Considerations for Encryption in Public Safety Radio Systems

Determining the Need for Encryption in Public Safety Radios

We live in an ever-changing world, and the world is becoming a more complicated and dangerous place to live and work. This heightened danger has caused public safety agencies to place greater importance on how they use technology and how they enhance their ability to protect and serve. Since the terrorist attacks of September 11, 2001, public safety continues to rethink communications strategies to meet new challenges. Today many public safety communications channels get streamed across the Internet and are openly broadcast to the public, media, criminals, and potential terrorists providing immediate access to sensitive public safety information.

As agencies work to enhance interoperability, they also have to remain keenly aware of the need to protect sensitive public safety communications. Compromised information can be used to hinder emergency response, impede investigations and surveillance, and endanger the public. Many public safety agencies combine local, regional, or statewide government communications needs into multi-jurisdictional or multi-discipline systems. These large shared systems often integrate public safety, public service, maintenance, and administration into a single radio system. Although these disciplines are not always critical to the safety of life, they *do* support law enforcement, firefighting, and emergency medical missions that include:

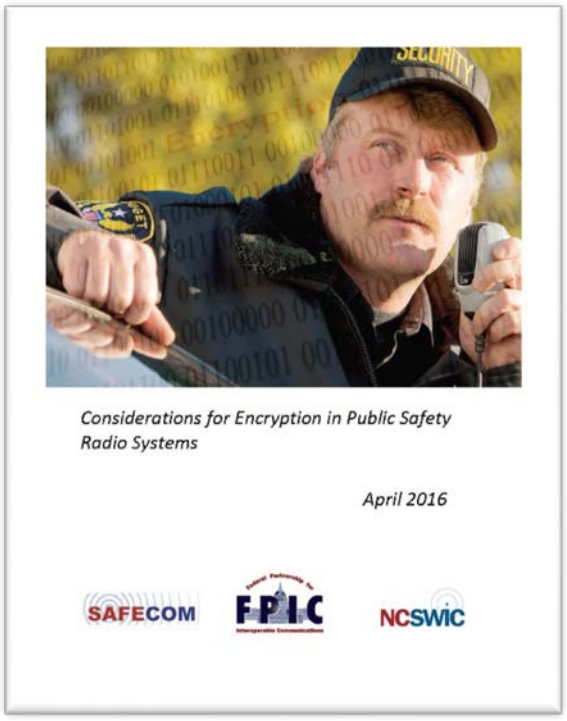
- **Safety of personnel, and enhanced safety of the public and property**
- **Sensitive law enforcement information including active investigations and surveillance**
- **Personally identifiable information or protected health information**
- **Tactical/investigative information that may jeopardize law enforcement operations, and**
- **Disaster incident information that may reduce reaction abilities of public safety officials.**

In many cases, public safety radio communications are transmitted "in the clear[1]," removing protection from monitoring by someone with a basic knowledge of radio communications by using fairly simple over the counter equipment. In a threat-based environment, compromise of any information can be problematic and may jeopardize safety and mission integrity. Radio encryption would help to decrease a threat of compromise and reduce the risk to personnel safety while providing protection of sensitive information.

[1] "In the clear" transmissions are unencrypted radio signals that are open to reception and listening by anyone with a receiver.

THE REPORT

This document examines why encryption may be necessary during critical operations. Encryption provides a method of protecting personally identifiable and/or sensitive information. Different jurisdictions may have differing legal requirements relating to encryption of communications on public safety radio systems. Therefore, when considering encryption, a legal analysis should be conducted. Recent incidents illustrate why encryption is a must for public safety are discussed in this document. They include:



- **Active shooter**
- **Public knowledge of sensitive public safety information**
- **Safety of public safety personnel and the public**

Other scenarios might involve Urban Search and Rescue, training, emergency response, active investigation and surveillance, personally identifiable information, and scanners/social media are discussed. The examples discussed in this document provide examples of how encryption did or would have affected the outcome of public safety actions regarding criminal activity or the compromise of protected personal information.

IMPLICATIONS FOR THE PUBLIC SAFETY COMMUNITY

Radio encryption provides the best way to protect critical information from compromise and disclosure when necessary to transmit it over airwaves. Use of encryption is an important policy decision that stakeholders, decision-makers, and leadership must understand and carefully consider as they plan for the future. Encryption can significantly decrease the risk that sensitive public safety information can be compromised and used to impede effective emergency response. The policy and legal decision to use encryption is not without complexities. The threat of compromise of critical information resulting in increased threats to the safety of the public is clear.

Before decision makers decide when and how to encrypt, it is important to consider what information to protect. Each jurisdiction will have different perspectives; the primary questions to be addressed will include:

- **What information should be protected (encrypted)?**
- **What method of encryption should be implemented?**
- **What is the impact on communications interoperability?**
- **What about the added cost vs. the impact of compromise?**
- **What is the effect on public information access?**

All the factors discussed in this document should be carefully considered in determining the appropriate encryption for that public safety radio system in that specific jurisdiction. Federal agencies recognize the importance of encrypting public safety mission critical radio communications and embrace the fact that encryption is vital to national security and mission integrity. State and local governments must answer for themselves the basic question: *Does the cost and effort related to the implementation and management of encryption outweigh the risks associated with the exposure of sensitive information?*

This document is provided to assist public safety users as they embark on a process to assess their need for encryption.