L3HARRIS
FAST. FORWARD.

L3Harris Technologies, Inc.

HI E PAPER

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

›

›

1 2 N A 3 4 LMR

I I

a

FM

/A /A /

M a A D a P (ADP) L3Ha F L RC4 (ARC4), a Pa C 4 (RC4). A RC4 RC4

ARC4, LMR a 40- .I H

[illegible]

[illegible] (NIST) [illegible]

[illegible] ([illegible])

[illegible] NIST C[illegible] M[illegible] P[illegible]al (CMVP) [illegible].[3]

FIPS 140-2

[illegible] 2001, FIPS 140-2, *Security Requirements for Cryptographic Modules*, [illegible] NIST [illegible].

[illegible]

FIPS 140-2 [illegible] N[illegible] A):[4]

[illegible] 11.8 [illegible])2.1 (N)3.4 (I) [illegible] 33.9 [illegible])-3.7 ()0.5 [illegible] 4325I[illegible])-7. N [illegible] 2-243-9.422[illegible]6[illegible])-5.9

I I	1	2		
A a				
a				
- a a a				
a a				
I - a a a				
a a a a a a				
a a				

Table 1: FIPS 140 Security Levels

I

A

I -a A

DES, ARC4, and other proprietary encryption methods are helpful to prevent casual eavesdropping, but FIPS-approved encryption algorithms are essential for true information security. Today, for LMR communications, AES is the approved algorithm. In the future, as computing power increases and potential weaknesses to AES are discovered, other algorithms will be published by NIST and implemented by LMR vendors.

a I

When implementing AES encryption, it is essential that the cryptographic module be validated (certified) by the CMVP. Without this certification, one cannot ensure that encryption has been properly implemented or communications adequately secured. Do not accept an unvalidated encryption module.

FIP 140-2

NI

FIP 140-2

1

Several LMR vendors offer FIPS 140-2 Level 1-certified encryption modules. Only one vendor offers a Level 3-certified module.

Level 3 offers some advantages over Level 1: When a module is tampered with, Level 3-certified encryption prevents access to the encryption keys by

on encrypted communications from a lost or stolen radio. In addition, all aspects of manual or over-the-air key filling are encrypted, preventing anyone from manually copying the text of a key.

The most serious disadvantage to Level 3 mode is entering a password when the radio is powered on. Imagine a police officer during a life-threatening situation whose radio is powered off accidentally. To call for help, not only does he have to turn the radio back on, he must re-enter his password as well. Any delay in making that call may be the difference between life and death. To most public-safety users, this risk far outweighs the additional security provided by Level 3.

While Level 3-certified encryption modules may prevent eavesdropping on encrypted communications, P25 offers system administrators other ways to prevent eavesdropping via lost or stolen radio3 (e)-11(o)-15.2n1fW2 (o)-10.4 (r)-24(u)-18y. Tsuc


FAST. FORWAR