
# NPSTC Update

## IACP Communications & Technology Committee

## Sunday, May 21, 2017

## St. Louis, MO

Stu Overby, NPSTC Support Office
Soverby@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.

# Why NPSTC?

The National Public Safety Telecommunications Council is a federation of public safety organizations whose **mission is to improve public safety communications and interoperability through collaborative leadership**.

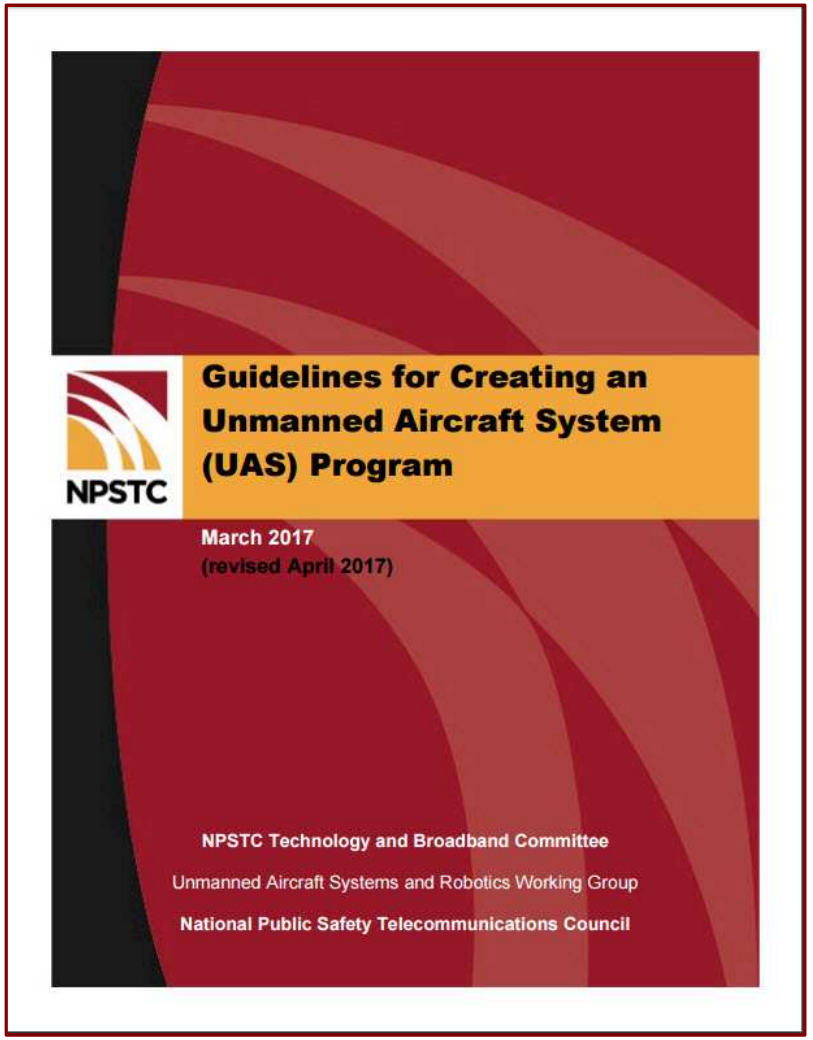
NPSTC pursues the role of **resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications**.

# NPSTC Results

- Since the IACP C&T Committee last met October 16, 2016, NPSTC has:
  - Developed/issued five reports and contributed to two others. For full list/reports see http://www.npstc.org/npstcReports.jsp
  - Submitted 11 sets of input/recommendations to regulatory agencies. For full list/documents see http://www.npstc.org/regulatoryActions.jsp
- Some highlights follow.

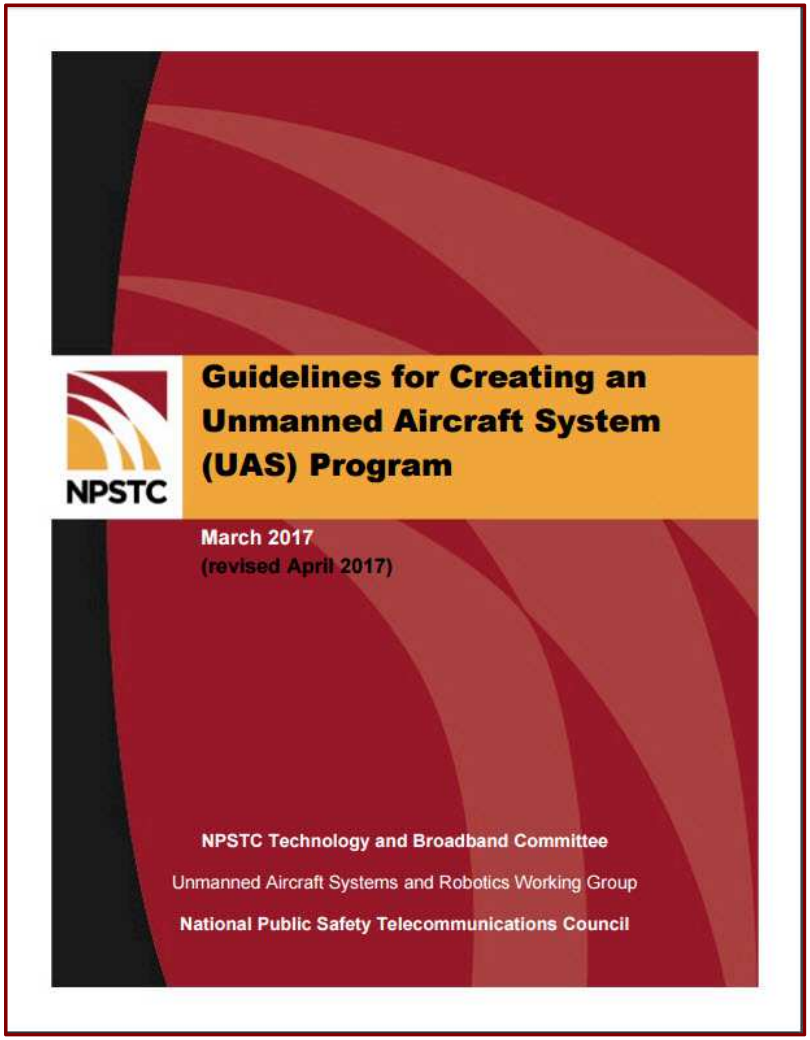
# Guidelines for Creating an Unmanned Aircraft System (UAS) Program

- Identifies specific components public safety agencies need to evaluate
- Program Planning
- Policy Development
- Cost Considerations
- Public Perception and Privacy
- Legal Concerns
- UAS Operational Capabilities
- UAS Airspace Integration



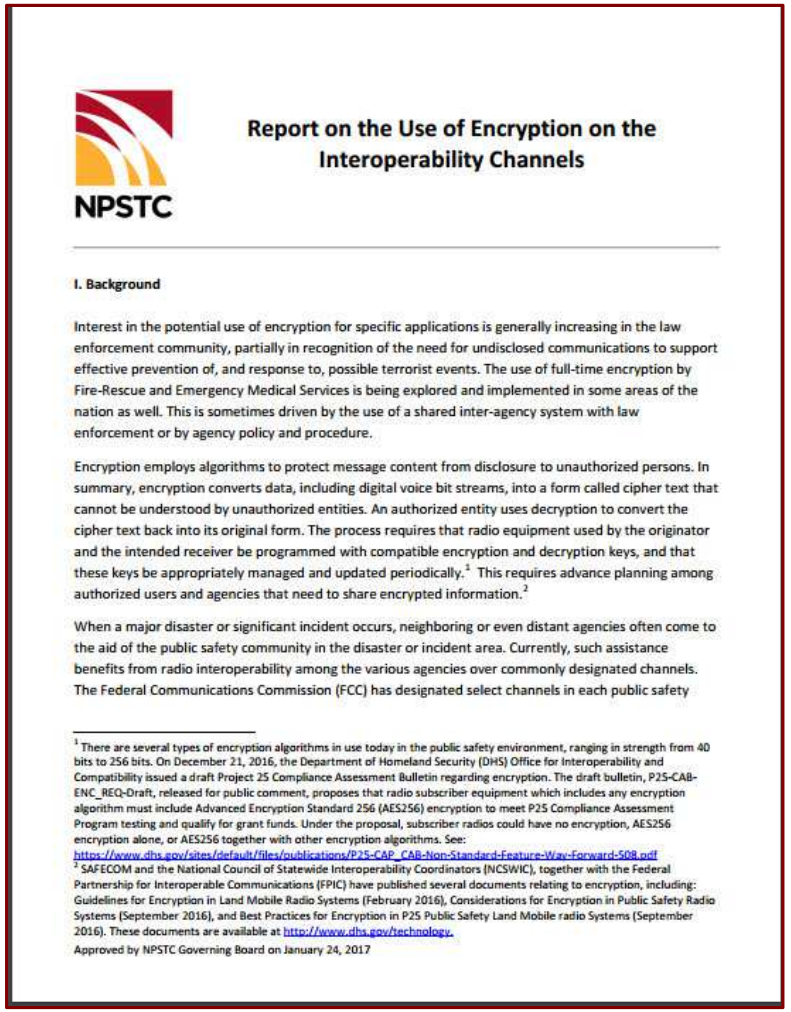
# Broadband Deployable Systems in the Nationwide Public Safety Broadband Network

- Report from NPSTC and the Defence Research and Development Canada - Centre for Security Science (DRDC-CSS).
- Operational, technical and background information.
- Public safety technical requirements.
- Technical challenges.
- Conclusions and recommendations.
  - Illustrate public safety expectations
  - Articulate a path forward for implementation and use



# Report on the Use of Encryption on the Interoperability Channels

- Recognizes benefits of encryption.
- Notes challenges when used on interoperability channels.
- Discusses results of NPSTC questionnaire.
- Addresses FCC Rules.
- Provides list of FCC designated interoperability channels with frequency and NIFOG channel name.



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

# NPSTC Regulatory Filings

| Date Filed | Topic | Type of Filing |
|---|---|---|
| **5/01/17** | **700 MHz A-G Border** | **Comments, FCC** |
| 4/12/17 | V2V Mandate & Standardization | Comments, DOT/NHTSA |
| **3/24/17** | **Wilson/Cellular Boosters** | **Comments, FCC** |
| 3/06/17 | Higher Ground | Comments, FCC |
| 1/27/17 | North Dakota on-VLAW 31 | Comments, FCC |
| 1/22/17 | P25 Encryption Capabilities | Letter, DHS/OIC |
| 12/07/16 | IMSA 6.25 Waiver Request | Ex Parte, FCC |
| 11/22/16 | Conditional licensing/other issues | Comments |
| 11/16/16 | Rules on CMRS vs. PMRS | Reply Comments |
| 11/08/16 | AEP/Sprint vacated channels | Reply Comments |
| 10/26/16 | P25 CAP | Comments |

# 700 MHz Public Safety Air-to-Ground (ATG)

- Eight Channels previously designated for ATG in U.S.
- Current U.S./ Canada Agreement does not cover ATG.
- FCC-U.S./ISED-Canada in discussions.
- NPSTC recommendations filed with FCC May 1, 2017:
  - Designate different channels in U.S. and Canada for day-to-day ATG use to enable greater use and flexibility in both countries
  - Select Canada day-to-day ATG channels in 775-776/805-806 MHz
  - Provide for Canada PS to use one or more U.S. ATG channels only for joint U.S./Canada operations, to enable interoperability

# Wilson Electronics Petition

- Wilson Electronics petition seeks to eliminate “personal use” restrictions in Section 20.21 of FCC rules for sale and use of consumer signal boosters.
- Rule applies to commercial and not public safety spectrum.
- However, rule can impact public safety entities and businesses that use commercial wireless systems.
- NPSTC submitted comments March 23, 2017 supporting the Wilson Electronics request.
  - Note: *NPSTC representatives from IACP and IAFC took a key interest in supporting the request.*

# Education on Spectrum Sharing

- NPSTC Spectrum Management Committee held two educational sessions to learn how dynamic spectrum management through a spectrum access system (SAS) is designed and is being tested at 3.5 GHz.
- 3.5 GHz not a local/state public safety band, but FCC and industry approach is instructive.
- Initial conclusion: spectrum environment in a particular band is a key factor in viability of sharing mechanisms.

# Public Safety Internet of Things (IoT)

- NPSTC Governing Board approved a new IoT working group on January 24, 2017. WG Chair: Barry Fraser
- 80 members from public safety, industry and academia.
- Work items in the IoT WG charter:
  - Examine current state of IoT.
  - Examine specific issues that impact public safety (e.g., sensor support for public safety responses; analytic processing).
  - Identify issues and concerns for action by the NPSTC Governing Board.
- Additional work may include developing outreach material, examining role of standardization, etc.
- The WG meets 1st Thursday each month, noon eastern time

# Upcoming

- May (date TBD): Release of new NPSTC whitepaper on FirstNet and Public Safety Broadband Data: Implications for Rural EMS Organizations
- June 6: NPSTC Webinar on U.S./Canada Cross Border Communications
  - Noon eastern time
  - 510-227-1018 PIN 446-1830 (audio)
  - http://Join.me/npstcsupport1 (view slides)

# Upcoming, *continued*

- June 22: Planned FCC issuance of Blue Alert proposal
  - Announced by FCC Chairman Pai May 19.
  - FCC would seek comment on proposal to add a Blue Alert code to the Emergency Alert System (EAS).
  - If ultimately approved, local and state governments would have option to use dedicated Blue Alert code to advise public of imminent threat against law enforcement.
  - FCC Goal is to spur coordinated nationwide framework.

# Thank you to NPSTC participants for creating:


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