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

band to serve as nationwide interoperability channels.[3] Although encryption is useful in a number of circumstances, its use on these designated channels can present a challenge to interoperability and shared assistance among agencies. Accordingly, NPSTC recommended that encryption not be deployed on the FCC-designated nationwide interoperability channels. These channels are few in number compared to the overall operational channels available. Therefore, any information that must be encrypted can be transmitted over operational channels outside those specifically designated by the FCC for nationwide interoperability. For example, local, regional, and statewide interoperability channels that are distinct from these nationwide interoperability channels are not affected by the FCC order and have the option to be used with encryption. There are also a number of public safety mutual aid channels in use across the U.S. which are not affected by this order.[4] Finally, the NTIA designated interoperability channels (e.g., IR and LE) channels are not impacted by the FCC order.

In early 2016, NPSTC coincidentally was beginning an examination of encryption and its potential use on the nationwide interoperability channels. While there was no call to change the previous recommendation that encryption not be used on nationwide interoperability channels, NPSTC periodically reviews its positions to ensure they continue to reflect public safety requirements. An FCC decision released in April 2016 helped answer the question.

To help promote interoperability, the 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.[5] While the rule changes did not specifically address encryption, the requirement for analog FM modulation on the nationwide interoperability channels effectively prevents the use of encryption on those channels. Also, the FCC decision is specific that the analog FM requirement applies both to the calling and tactical public safety nationwide interoperability channels in the VHF, UHF, and 800 MHz bands. In reaching its decision, the FCC noted that given its prevalence, analog FM was already the *de facto* interoperability standard on these channels. NPSTC also notes that mobiles and portables designed to be compliant with the Project 25 (P25) standard used by public safety include an analog FM mode for backward compatibility. The FCC undertook codifying the analog FM requirement for interoperability as a result of other digital equipment becoming available which did not include an analog FM mode of operation.

II. NPSTC Follow-Up

In May 2016, NPSTC created a task force within its Interoperability Committee to examine the FCC decision and assess its impact, if any, on public safety operations. To help make this assessment, the task force issued a questionnaire in July 2016 to NPSTC participants. The questionnaire included the following three questions:

[3] For purposes of his paper, NPSTC will refer to the FCC-designated nationwide interoperability and mutual aid channels collectively as nationwide interoperability channels.

[4] This includes the VFIRE, VMED, VLAW, UHF MED frequencies and all 700 MHz Air to Ground channels, on which encryption can occur.

[5] Report and Order, PS Docket No. 13-209, released April 25, 2016.

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 received 42 responses to the questionnaire. Thirty-nine of the respondents were from local and state agencies geographically located across 21 states. The remaining three responses were from a consultant and two parties whose affiliation could not be identified. The responses to the questionnaire show the FCC rule will have virtually no impact on the use of encryption by public safety agencies. These agencies advised they were not using encryption on the VHF, UHF, or 800 MHz nationwide interoperability channels and that they see no issues with the FCC rules adopted in April 2016. Five of the respondents indicated their agencies use encryption on a portion of the 700 MHz band interoperability channels the FCC designated for tactical use. This is consistent with the FCC rules. At 700 MHz, the FCC prohibits encryption only on the nationwide interoperability calling channels. There is no FCC prohibition re encryption on the 700 MHz band nationwide interoperability tactical channels. Also, the analog FM requirement adopted in April 2016 that effectively prevents the use of encryption applies only to VHF, UHF, and 800 MHz nationwide interoperability channels, not to the 700 MHz band interoperability channels.

In a subsequent decision released in August 2016 to allow Railroad Police access to the public safety nationwide interoperability channels, the FCC published a list of the interoperability channels in the rules.[6] The list of designated nationwide interoperability channels as recognized collectively by the FCC and the Department of Homeland Security National Interoperability Field Operations Guide (NIFOG) is included as an Appendix to this document. [7] That FCC decision specifically addressed encryption and indicated that encryption is prohibited on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz, and 700 MHz bands. Given that decision appears to yield different results from those of the April 2016 FCC decision regarding analog FM use, NPSTC contacted FCC staff for clarification. NPSTC learned that the lack of any mention regarding any prohibition of encryption on the tactical channels in the VHF, UHF, and 800 MHz bands in the Railroad Police decision does not supersede the requirement for analog FM modulation. The FCC staff advised that any change to that outcome would require initiation of a new rulemaking proceeding.

Accordingly, as the rules now stand, encryption is effectively prohibited on both the calling and tactical nationwide interoperability channels in the VHF, UHF, and 800 MHz bands and on the calling nationwide interoperability channels in the 700 MHz band.

[6] Report and Order, PS Docket No. 15-199, released August 23, 2016, revisions to Section 90.20(i) of the rules.
[7] See https://www.dhs.gov/publication/nifog-documents

Appendix-List of Public Safety Nationwide Interoperability Channels by Band[8]

VHF Band PS Interoperability Channel (MHz)
[Encryption Effectively Prohibited by FM Analog Requirement]
151.1375 MHz (base/mobile) Tactical (VTAC11)
154.4525 MHz (base/mobile) Tactical (VTAC12)
155.7525 MHz (base/mobile) Calling (VCALL10)
158.7375 MHz (base/mobile) Tactical (VTAC13)
159.4725 MHz (base/mobile) Tactical (VTAC14)

UHF Band PS Interoperability Channel (MHz)
[Encryption Effectively Prohibited by FM Analog Requirement]
453.2125 MHz (base/mobile) Calling (UCALL40)
458.2125 MHz (mobile) (UCALL40D)

453.4625 MHz (base/mobile) Tactical (UTAC41)
458.4625 MHz (mobile) (UTAC41D)

453.7125 MHz (base/mobile) Tactical (UTAC42)
458.7125 MHz (mobile) (UTAC42D)

453.8625 MHz (base/mobile) Tactical (UTAC43)
458.8625 MHz (mobile) (UTAC43D)

800 MHz Band PS Mutual Aid Channel (MHz)
[Encryption Effectively Prohibited by FM Analog Requirement]
851.0125 MHz (base/mobile) Calling (8CALL90)
806.0125 MHz (mobile)

851.5125 MHz (base/mobile) Tactical (8TAC91)
806.5125 MHz (mobile)

852.0125 MHz (base/mobile) Tactical (8TAC92)
807.0125 MHz (mobile)

852.5125 MHz (base/mobile) Tactical (8TAC93)
807.0125 MHz (mobile)

[8] Channels listed are those identified collectively by the FCC in Section 90.20(i) of the rules and by the 2016 DHS National Interoperability Field Operations Guide (NIFOG). See https://www.dhs.gov/publication/nifog-documents. Common channel names shown are from the 2016 NIFOG. Section 90.20(i) of the FCC rules also list five channel pairs of interoperability/mutual aid channels available for public safety in the 220-222 MHz bands, however, the NIFOG does not include those channels, so they are not listed here at this time.

853.0125 MHz (base/mobile) Tactical (8TAC94)
808.0125 MHz (mobile)

700 MHz Band PS Interoperability Channel (MHz)
[Encryption Specifically Prohibited on Calling Channels But Allowed on Tactical Channels]

769.24375 MHz (base/mobile) Calling (7CALL50)
799.24375 MHz (mobile)

769.14375 MHz (base/mobile) Tactical (7TAC51)
799.14375 MHz (mobile)

769.39375 MHz (base/mobile) Tactical (7MED65)
799.39375 MHz (mobile)

769.49375 MHz (base/mobile) Tactical (7MED66)
799.49375 MHz (mobile)

769.64375 MHz (base/mobile) Tactical (7TAC52)
799.64375 MHz (mobile)

769.74375 MHz (base/mobile) Tactical (7TAC55)
799.74375 MHz (mobile)

769.89376 MHz (base/mobile) Tactical (7FIRE63)
799.89375 MHz (mobile)

769.99375 MHz (base/mobile) Tactical (7FIRE64)
799.99375 MHz (mobile)

770.14375 MHz (base/mobile) Tactical (7TAC53)
800.14375 MHz (mobile)

770.24375 MHz (base/mobile) Tactical (7TAC56)
800.24375 MHz (mobile)

770.39375 MHz (base/mobile) Tactical (7LAW61)
800.39375 MHz (mobile)

770.49375 MHz (base/mobile) Tactical (7LAW62)
800.49375 MHz (mobile)

770.64375 MHz (base/mobile) Tactical (7TAC54)
800.64375 MHz (mobile)

770.89375 MHz (base/mobile) Tactical (7MOB59)
800.89375 MHz (mobile)

770.99375 MHz (base/mobile) Tactical (7GTAC57)
800.99375 MHz (mobile)

773.00625 MHz (base/mobile) Tactical (7MED86)
803.00625 MHz (mobile)

773.10625 MHz (base/mobile) 803.10625 MHz (mobile)	Tactical (7TAC71)
773.25625 MHz (base/mobile) 803.25625 MHz (mobile)	Calling (7CALL70)
773.35625 MHz (base/mobile) 803.35625 MHz (mobile)	Tactical (7MED87)
773.50625 MHz (base/mobile) 803.50625 MHz (mobile)	Tactical (7FIRE83)
773.60625 MHz (base/mobile) 803.60625 MHz (mobile)	Tactical (7TAC72)
773.75625 MHz (base/mobile) 803.75625 MHz (mobile)	Tactical (7TAC75)
773.85625 MHz (base/mobile) 803.85625 MHz (mobile)	Tactical (7FIRE84)
774.00625 MHz (base/mobile) 804.00625 MHz (mobile)	Tactical (7LAW81)
774.10625 MHz (base/mobile) 804.10625 MHz (mobile)	Tactical (7TAC73)
774.25625 MHz (base/mobile) 804.25625 MHz (mobile)	Tactical (7TAC76)
774.35625 MHz (base/mobile) 804.35625 MHz (mobile)	Tactical (7LAW82)
774.50625 MHz (base/mobile) 804.50625 MHz (mobile)	Tactical (7MOB79)
774.60625 MHz (base/mobile) 804.60625 MHz (mobile)	Tactical (7TAC74)
774.85625 MHz (base/mobile) 804.85625 MHz (mobile)	Tactical (7TAC77)
774.75625 MHz (base/mobile) 804.75625 MHz (mobile)	Data/Voice[9] (7DATA89)

[9] Voice is allowed on a secondary basis per FCC Rule 90.531(b)(1)(i)