



June 15, 2017

To: Department of Homeland Security
Office of Interoperability and Compatibility

Subject: Implementing Single-Key AES in Encrypted Harris Public Safety Radios

This Memorandum will document the Harris Corporation plans to be fully compliant with the Department of Homeland Security (DHS) guidelines for encryption in grant eligible equipment ("P25 CAP Encryption Requirements (March 2017)"). Harris fully supports the DHS efforts to enable first responders to communicate between agencies using equipment from different manufacturers.

Today, Harris radios are available: (1) completely unencrypted, (2) with free single-key DES and ARC4 encryption, or (3) with full multi-key AES/DES encryption. We understand the intent to encourage the use of standard AES encryption and to avoid user reliance on non-standard algorithms.

To comply with DHS guidelines, Harris is adding single-key AES encryption to our product basket. Single-key AES operation will automatically be bundled with our lower-tier simple encryption package. With this update, Harris radios will be available: (1) completely unencrypted, (2) with free simple encryption (including single-key AES encryption), or (3) with full multi-key AES/DES encryption. Radios with any encryption will always have the AES-256 algorithm included. Based on earlier discussions between DHS and Harris, we believe this plan will satisfy the DHS guidelines for grant eligible equipment.

Harris has already started developing the single-key AES feature. Thanks to this early start, field trials of single-key AES operation are scheduled to begin soon with the expectation that Harris will provide single-key AES operation to customers this calendar year. Harris plans to offer to users who have already taken delivery of radios with non-standard ARC4 encryption, at no charge, a software upgrade that will include single-key AES encryption. This software upgrade will be offered when full release of the new single-key AES encryption code is available.

Harris' commitment to single-key AES encryption and P25 open standards is intended to directly support the policies and guidelines being promoted by the Department of Homeland Security. Please contact the undersigned if you have any questions or need additional information regarding the Harris encryption planning.

Regards,



Mark Tesh
Senior Product Manager
Harris Corporation

