



Standard Operating Procedure

Title / Subject <u>Encryption</u>	Effective Date 09/13/11	Revision Date 09/13/11
---	----------------------------	---------------------------

References

Contents

1. Purpose:.....	2
2. Policy:.....	2

1. Purpose:

The Statewide Interoperable Radio Network (SIRN) acknowledges the need for emergency responders to have secure communications. The SIRN also acknowledges that the APCO P-25 Trunking System provides a more secure base of communications, in and of itself, than most agencies and end users are accustomed to in West Virginia. This is achieved through the trunking technology. The SIRN recognizes that to achieve true interoperability, accepted encryption must be standardized within the system.

2. Policy:

2.1 The only type of encryption that may be utilized for any interoperable connectivity on the system is the AES standard.

2.1.1 AES is approved by the US Secretary of Commerce as the official US government standard, effective May 26, 2002. AES is the Federal Information Processing Standard (FIPS) that specifies a cryptographic algorithm for use by US government organizations to protect sensitive, unclassified information. AES is a 256 bit algorithm and will pass over a digital channel.

2.1.2 This standard is available from several different major manufacturers. If required for encryption, each radio needs to have a hardware board installed in the radio, preferably at the time of purchase. Purchasers are encouraged to buy their equipment in the most efficient method, and normally, purchasing hardware options at the time of purchase rather than at a later date is more economical.

2.2 Proprietary encryption is not compatible with interoperability due to equipment variations among end users (mobiles and portables) and defeats the purpose of a truly interoperable system.

2.3 Encryption shall not be used on any primary dispatch channel /talk group by any Dispatch Center or E9-1-1 Center.

2.3.1 When an agency determines that it is operationally necessary to engage in encrypted communications, they shall utilize a designated channel /talk group other than a primary dispatch channel /talk group.

2.3.2 Participants of the system should not use encrypted methods of communication as a common practice. Encrypted communications should be utilized only for operational needs of the participating agency.

2.3.3 In the event the SIRN determines a talk group is in violation of this policy, that talk group may be configured in the system to prevent encryption on said talk group.