The Commonwealth of Massachusetts
Executive Office of Public Safety and Security
One Ashburton Place, Room 2133
Boston, Massachusetts 02108
Tel: (617) 727-7775
TTY Tel: (617) 727-6618
Fax: (617) 727-4764
www.mass.gov/eopss

CHARLES D. BAKER
Governor
KARYN E. POLITO
Lt. Governor

THOMAS A. TURCO, III
Secretary

Guidance Bulletin #20-1

Public Safety Agency Encryption

The following informational bulletin provides basic guidance to public safety agencies on the encryption of land mobile radio (LMR) equipment. This bulletin does not mandate the use of encryption, or the sharing of encryption keys. Instead, the goal is to encourage encryption coordination among local, regional and federal agencies. Additionally, this guidance helps standardize and ensure interoperable use of LMR encryption in the Commonwealth.

Agency administrators should ask "Who are we intending to secure our communications from?" and choose an encryption standard that accomplishes this goal by being secure and meeting P25 digital standards. There are no compliant forms of analog encryption. Here are three areas to consider when planning encryption deployment and equipment programming.

Purchasing Guidelines

Agencies should ensure the following minimum purchase requirements are met:

- LMR equipment should support a minimum encryption type of **AES-256.** Older standards, or proprietary algorithms (ex: ADP, DES), are not recommended for public safety, and do not meet P25 standards or grant requirements.
- LMR equipment should support more than one encryption key (often referred to as "multikey").

CKR/SLN and KID/LID Assignments

To avoid encryption key conflict, agencies should:

- Prohibit the use of CKR/SLN #'s 1 through 20. These are reserved for nationwide interoperability.
- Each KID/LID should be a randomly generated hexadecimal code between 0001 - FFFF OR agency may choose to use the CKR/SLN number.
- Contact the SWIC for all CKR/SLN assignments. This applies to all algorithm types. **EOPSS does not record, nor will it request your "key data". The sharing of keys is at the discretion of the home agency.
- Consider the use of common encryption keys to ensure interoperability with neighboring agencies/partners.

Channel Programming

- "Strapped" encrypted channels / zones are recommended as opposed to a "clear / coded" switch.
- Agencies shall ensure that their LMR equipment has zones / banks that include and conform explicitly with the Massachusetts Tactical Channel Plan (MTCP). The most current version of the MTCP is available through the SWIC.

For further guidance and information about encryption, or for any questions regarding this bulletin, please contact the Commonwealth's Statewide Interoperability Coordinator (SWIC) at ma.swic@mass.gov.