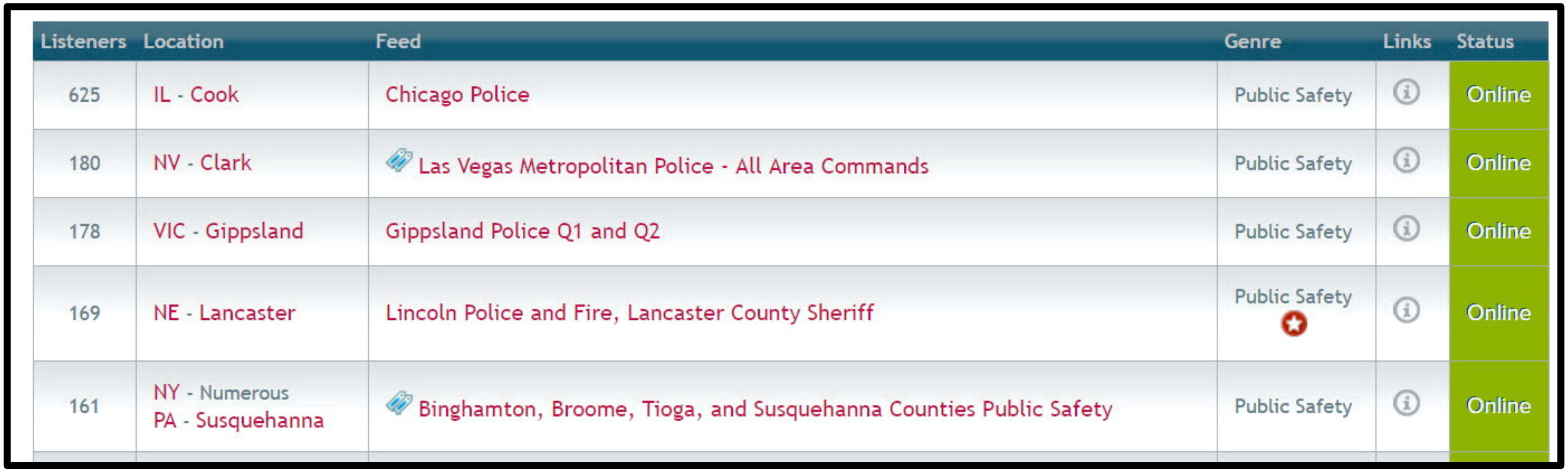
Why do we use encryption?

- Easier monitoring of public safety:
  - Scanners, digital and trunked
  - Web based scanner services
  - Smart Phone app based services

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

How easy is it to listen in?

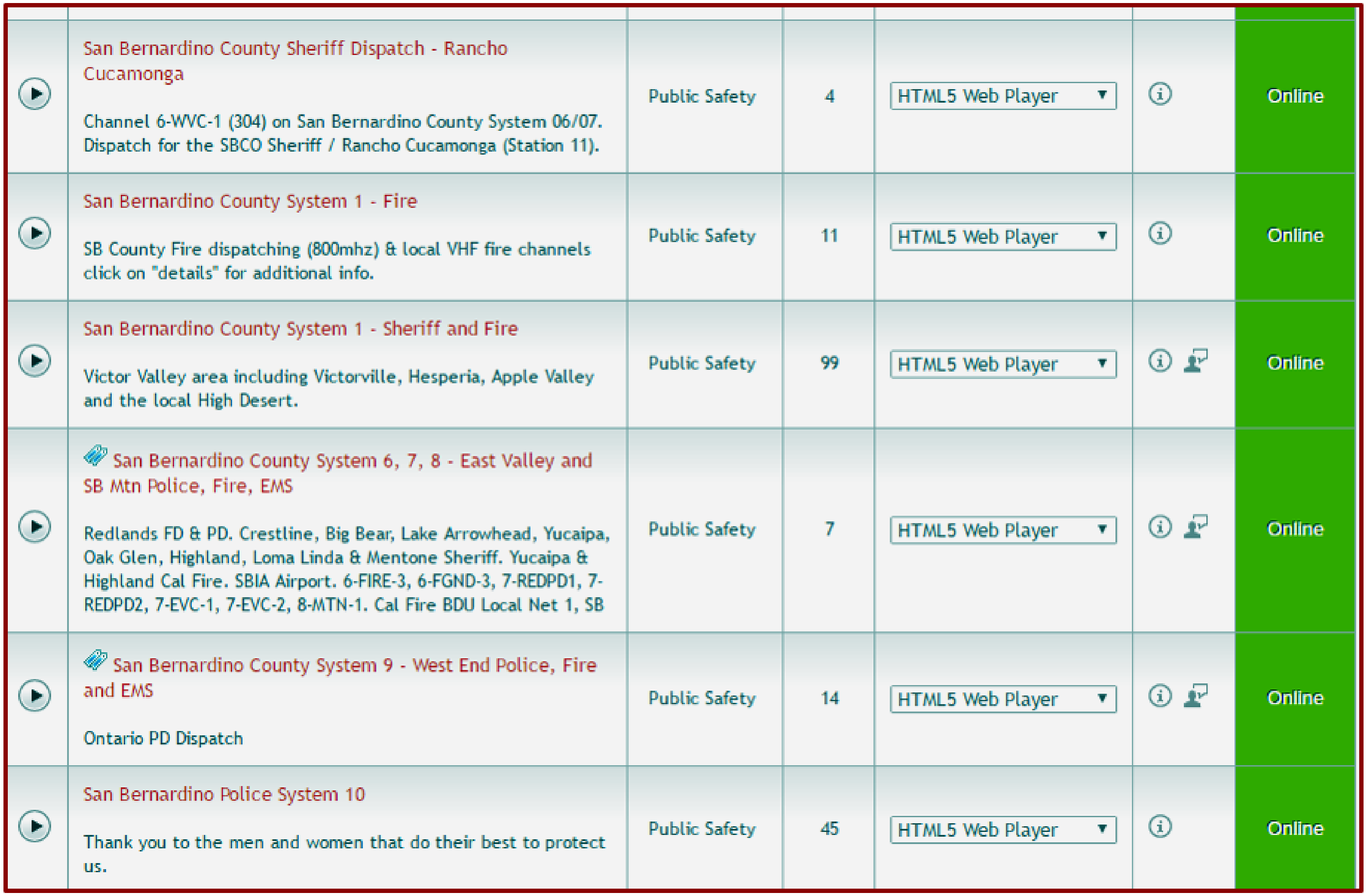




Listeners	Location	Feed	Genre	Links	Status
625	IL - Cook	Chicago Police	Public Safety	ⓘ	Online
180	NV - Clark	Las Vegas Metropolitan Police - All Area Commands	Public Safety	ⓘ	Online
178	VIC - Gippsland	Gippsland Police Q1 and Q2	Public Safety	ⓘ	Online
169	NE - Lancaster	Lincoln Police and Fire, Lancaster County Sheriff	Public Safety	ⓘ	Online
161	NY - Numerous PA - Susquehanna	Binghamton, Broome, Tioga, and Susquehanna Counties Public Safety	Public Safety	ⓘ	Online

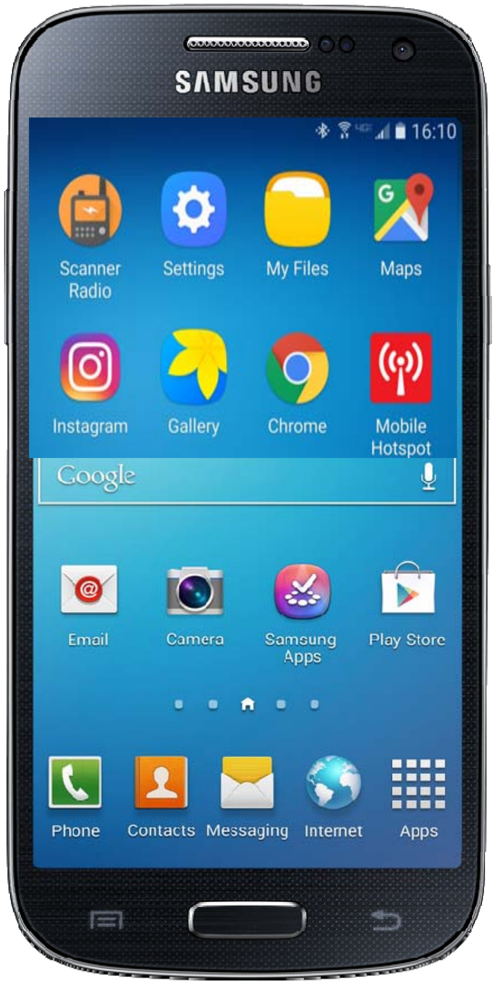
NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

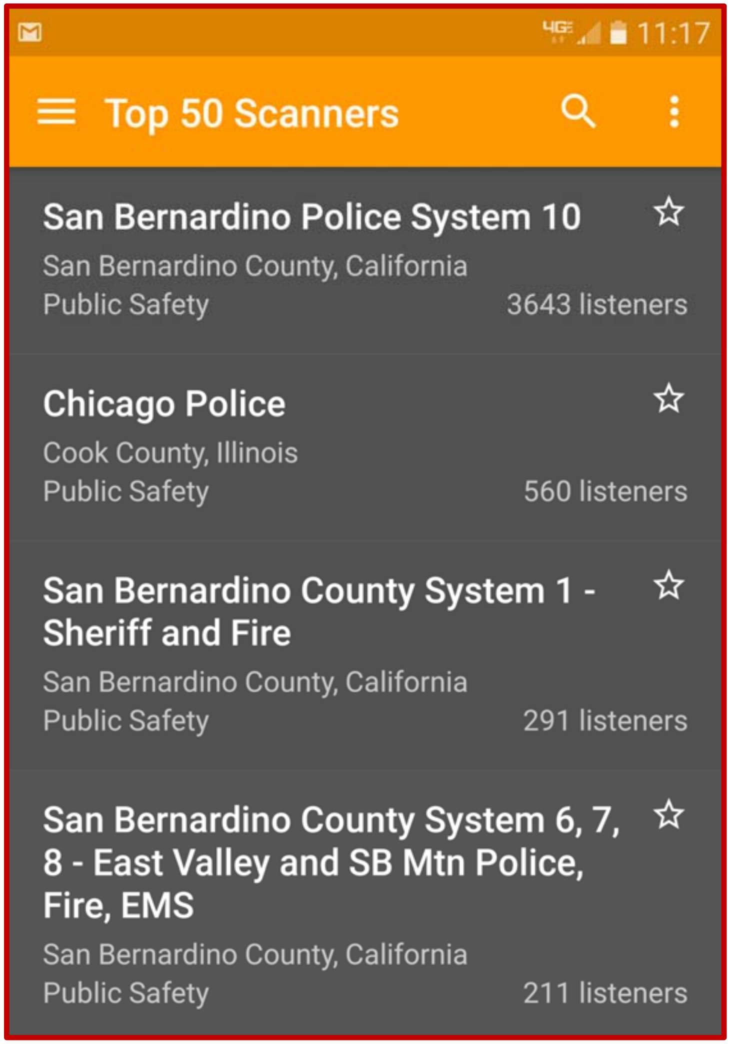
How easy is it to listen in?



▶	San Bernardino County Sheriff Dispatch - Rancho Cucamonga Channel 6-WVC-1 (304) on San Bernardino County System 06/07. Dispatch for the SBCO Sheriff / Rancho Cucamonga (Station 11).	Public Safety	4	HTML5 Web Player ▼	ⓘ	Online
▶	San Bernardino County System 1 - Fire SB County Fire dispatching (800mhz) & local VHF fire channels click on "details" for additional info.	Public Safety	11	HTML5 Web Player ▼	ⓘ	Online
▶	San Bernardino County System 1 - Sheriff and Fire Victor Valley area including Victorville, Hesperia, Apple Valley and the local High Desert.	Public Safety	99	HTML5 Web Player ▼	ⓘ	Online
▶	San Bernardino County System 6, 7, 8 - East Valley and SB Mtn Police, Fire, EMS Redlands FD & PD. Crestline, Big Bear, Lake Arrowhead, Yucaipa, Oak Glen, Highland, Loma Linda & Mentone Sheriff. Yucaipa & Highland Cal Fire. SBIA Airport. 6-FIRE-3, 6-FGND-3, 7-REDPD1, 7-REDPD2, 7-EVC-1, 7-EVC-2, 8-MTN-1. Cal Fire BDU Local Net 1, SB	Public Safety	7	HTML5 Web Player ▼	ⓘ	Online
▶	San Bernardino County System 9 - West End Police, Fire and EMS Ontario PD Dispatch	Public Safety	14	HTML5 Web Player ▼	ⓘ	Online
▶	San Bernardino Police System 10 Thank you to the men and women that do their best to protect us.	Public Safety	45	HTML5 Web Player ▼	ⓘ	Online

How easy is it to listen in?




11:17

Top 50 Scanners

San Bernardino Police System 10
San Bernardino County, California
Public Safety — 3643 listeners

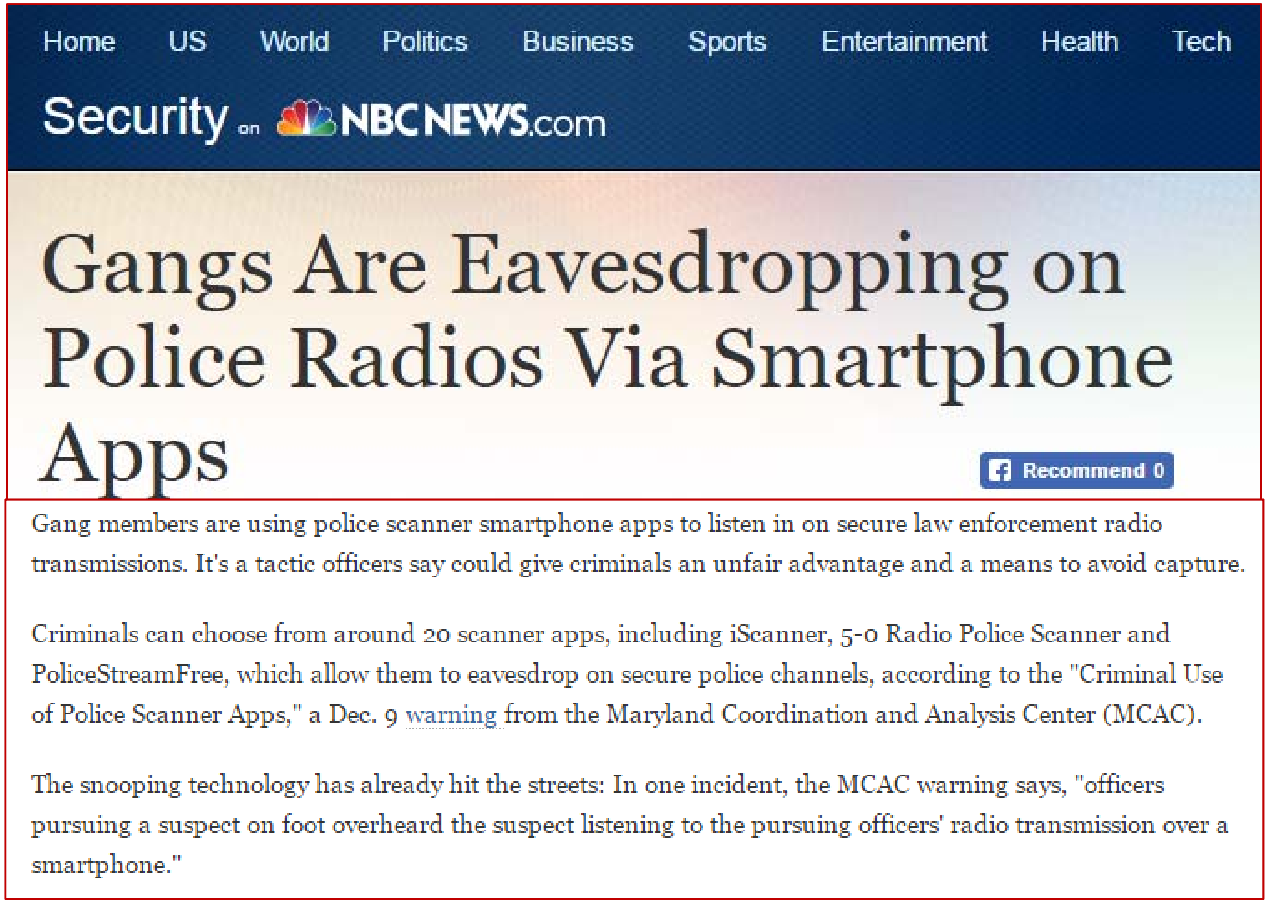
Chicago Police
Cook County, Illinois
Public Safety — 560 listeners

San Bernardino County System 1 - Sheriff and Fire
San Bernardino County, California
Public Safety — 291 listeners

San Bernardino County System 6, 7, 8 - East Valley and SB Mtn Police, Fire, EMS
San Bernardino County, California
Public Safety — 211 listeners

Why do we use encryption?

- Criminals using monitoring technology.



Gangs Are Eavesdropping on Police Radios Via Smartphone Apps

Gang members are using police scanner smartphone apps to listen in on secure law enforcement radio transmissions. It's a tactic officers say could give criminals an unfair advantage and a means to avoid capture.

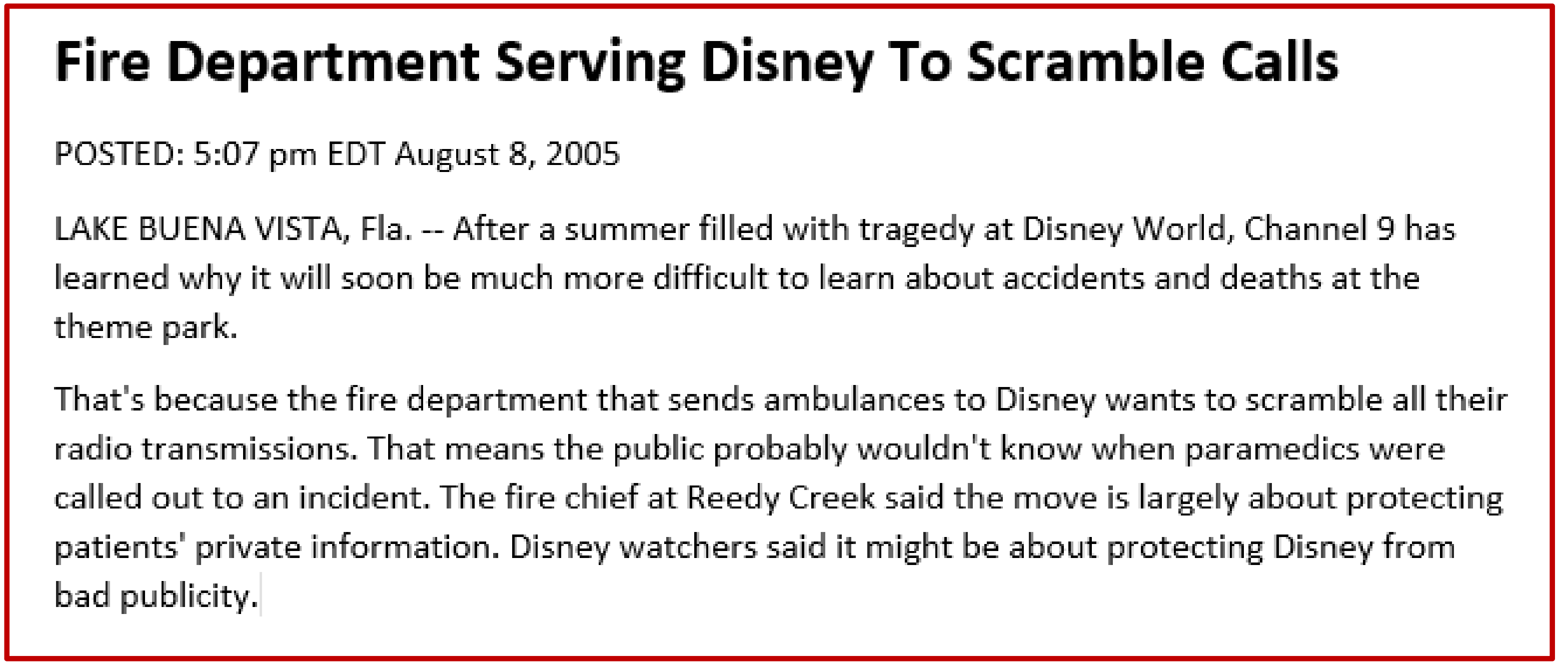
Criminals can choose from around 20 scanner apps, including iScanner, 5-0 Radio Police Scanner and PoliceStreamFree, which allow them to eavesdrop on secure police channels, according to the "Criminal Use of Police Scanner Apps," a Dec. 9 warning from the Maryland Coordination and Analysis Center (MCAC).

The snooping technology has already hit the streets: In one incident, the MCAC warning says, "officers pursuing a suspect on foot overheard the suspect listening to the pursuing officers' radio transmission over a smartphone."

Why do we use encryption?

- Law Enforcement agencies need secure communications.
  - Initially with SRT/SWAT.
  - Daily Use is becoming more common.
- Fire and EMS agencies are becoming interested in encryption for privacy.

Why do we use encryption?



Fire Department Serving Disney To Scramble Calls

POSTED: 5:07 pm EDT August 8, 2005

LAKE BUENA VISTA, Fla. -- After a summer filled with tragedy at Disney World, Channel 9 has learned why it will soon be much more difficult to learn about accidents and deaths at the theme park.

That's because the fire department that sends ambulances to Disney wants to scramble all their radio transmissions. That means the public probably wouldn't know when paramedics were called out to an incident. The fire chief at Reedy Creek said the move is largely about protecting patients' private information. Disney watchers said it might be about protecting Disney from bad publicity.

Encryption Explained

- Voice and data messages are converted from their normal “clear” format into an encrypted message containing cipher text using algorithms (also called a “key”).
  - Key strength is based on the number of “bits” involved in the algorithm.
  - Encryption solutions range from 40-256 bits.

Encryption Explained

- The encrypted message is transmitted to it's destination.
- An authorized receiver of the message has a "key" that reconstructs the voice or data message back into normal message format.
- An unauthorized user may receive the message, but will not be able to use it.

Encryption Explained

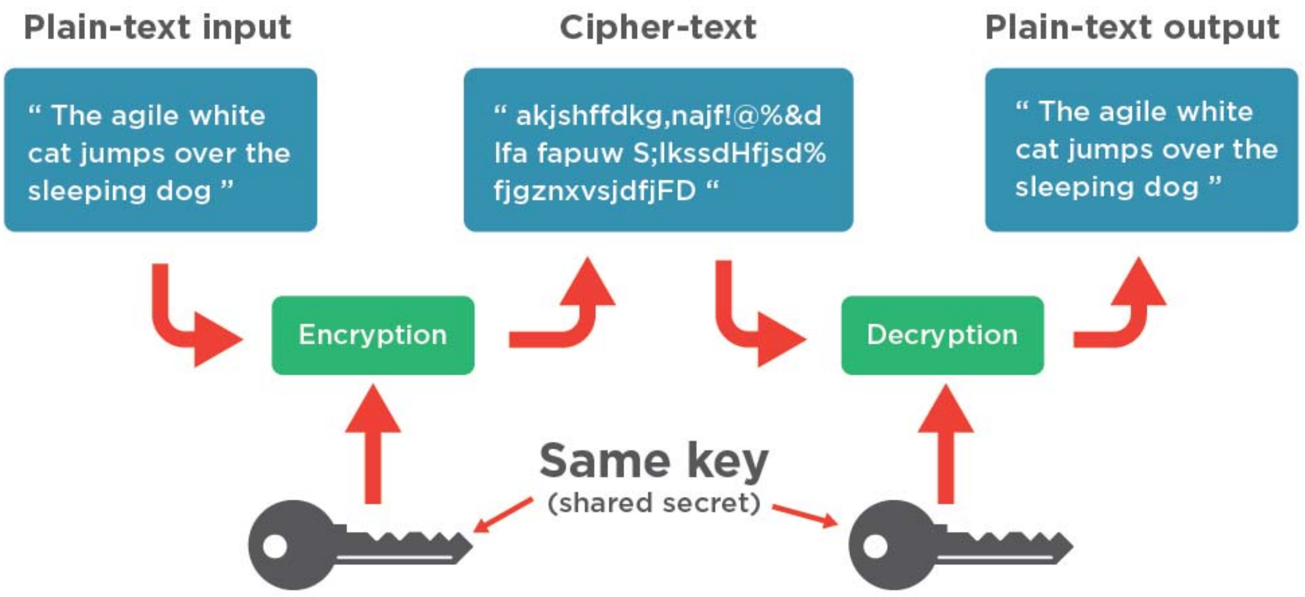

Plain-text input
“ The agile white cat jumps over the sleeping dog ”
Cipher-text
“ akjshffdkg,najf!@%&d lfa fapuw S;lkssdHfjsd% fjgznxvsjdfjFD “
Plain-text output
“ The agile white cat jumps over the sleeping dog ”
Encryption
Decryption
Same key
(shared secret)

Figure 1: Symmetric Block Cipher

Encryption Explained

- Both the message “sender” and “receiver” must use the same:
  - Encryption Algorithm
  - Encryption Key
- Subscriber equipment must be configured using the same parameters:
  - Key ID (KID)
  - Traffic Encryption Key (TEK)
  - Storage Location Number (SLN)
  - Algorithm ID (ALGID)

Types of Encryption

- Analog Voice Inversion Scrambling
  - Vintage technology
  - “Donald Duck” sounding transmissions
  - Not considered “encryption”

Types of Encryption

- Digital Encryption
  - In the U.S. there are four general “types” of encryption algorithms:
    - **Type 1** is for U.S. classified material (national security).
    - **Type 2** is for general U.S federal interagency security.
    - **Type 3** is interoperable interagency security between U.S. federal, state and local agencies.
    - **Type 4** is for proprietary solutions.

Types of Encryption

- Digital Encryption
  - Vendor Proprietary
    - Motorola (ADP)
    - Harris (ARC4)
  - Standards based
    - NIST issues Federal Information Processing Standard (FIPS) requirements.
    - Data Encryption Standard (DES) 64 bit.
    - Advanced Encryption Standard 256 (AES256).

Encryption and Grant Funds

- Changes to Encryption Requirements.
  - P25 Compliance Assessment Program (CAP) Advisory Panel (P25 CAP AP) reviewed current industry practices and the impact on interoperability.
  - DHS OIC issued a revised requirement on March 26, 2017.
    - AES256 encryption must be included in any radio shipped with an encryption solution.
    - Affects radio purchases made with federal grant dollars.
    - Impacts vendor equipment listings on the P25 Compliance Assessment Bulletins.

Encryption and Interoperability

- There are documented problems with the use of encryption by public safety agencies.
- Problems within a single public safety agency:
  - Training (field user and PSAP)
  - Key Management
  - Key Updates
    - OTR
    - Manual

Encryption and Interoperability

- There are documented problems when encryption is attempted during multi-agency incidents.
  - Agency encryption compatibility.
    - Same or different encryption type.
    - Use of common/shared key.
  - Management of Common/Shared Encryption Keys.
    - Key Refresh.

Encryption and Interoperability

- Awareness
  - When Encryption is not Encryption
    - Switching channels/talkgroups
    - Console Patching
    - Gateway Patching
- Using encryption solutions take agency commitment and effort.
  - There are many success stories involving agencies who have implemented encryption.

NPSTC Survey on Encryption

- NPSTC issued a survey in May of 2016.
  - Concern over reported problems with use of encryption.
  - Concern over discussions advancing the need to encrypt Interoperability channels.
  - Survey was designed to determine if public safety agencies were using encryption of nationwide designated interoperability channels.

NPSTC Survey on Encryption

1) Does your agency currently use encryption on any of the FCC-designated nationwide interoperability channels?
2) If yes, how have you ensured interoperability on these channels in your area or region?
3) Also, please explain how you plan to implement the new FCC rule or what, if any, issues this rule raises for you.

NPSTC Survey

- 42 responses were received.
- 39 of the respondents were from local and state agencies geographically located across 21 states.
- No agency reported using encryption on nationwide I/O channels.
  - NPSTC is aware of some agencies who use encryption on the direct mode/simplex side in 700 and 800 MHz frequency bands.

FCC Report and Orders - 2016

- On April 25, 2016, the FCC released Report and Order, PS Docket No. 13-209.
  - Analog Voice Operations
- On August 23, 2016, the FCC issued Report and Order, PS Docket No. 15-199, revising Section 90.20(i).
  - Railroad Police Eligibility

FCC Report and Order #1

- On April 25, 2016, the FCC released Report and Order, PS Docket No. 13-209.
  - Responding to an inquiry by Harris Corporation regarding use of Digital Emission Mask “H”.
  - This was an issue with the introduction of TETRA radio technology into FCC rules.
  - The Report and Order discussion was never about encryption.
  - The FCC confirmed that analog FM was required for interoperability, noting that some TETRA radios did not have analog capability.

FCC Report and Order #1

- On April 25, 2016, the FCC released Report and Order, PS Docket No. 13-209.
  - FCC modified its rules to require the use of analog FM as the common modulation scheme for mobiles and portables operating on the designated public safety nationwide interoperability channels in the VHF, UHF, and 800 MHz bands.
  - The FCC decision is specific to the designated nationwide public safety nationwide interoperability Calling and Tactical channels.
  - Since the 700 MHz is digital only, it was not addressed in this order.

FCC Report and Order #1

- This FCC order does not mention "encryption".
  - However, the mandate for analog operations prevents the use of digital encryption.
  - Voice inversion scrambling is not digital and is not considered encryption; so technically it is allowed.

FCC Report and Order #2

- On August 23, 2016, the FCC issued Report and Order, PS Docket No. 15-199, revising Section 90.20(i).
- This R&O was to authorize railroad police departments to access nationwide interoperability channels.
- This order included an appendix of nationwide interoperability channels, using the DHS NIFOG Guide.
  - An expanded list of channels was included.

FCC Report and Order #2

- This FCC decision prohibited encryption on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz, and 700 MHz bands.
- Also includes language about the use of encryption on tactical channels with advance coordination.
  - This was later determined to be in conflict with the earlier FCC order.

FCC Report and Order Summary

- Encryption may not be used on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz, and 700 MHz bands.
  - VCALL10
  - UCALL40
  - 8CALL90
  - 7CALL50, 7CALL70

FCC Report and Order Summary

- Encryption may not be used on designated tactical channels in VHF, UHF and 800.
  - VTAC (VTAC11-14) & (VTAC33-38)
  - UTAC (UTAC41-43)
  - 8TAC (8TAC91-94)

Encrypted Interoperability Options

- FCC Order does not apply to certain channels, where encryption may be used:
  - Mutual Aid Channels:
    - VFIRE, VMED, VLAW
    - UHF MED frequencies
  - 700 MHz Tactical Channels
    - 7LAW, 7FIRE, 7TAC, 7MED,
    - 700 MHz Air to Ground channels

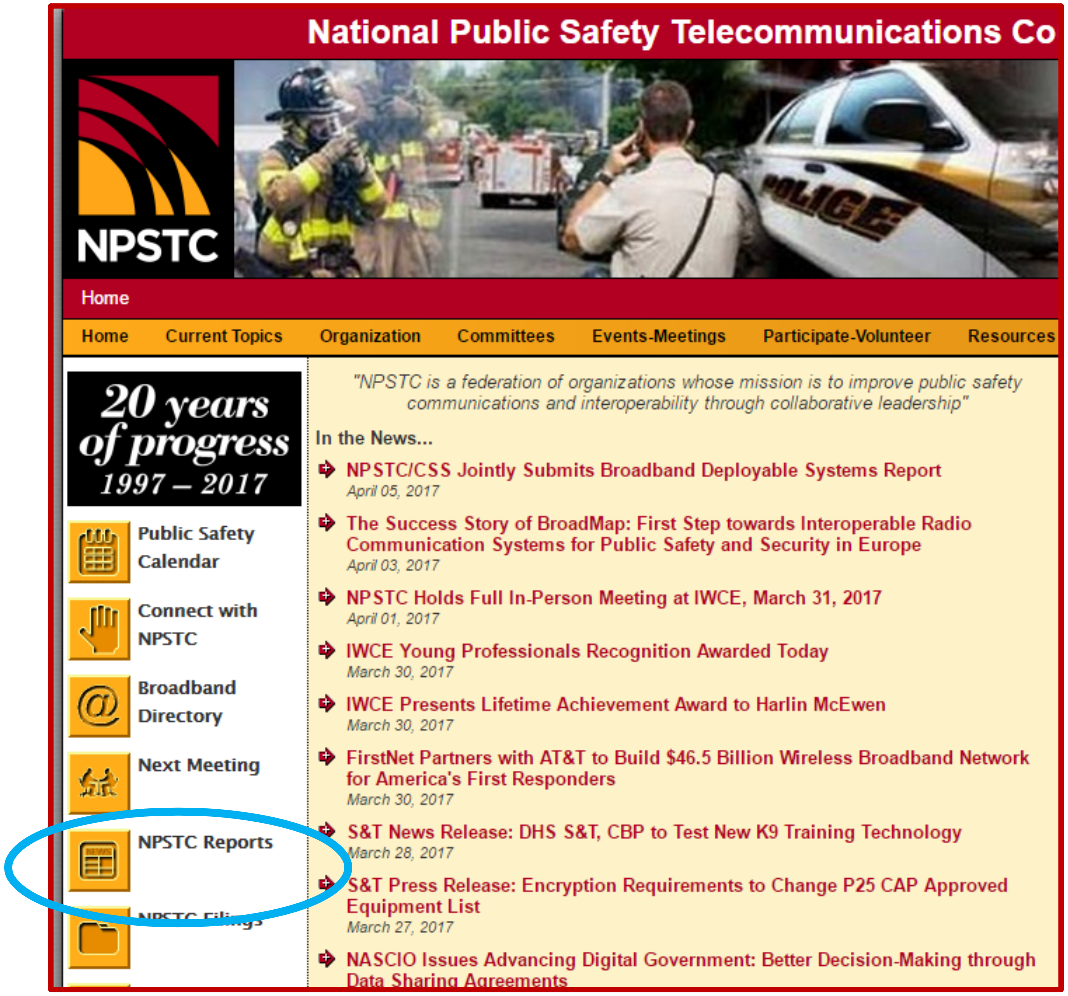
Encrypted Interoperability Options

- FCC Order does not apply to certain channels, where encryption may be used:
  - NTIA designated channels
    - IR and LE
  - State, Regional, and Local Interoperability channels and talkgroups
    - If allowed by SIEC/Local Authority

Encryption Best Practices

- The U.S. Department of Homeland Security has published several documents to support effective implementation of encryption:
  - Guidelines for Encryption in Land Mobile Radio Systems (February 2016),
  - Considerations for Encryption in Public Safety Radio Systems (September 2016)
  - Best Practices for Encryption in P25 Public Safety Land Mobile radio Systems (September 2016)
  - All Reports are located on the DHS website:
    - http://www.dhs.gov/technology

NPSTC Outreach Report on Encryption and Interoperability



National Public Safety Telecommunications Co

NPSTC

Home

Home | Current Topics | Organization | Committees | Events-Meetings | Participate-Volunteer | Resources

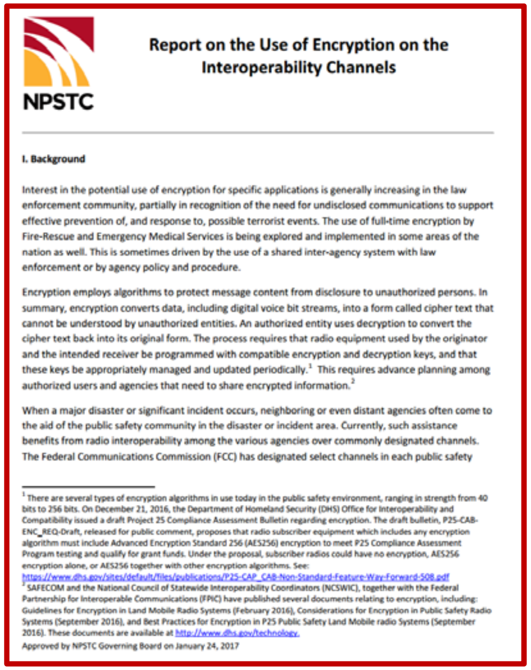
20 years of progress 1997 – 2017

- Public Safety Calendar
- Connect with NPSTC
- Broadband Directory
- Next Meeting
- NPSTC Reports
- NPSTC Filings

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

In the News...

- NPSTC/CSS Jointly Submits Broadband Deployable Systems Report
  April 05, 2017
- The Success Story of BroadMap: First Step towards Interoperable Radio Communication Systems for Public Safety and Security in Europe
  April 03, 2017
- NPSTC Holds Full In-Person Meeting at IWCE, March 31, 2017
  April 01, 2017
- IWCE Young Professionals Recognition Awarded Today
  March 30, 2017
- IWCE Presents Lifetime Achievement Award to Harlin McEwen
  March 30, 2017
- FirstNet Partners with AT&T to Build $46.5 Billion Wireless Broadband Network for America's First Responders
  March 30, 2017
- S&T News Release: DHS S&T, CBP to Test New K9 Training Technology
  March 28, 2017
- S&T Press Release: Encryption Requirements to Change P25 CAP Approved Equipment List
  March 27, 2017
- NASCIO Issues Advancing Digital Government: Better Decision-Making through Data Sharing Agreements



NPSTC

Report on the Use of Encryption on the Interoperability Channels

I. Background

Interest in the potential use of encryption for specific applications is generally increasing in the law enforcement community, partially in recognition of the need for undisclosed communications to support effective prevention of, and response to, possible terrorist events. The use of full-time encryption by Fire-Rescue and Emergency Medical Services is being explored and implemented in some areas of the nation as well. This is sometimes driven by the use of a shared inter-agency system with law enforcement or by agency policy and procedure.

Encryption employs algorithms to protect message content from disclosure to unauthorized persons. In summary, encryption converts data, including digital voice bit streams, into a form called cipher text that cannot be understood by unauthorized entities. An authorized entity uses decryption to convert the cipher text back into its original form. The process requires that radio equipment used by the originator and the intended receiver be programmed with compatible encryption and decryption keys, and that these keys be appropriately managed and updated periodically.[1] This requires advance planning among authorized users and agencies that need to share encrypted information.[2]

When a major disaster or significant incident occurs, neighboring or even distant agencies often come to the aid of the public safety community in the disaster or incident area. Currently, such assistance benefits from radio interoperability among the various agencies over commonly designated channels. The Federal Communications Commission (FCC) has designated select channels in each public safety

[1] There are several types of encryption algorithms in use today in the public safety environment, ranging in strength from 40 bits to 256 bits. On December 21, 2016, the Department of Homeland Security (DHS) Office for Interoperability and Compatibility issued a draft Project 25 Compliance Assessment Bulletin regarding encryption. The draft bulletin, P25-CAB-ENC_REQ-Draft, released for public comment, proposes that radio subscriber equipment which includes any encryption algorithm must include Advanced Encryption Standard 256 (AES256) encryption to meet P25 Compliance Assessment Program testing and qualify for grant funds. Under the proposal, subscriber radios could have no encryption, AES256 encryption alone, or AES256 together with other encryption algorithms. See: https://www.dhs.gov/sites/default/files/publications/P25-CAP_CAB-Non-Standard-Feature-Way-Forward-508.pdf

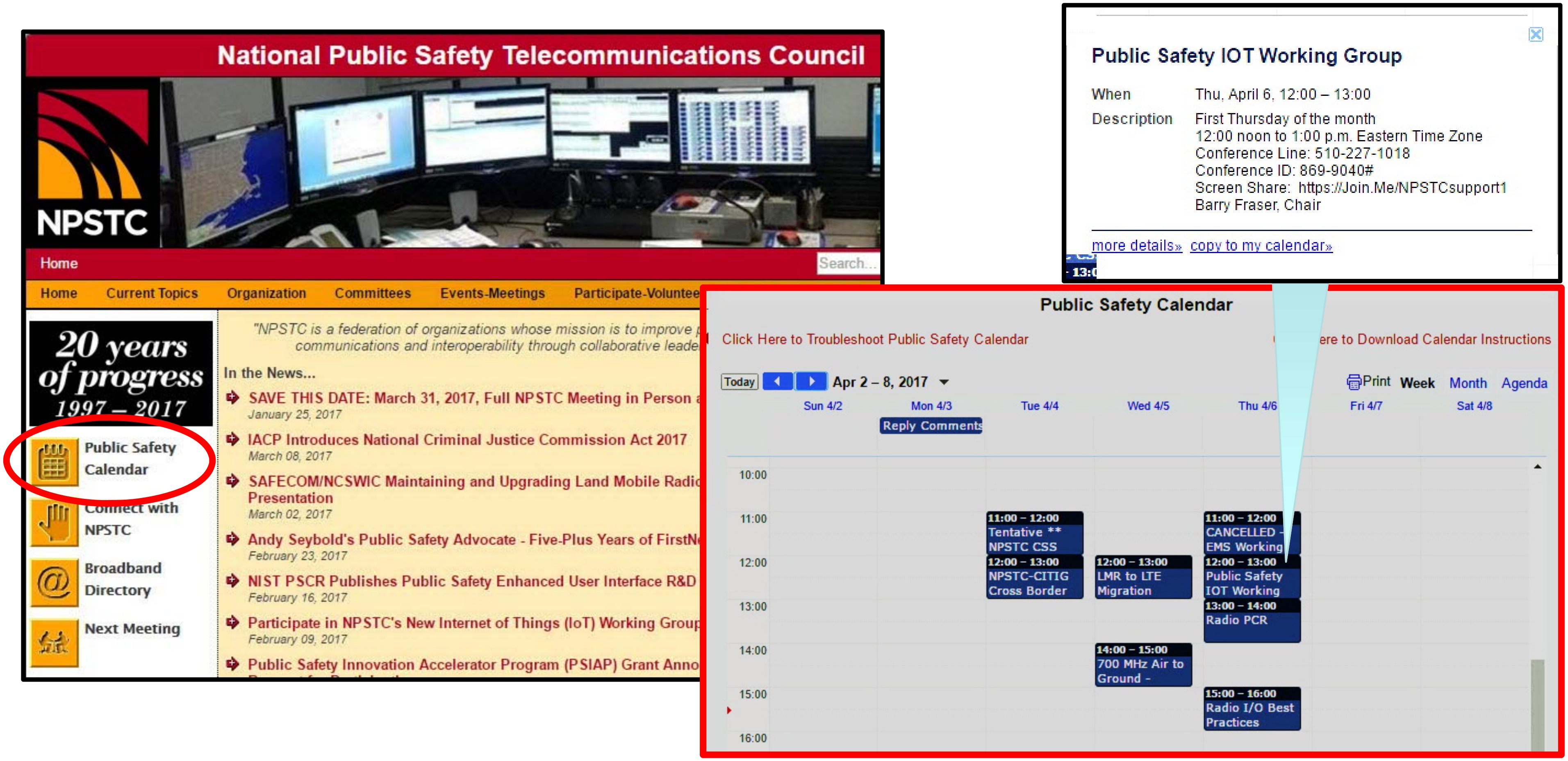
[2] SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), together with the Federal Partnership for Interoperable Communications (FPIC) have published several documents relating to encryption, including: Guidelines for Encryption in Land Mobile Radio Systems (February 2016), Considerations for Encryption in Public Safety Radio Systems (September 2016), and Best Practices for Encryption in P25 Public Safety Land Mobile radio Systems (September 2016). These documents are available at http://www.dhs.gov/technology.

Approved by NPSTC Governing Board on January 24, 2017

How To Get Involved

www.npstc.org

NPSTC Website and Calendar



National Public Safety Telecommunications Council

"NPSTC is a federation of organizations whose mission is to improve p communications and interoperability through collaborative leade

In the News...

- SAVE THIS DATE: March 31, 2017, Full NPSTC Meeting in Person a
  January 25, 2017
- IACP Introduces National Criminal Justice Commission Act 2017
  March 08, 2017
- SAFECOM/NCSWIC Maintaining and Upgrading Land Mobile Radio Presentation
  March 02, 2017
- Andy Seybold's Public Safety Advocate - Five-Plus Years of FirstN
  February 23, 2017
- NIST PSCR Publishes Public Safety Enhanced User Interface R&D
  February 16, 2017
- Participate in NPSTC's New Internet of Things (IoT) Working Group
  February 09, 2017
- Public Safety Innovation Accelerator Program (PSIAP) Grant Anno

Public Safety IOT Working Group

When Thu, April 6, 12:00 – 13:00

Description First Thursday of the month
12:00 noon to 1:00 p.m. Eastern Time Zone
Conference Line: 510-227-1018
Conference ID: 869-9040#
Screen Share: https://Join.Me/NPSTCsupport1
Barry Fraser, Chair

more details» copy to my calendar»

Public Safety Calendar

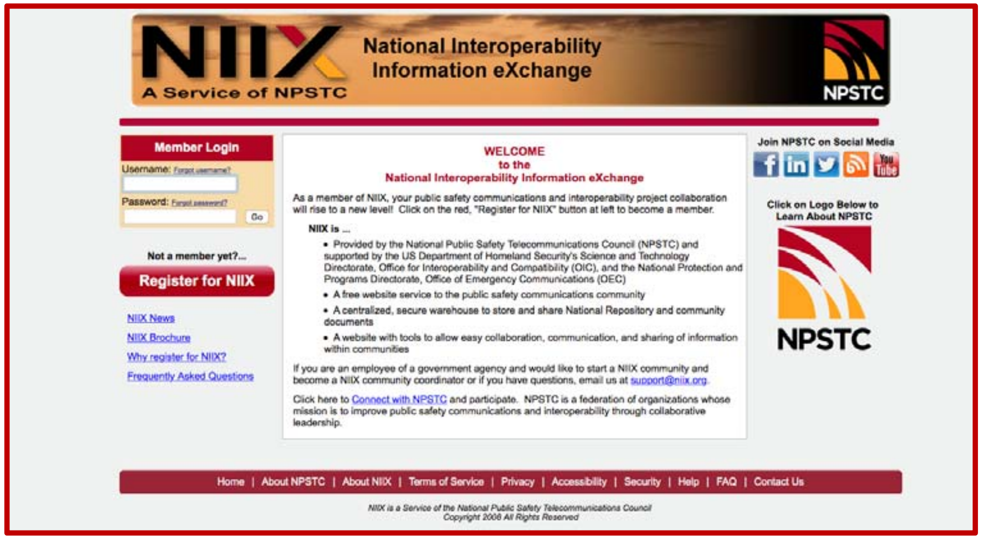
Click Here to Troubleshoot Public Safety Calendar ere to Download Calendar Instructions

- Tue 4/4: 11:00 – 12:00 Tentative ** NPSTC CSS
- Tue 4/4: 12:00 – 13:00 NPSTC-CITIG Cross Border
- Wed 4/5: 12:00 – 13:00 LMR to LTE Migration
- Wed 4/5: 14:00 – 15:00 700 MHz Air to Ground -
- Thu 4/6: 11:00 – 12:00 CANCELLED - EMS Working
- Thu 4/6: 12:00 – 13:00 Public Safety IOT Working
- Thu 4/6: 13:00 – 14:00 Radio PCR
- Thu 4/6: 15:00 – 16:00 Radio I/O Best Practices

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

National Interoperability Exchange (NIIX)

- NIIX
  - A free centralized, secure warehouse to store and share National Repository and community documents.
  - A website with tools to allow easy collaboration, communication, and sharing of information within communities.
  - Locally controlled.



NIIX
National Interoperability Information eXchange
A Service of NPSTC
NPSTC
Member Login
Username: Forgot username?
Password: Forgot password?
Go
Not a member yet?...
Register for NIIX
NIIX News
NIIX Brochure
Why register for NIIX?
Frequently Asked Questions
Join NPSTC on Social Media
Click on Logo Below to Learn About NPSTC
NPSTC
Home | About NPSTC | About NIIX | Terms of Service | Privacy | Accessibility | Security | Help | FAQ | Contact Us

WELCOME
to the
National Interoperability Information eXchange

As a member of NIIX, your public safety communications and interoperability project collaboration will rise to a new level! Click on the red, "Register for NIIX" button at left to become a member.

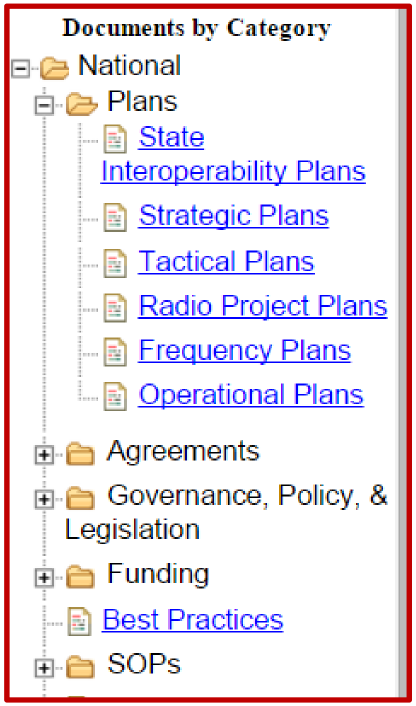
NIIX is ...

- Provided by the National Public Safety Telecommunications Council (NPSTC) and supported by the US 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)
- A free website service to the public safety communications community
- A centralized, secure warehouse to store and share National Repository and community documents
- A website with tools to allow easy collaboration, communication, and sharing of information within communities

If you are an employee of a government agency and would like to start a NIIX community and become a NIIX community coordinator or if you have questions, email us at support@niix.org.

Click here to Connect with NPSTC and participate. NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

NIIX is a Service of the National Public Safety Telecommunications Council
Copyright 2008 All Rights Reserved

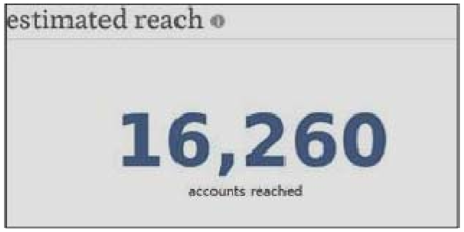


Documents by Category

- National
  - Plans
    - State Interoperability Plans
    - Strategic Plans
    - Tactical Plans
    - Radio Project Plans
    - Frequency Plans
    - Operational Plans
  - Agreements
  - Governance, Policy, & Legislation
  - Funding
  - Best Practices
  - SOPs

Social Media Outreach

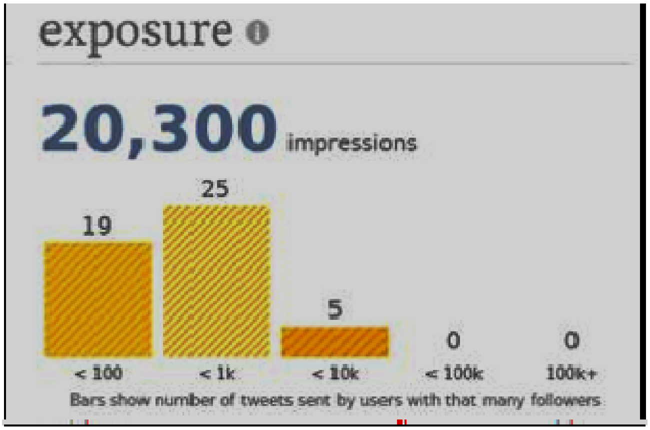
- Outreach and Distribution
  - Constant Contact
  - NPSTC Web Site
  - NPSTC Blog
  - Linked-In
  - Facebook
  - Twitter
  - Coordinate with industry and member publications
  - Broadband Directory



estimated reach

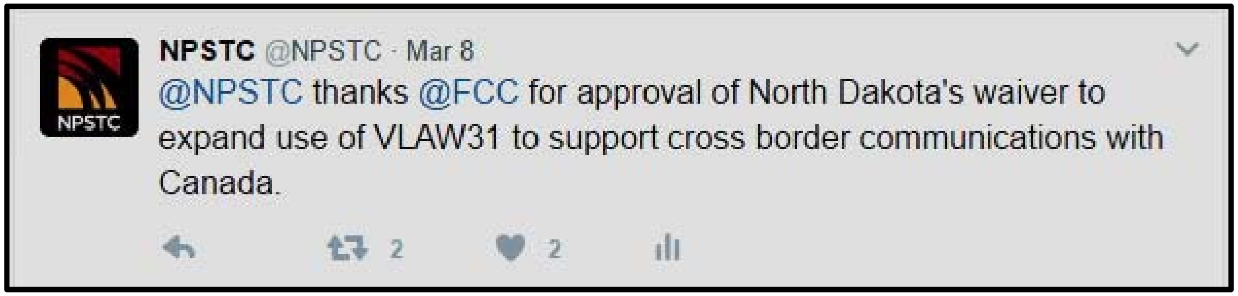
16,260

accounts reached



exposure

20,300 impressions

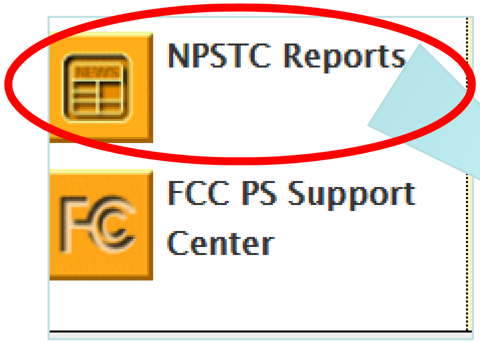


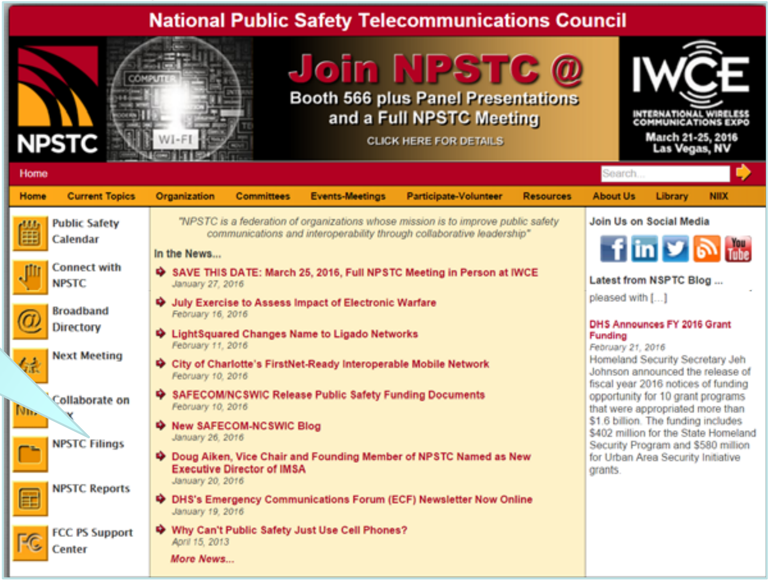
NPSTC @NPSTC · Mar 8

@NPSTC thanks @FCC for approval of North Dakota's waiver to expand use of VLAW31 to support cross border communications with Canada.

Reports Available for Review

- Reports located on NPSTC website, *www.npstc.org*
  - Launch SOR Qualitative
  - Mission Critical Voice Over LTE
  - Local Control Definitions
  - Priority and Quality of Service
  - Push to Talk Requirements for Public Safety
  - FirstNet Web Status Page
  - EMS Telemedicine Report





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

In the News...

- SAVE THIS DATE: March 25, 2016, Full NPSTC Meeting in Person at IWCE
  January 27, 2016
- July Exercise to Assess Impact of Electronic Warfare
  February 16, 2016
- LightSquared Changes Name to Ligado Networks
  February 11, 2016
- City of Charlotte's FirstNet-Ready Interoperable Mobile Network
  February 10, 2016
- SAFECOM/NCSWIC Release Public Safety Funding Documents
  February 10, 2016
- New SAFECOM-NCSWIC Blog
  January 26, 2016
- Doug Aiken, Vice Chair and Founding Member of NPSTC Named as New Executive Director of IMSA
  January 20, 2016
- DHS's Emergency Communications Forum (ECF) Newsletter Now Online
  January 19, 2016
- Why Can't Public Safety Just Use Cell Phones?
  April 15, 2013

More News...

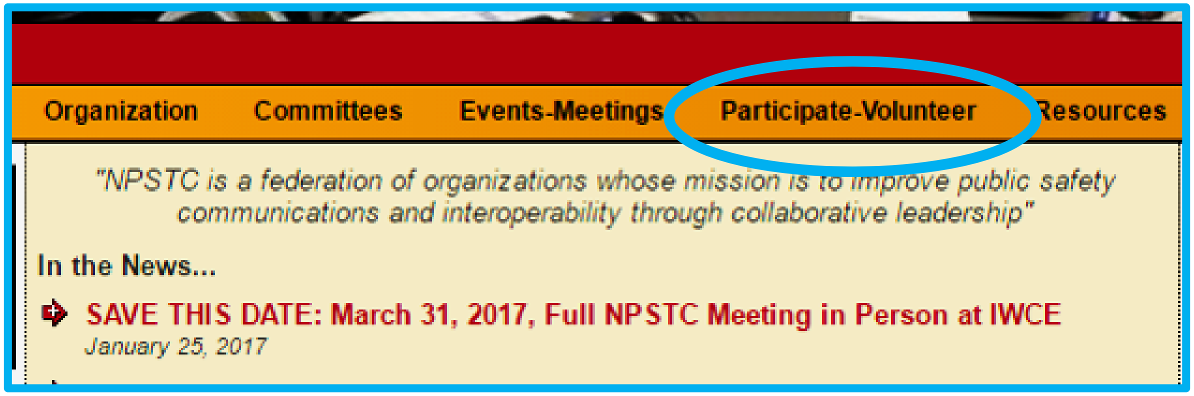
Latest from NSPTC Blog ...

pleased with [...]

DHS Announces FY 2016 Grant Funding
February 21, 2016
Homeland Security Secretary Jeh Johnson announced the release of fiscal year 2016 notices of funding opportunity for 10 grant programs that were appropriated more than $1.6 billion. The funding includes $402 million for the State Homeland Security Program and $580 million for Urban Area Security Initiative grants.

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

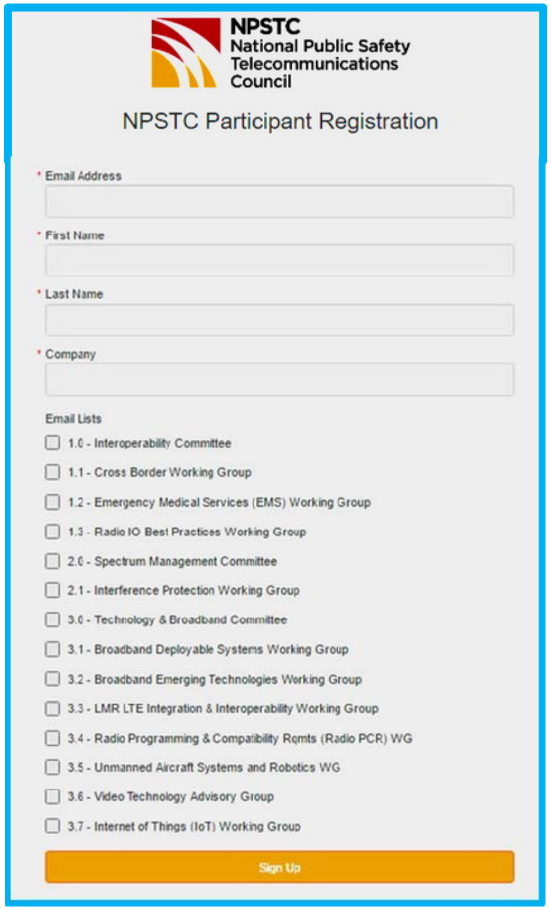
NPSTC Participation Sign Up



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

In the News...

SAVE THIS DATE: March 31, 2017, Full NPSTC Meeting in Person at IWCE
January 25, 2017



NPSTC Participant Registration

* Email Address

* First Name

* Last Name

* Company

Email Lists

- □ 1.0 - Interoperability Committee
- □ 1.1 - Cross Border Working Group
- □ 1.2 - Emergency Medical Services (EMS) Working Group
- □ 1.3 - Radio IO Best Practices Working Group
- □ 2.0 - Spectrum Management Committee
- □ 2.1 - Interference Protection Working Group
- □ 3.0 - Technology & Broadband Committee
- □ 3.1 - Broadband Deployable Systems Working Group
- □ 3.2 - Broadband Emerging Technologies Working Group
- □ 3.3 - LMR LTE Integration & Interoperability Working Group
- □ 3.4 - Radio Programming & Compatibility Rqmts (Radio PCR) WG
- □ 3.5 - Unmanned Aircraft Systems and Robotics WG
- □ 3.6 - Video Technology Advisory Group
- □ 3.7 - Internet of Things (IoT) Working Group

NPSTC

Thank You

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.