



Alcohol
and Gambling
Enforcement

Bureau of Criminal
Apprehension

Driver
and Vehicle
Services

Emergency
Communication
Networks

Homeland Security
and Emergency
Management

Minnesota
State Patrol

Office of
Communications

Office of
Justice Programs

Office of
Traffic Safety

State Fire Marshal

Emergency Communication Networks

445 Minnesota Street • Suite 137 • Saint Paul, Minnesota 55101-5137
Phone: 651.201.7547 • Fax: 651.296.2665 • TTY: 651.282.6555
www.ecn.state.mn.us

To: Emergency Communications/Services Board Grant Administrators
From: James Stromberg, ARMER Program Manager
Date: August 27, 2020
Subject: Grant funding eligible for LMR encryption costs

The Minnesota Allied Radio Matrix for Emergency Response (ARMER) system has long used the Digital Encryption Standard-Output Feedback (DES-OFB) algorithm as an optional tool to encrypt land mobile radio communications. DES-OFB is an aging algorithm that could arguably be replaced by a more modern algorithm known as the Advanced Encryption Standard (AES). Unfortunately, there are many obstacles to moving to AES; one of them being that most encryption-enabled end user radios are only enabled to use DES-OFB.

In October 2019, the Finance Committee of the Statewide Emergency Communications Board (SECB) authorized the use of grant funding to facilitate the migration of LMR equipment from DES-OFB to AES with the caveat that the purchase of encryption capabilities must align with current SAFECOM guidance. The [SAFECOM Guidance on Emergency Communication Grants](#) states:

- Recipients investing in encryption must implement the Advanced Encryption Standard (AES) 256-bit Encryption Algorithm as specified in the P25 Block Encryption Protocol.
- Recipients seeking to use federal grant funds to purchase non-standard encryption features (e.g., 40-bit encryption, DES-OFB) or capabilities for new or existing equipment must ensure AES 256-bit is also included to ensure their devices have the capability to interoperate in an encrypted mode.
- Agencies currently using DES-OFB may continue to invest in this encryption method but should plan to migrate to AES as soon as possible. The continued use of DES-OFB or other non-standard encryption algorithms is strongly discouraged.

In summary, local jurisdictions may use grant funds to purchase encryption provided that the purchase is an allowable expense under the provisions of the grant program and both AES and DES-OFB capabilities are included. This should not have a financial impact to the purchasing entity in that most radio manufacturers are now providing AES and DES-OFB encryption at the same cost as just DES-OFB. Be sure to confirm this with your sales representative before making a purchase.

Please reach out to your [Regional Interoperability Coordinator](#) if you have any questions.