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 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
How easy is it to listen in?

Broadcastify

<table>
<thead>
<tr>
<th>Listeners</th>
<th>Location</th>
<th>Feed</th>
<th>Genre</th>
<th>Links</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>625</td>
<td>IL - Cook</td>
<td>Chicago Police</td>
<td>Public Safety</td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>180</td>
<td>NV - Clark</td>
<td>Las Vegas Metropolitan Police - All Area Commands</td>
<td>Public Safety</td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>178</td>
<td>VIC - Gippsland</td>
<td>Gippsland Police Q1 and Q2</td>
<td>Public Safety</td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>169</td>
<td>NE - Lancaster</td>
<td>Lincoln Police and Fire, Lancaster County Sheriff</td>
<td>Public Safety</td>
<td></td>
<td>Online</td>
</tr>
<tr>
<td>161</td>
<td>NY - Numerous PA - Susquehanna</td>
<td>Binghamton, Broome, Tioga, and Susquehanna Counties Public Safety</td>
<td>Public Safety</td>
<td></td>
<td>Online</td>
</tr>
</tbody>
</table>
How easy is it to listen in?

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Type</th>
<th>Channel</th>
<th>Location</th>
<th>Audio Player</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Bernardino County Sheriff Dispatch - Rancho Cucamonga</td>
<td>Public Safety</td>
<td>4</td>
<td>Channel 6-WVC-1 (104) on San Bernardino County System 06/07. Dispatch for the SBCO Sheriff / Rancho Cucamonga (Station 11).</td>
<td>HTML5 Web Player</td>
</tr>
<tr>
<td>San Bernardino County System 1 - Fire</td>
<td>Public Safety</td>
<td>11</td>
<td>SB County Fire dispatching (800mhz) &amp; Local VHF fire channels click on “details” for additional info.</td>
<td>HTML5 Web Player</td>
</tr>
<tr>
<td>San Bernardino County System 1 - Sheriff and Fire</td>
<td>Public Safety</td>
<td>99</td>
<td>Victor Valley area including Victorville, Hesperia, Apple Valley and the local High Desert.</td>
<td>HTML5 Web Player</td>
</tr>
<tr>
<td>San Bernardino County System 6, 7, 8 - East Valley and SB Attn Police, Fire, EMS</td>
<td>Public Safety</td>
<td>7</td>
<td>Redlands FD &amp; PD, Crestline, Big Bear; Lake Arrowhead, Yucaipa, Oak Glen, Highland, Loma Linda &amp; Mentone Sheriff. Yucaipa &amp; Highland Cal Fire. SBI 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</td>
<td>HTML5 Web Player</td>
</tr>
<tr>
<td>San Bernardino County System 9 - West End Police, Fire and EMS</td>
<td>Public Safety</td>
<td>14</td>
<td>Ontario PD Dispatch</td>
<td>HTML5 Web Player</td>
</tr>
<tr>
<td>San Bernardino Police System 10</td>
<td>Public Safety</td>
<td>45</td>
<td>Thank you to the men and women that do their best to protect us.</td>
<td>HTML5 Web Player</td>
</tr>
</tbody>
</table>
How easy is it to listen in?

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

Figure 1: Symmetric Block Cipher

“ The agile white cat jumps over the sleeping dog ”

“ akjshffdkg,najfl@%&d lfa fapuw S;IkssdHfjsd% fjgznxvsjdfjFD “

Plain-text input

Cipher-text

Plain-text output

Encryption

Decryption

Same key
(shared secret)
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.
  – 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.
    - 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.
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, VLA
    - 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)
  – All Reports are located on the DHS website:
    • http://www.dhs.gov/technology
NPSTC Outreach Report on Encryption and Interoperability

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

In the News...
- NPSTC/GCSS 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
  March 27, 2017
- NASCIO Issues Advancing Digital Government: Better Decision-Making through Data Sharing Agreements
  March 27, 2017

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, particularly in recognition of the need for unclassified communications to support effective operations and to resolve terrorist events. The use of full-time encryption by First-Responder and Emergency Medical Services is being realized and implemented in some areas of the nation as well. This is sometimes driven by the use of a shared interoperability system with law enforcement or by agency policy and directives.

Encryption employs algorithms to protect message content from disclosure to unauthorized persons. In summary, encryption converts data, including digital text streams, into a form called ciphertext that cannot be understood by unauthorized entities. An authorized entity uses decryption to convert the ciphertext back into intelligible form. The process requires that equipment used by the engineer and the intended receiver be programmed with compatible encryption and decryption keys, and that both keys be appropriately managed and updated periodically. If these keys are not appropriately managed and updated periodically, this requires advanced planning among authorized users and agencies that need to exchange information.

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 effective interoperability among the various agencies over community designated channels. The Federal Communications Commission (FCC) has designated select channels in each public safety band.

Notes:

1. There are several types of corruption algorithms in use today in the public safety environment, ranging in strength from 40 bits (DES) to 256 bits (AES). In December 2013, the Department of Homeland Security (DHS) released its 2013 encryption policy, Title 6 Code of Federal Regulations (6 CFR) Part 528. The policy requires that all public safety communications equipment be considered vulnerable unless its encryption strength is currently the strongest (256 bits). The policy defines a few “handsets,” as above, with a 16-bit encryption strength. Any device adjudged to be vulnerable will be, by final rulemaking, required to be replaced or otherwise resolved. This is expected to occur within five years.

2. A list of all encryption devices used by public safety and other agencies, and which are not vulnerable, is maintained by the Federal Communications Commission (FCC) and is available on its website. This list is updated periodically to reflect changes in technology and standards. Any device that is not vulnerable is considered compliant with the 6 CFR Part 528 encryption policy. The list is available at the following link: https://www.fcc.gov/safety/emergency-communications/fcc-develops-encryption-list-first-responders-38
NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

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

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 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 (RADIO PCR) Working Group
- 3.5 - Unmanned Aircraft Systems and Robotics WG
- 3.6 - Video Technology Advisory Group
- 3.7 - Internet of Things (IoT) Working Group

Sign Up
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.

Thank You