



Department of Defense INSTRUCTION

NUMBER 4650.10

July 28, 2015

Incorporating Change 1, Effective April 13, 2016

CIO DoD

SUBJECT: Land Mobile Radio (LMR) Interoperability and Standardization

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)) and guidance in DoDD 3025.18 (Reference (b)), DoD Instruction (DoDI) 8330.01 (Reference (c)), and DoDI 5535.10 (Reference (d)), this instruction:

a. Establishes policy and assigns responsibilities to ensure that LMR systems support interoperable and secure communications with other federal, State, local, and tribal LMR users.

b. Directs the establishment of a list of DoD-required Telecommunications Industry Association (TIA) International Project 25 (P25) interfaces (referred to in this instruction as “DoD P25 interfaces”) to support LMR interoperability.

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the “DoD Components”).

b. Applies to all DoD operations, activities, and installations worldwide.

c. Will not alter or supersede the existing authorities, policies, and legal requirements of the National Guard Bureau, pursuant to Title 32, United States Code (U.S.C.) (Reference (e)), Title 10, U.S.C. (Reference (f)), and DoDD 5105.83 (Reference (g)).

3. POLICY. It is DoD policy that:

a. All DoD LMR equipment procured after the effective date of this instruction will:

(1) Conform with the TIA International P25 standards for LMR systems in DoD IT Standards Registry (References (h) and (i)).

(2) Be capable of operating on ~~all~~ United States and Possessions (US&P) DoD, federal, and non-federal LMR spectral allocations and channel plans between 138-869 MHz using either P25 Phase 1 or Phase 2 modulation and signaling; or narrowband frequency modulation (FM) (12.5 kHz ~~deviation~~ *channel bandwidth*) with associated Continuous Tone-Coded Squelch System/Digital Coded Squelch (CTCSS/DCS) signaling to facilitate direct interoperation with non-DoD P25 and FM LMR systems. Equipment that can also interoperate (both in terms of spectrum and modulation / signaling) on commonly-used LMR allocations for host nations (*HNs*) is highly desirable, but not required for US&P deployment.

(3) Comply with Committee on National Security Systems Policy 15 (Reference (j)) on the inclusion of appropriate algorithms and use National Security Agency (NSA)-approved cryptographic products when transmitting sensitive and classified information.

(4) Use National Institute of Standards and Technology (NIST)-validated cryptographic products when transmitting controlled unclassified information in accordance with Reference (j).

(5) Possess an authorization to operate following the categorization of system and the selection, implementation, and assessment of the security control for each LMR system in accordance with DoDI 8510.01 (Reference (k)).

b. All DoD LMR systems that employ:

(1) Encryption will comply with applicable security standards as set by the NIST Federal Information Processing Standards (FIPS) *Publication* Level 1 140-2 (Reference (l)), FIPS *Publication* 197 (Reference (m)), and NIST Special Publication (SP) 800-38A (Reference (n)). Systems will not use the Data Encryption Standard (DES) or Triple DES encryption algorithms. If equipped with encryption capability, be equipped with:

(a) A warning (audible or visual) to positively alert the user that a given transmission is not encrypted.

(b) Over-the-air-rekeying (OTAR) where security or operational requirements do not supersede this capability.

(c) Over-the-air-zeroization (OTAZ) or similar related to remote management of encryption keys where security or operational requirements do not supersede this capability.

(2) LMR trunking will comply with the P25 trunking specification, testing, and compliance assessment documents identified in Reference (i).

(3) LMR wide-area networks (also known as “Enterprise LMR”) will comply with the P25 inter-radio frequency (RF) subsystem interface specification, testing, and compliance assessment documents identified in Reference (i).

c. All DoD LMR systems operating inside of the ~~United States and its possessions~~ *US&P* will obtain frequency allocations for LMR enterprise network systems in accordance with the U.S. Manual of Regulations and Procedures for Federal Radio Frequency Management of the National Telecommunications and Information Administration (NTIA), commonly known as the “NTIA Redbook” (Reference (o)).

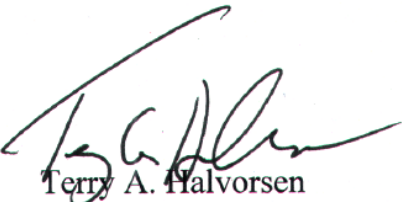
d. All DoD LMR systems operating outside of the ~~United States and its possessions~~ *US&P* will obtain ~~host nation~~-(HN) certification of spectrum support and HN authorization to operate in accordance with Reference (o), DoDI 4650.01 (Reference (p)), and policies of the CCMDs in whose areas of operations the LMR system is to be deployed and operated.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release.** This instruction is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This instruction is effective July 28, 2015.



Terry A. Halvorsen
DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....7

 CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE (CIO DoD)...7

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA)7

UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND

LOGISTICS (USD(AT&L)).....8

~~DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY~~

~~SERVICE (DIRNSA/CHCSS).....8~~

 DoD COMPONENT HEADS.....8

 CJCS9

 CDRUSNORTHCOM AND CDRUSPACOM9

 CNGB9

ENCLOSURE 3: PROCEDURES.....10

 LMR P25 STANDARDS COMPLIANCE.....10

 CYBERSECURITY.....10

 FIPS-Validated Cryptography10

 Key Management10

 INTEROPERABILITY STANDARDS FOR FIXED AND DEPLOYABLE LMR

 SYSTEMS.....11

 SPECTRUM SUPPORTABILITY11

 WAVEFORM MODIFICATIONS.....11

GLOSSARY12

 PART I: ABBREVIATIONS AND ACRONYMS12

 PART II: DEFINITIONS.....13

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
- (b) DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)," December 29, 2010, as amended
- (c) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
- (d) DoD Instruction 5535.10, "Coordination of DoD Efforts to Identify, Evaluate, and Transfer DoD Technology Items, Equipment, and Services to Federal, State, and Local First Responders," November 24, 2009
- (e) Title 32, United States Code
- (f) Title 10, United States Code
- (g) DoD Directive 5105.83, "National Guard Joint Force Headquarters – State (NG JFHQs – State)," January 5, 2011, as amended
- (h) Telecommunications Industry Association, Project 25 Statement of Requirements (P25 SoR) December 11, 2013
- (i) DoD Information Technology Standards Registry¹
- (j) Committee on National Security Systems Policy 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," October 1, 2012
- (k) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
- (l) Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001
- (m) Federal Information Processing Standards Publication 197, "Advanced Encryption Standard (AES)," November 26, 2001
- (n) National Institute of Standards and Technology Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation Methods and Techniques," December 2001
- (o) National Telecommunications and Information Administration, "Manual of Regulations and Procedures for Federal Radio Frequency Management," ~~2013 Edition~~ (May 2013), *as amended*
- (p) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
- (q) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," May 19, 2011
- (r) DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," January 13, 2009, as amended
- (s) Unified Command Plan, current edition²

¹ Available on the Internet for CAC users at <https://gtg.csd.disa.mil/disr/dashboard.html>

² For official use only and on a need-to-know basis, a copy can be requested from the J-5/Joint Staff.

- (t) DoD Instruction 8220.02, “Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations,” April 30, 2009
- (u) National Institute of Standards and Technology Special Publication 800-38B, “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,” May 2005
- (v) DoD Instruction 4630.09, “Wireless Communications Waveform Development and Management,” July 15, 2015
- (w) Section 90.7-~~Definitions~~ of Title 47, Code of Federal Regulations

ENCLOSURE 2

RESPONSIBILITIES

1. CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE (CIO DoD).

The CIO DoD provides oversight and policy development for all DoD LMR systems and activities.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the CIO DoD and in addition to the responsibilities in section 5 of this enclosure, the Director, DISA:

a. Supports the Commander, United States Northern Command (CDRUSNORTHCOM) and the Commander, United States Pacific Command (CDRUSPACOM) by monitoring the progress and issuance of P25 standards and providing guidance to DoD Components on LMR systems implementation.

b. Provides subject matter expert support to the CDRUSNORTHCOM and the CDRUSPACOM in the implementation of interoperability standards for fixed and deployable LMR systems.

c. Provides subject matter expert support to the CCMDs in the implementation of interoperability standards for fixed and deployable LMR systems and in the selection and implementation of interoperability solutions for interfacing of LMR systems to HN LMR radio and wireline systems, including those using Voice over ~~IP~~ *Internet Protocol* (VoIP).

d. With the support of the CDRUSNORTHCOM and CDRUSPACOM, establishes and maintains a list of DoD interfaces for which DoD LMR equipment and systems must be P25 certified for use throughout the US&P.

e. With the support of the CDRUSNORTHCOM, CDRUSPACOM, and Chief, National Guard Bureau (CNGB), represent the DoD with CJCS at working groups and forums, including, but not limited to, the TIA P25 User Needs Subcommittee, the National Public Safety Telecommunications Council, and the DoD Public Safety Communications Working Group.

f. Provides Joint Interoperability Test Command operational test certification capabilities in accordance with Reference (c) to support this instruction.

g. Establish and maintain through the Joint Spectrum Center (JSC), with the support of the JCS Military Command, Control, Communications, and Computers Executive Board, a set of all-DoD interoperability assignments in the 30-50, 138-150, and 380-400 MHz DoD spectrum allocations to be used for contingency, quick-response inter-Component communications. These assignments should include both simplex frequencies and half-duplex frequency pairs.

h. Support the Director, National Security Agency/*Chief, Central Security Service (DIRNSA/CHCSS)*, in the development, certification, and implementation of encryption systems suitable for classified communications over P25 networks.

3. *UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L))*. In coordination with the CIO DoD, the USD(AT&L):

a. ~~Oversees the implementation of this instruction by ensuring~~ *Directs* that ~~any reviews for~~ acquisition programs or procurements containing LMR equipment and systems comply with this instruction and validated LMR capability requirements.

b. Directs the development of DoD LMR system acquisition strategies to promote interoperability and reduce costs of procuring equipment and services, in accordance with Reference (a).

4. ~~DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS)~~. Under the authority, direction, and control of the Under Secretary of Defense for Intelligence, consistent with section 142 of Reference (f), and in addition to the responsibilities in section 5 of this enclosure, the DIRNSA/CHCSS supports DISA in the development, certification, and implementation of encryption systems suitable for classified communications over P25 networks.

5. DoD COMPONENT HEADS. The DoD Component heads:

a. Ensure the requirements of this instruction are implemented during the LMR systems acquisition process.

b. Promote acquisition strategies that leverage economies of scale and procurement of P25 interfaces onto existing DoD communications equipment.

c. Establish and maintain an inventory of DoD LMR equipment and systems, in accordance with DoDI 5000.64 (Reference (q)).

d. Properly train users on the operation of DoD LMR equipment and systems that are P25 certified, and the encrypted transmission of sensitive information.

e. Ensure that LMR equipment and systems are incorporated into the DoD Installation Emergency Management Program, in accordance with DoDI 6055.17 (Reference (r)).

f. Ensure that LMR systems support interoperability and secure communications at the base, post, camp, and station level with State, local and tribal LMR users.

6. CJCS. In addition to the responsibilities in section 5 of this enclosure, the CJCS:

a. Ensures the Military Command, Control, Communications, and Computers Executive Board coordinates with the CCMDs to develop frequency management plans for LMR systems supporting installation management activities in HNs.

b. Supports DISA JSC in defining all-DoD interoperability assignments in the 30-50, 138-150, and 380-400 MHz spectrum allocations to be used for contingency, quick-response, inter-Component communications.

c. Represents the DoD with DISA at working groups and forums, including, but not limited to, the TIA P25 User Needs Subcommittee, the National Public Safety Telecommunications Council, and the DoD Public Safety Communications Working Group.

7. CDRUSNORTHCOM AND CDRUSPACOM. In addition to the responsibilities in section 5 of this enclosure and in accordance with the Unified Command Plan (Reference (s)), CDRUSNORTHCOM and CDRUSPACOM:

a. With the support of the CNGB, implement interoperability standards and develop capability requirements for fixed and deployable LMR systems to support interoperability between DoD Components and federal, local, State, and tribal public safety agencies, pursuant to Reference (f) and DoDI 8220.02 (Reference (t)).

b. In coordination with DISA, monitor the progress and issuance of P25 standards and provide guidance to DoD Components within the United States Northern Command and United States Pacific Command areas of responsibility on LMR systems implementation.

c. Support DISA to establish and maintain a list of DoD interfaces for which DoD LMR equipment and systems must be P25 certified.

d. Support DISA in its representation at working groups and forums, including, but not limited to, the TIA P25 User Needs Subcommittee, the National Public Safety Telecommunications Council, and the DoD Public Safety Communications Working Group.

8. CNGB. In addition to the responsibilities in section 5 of this enclosure, the CNGB assists the CDRUSNORTHCOM, the CDRUSPACOM, and the Director, DISA, to implement interoperability standards and develop capability requirements for fixed and deployable LMR systems to support interoperability between DoD Components and federal, local, State, and tribal public safety agencies.

ENCLOSURE 3

PROCEDURES

1. LMR P25 STANDARDS COMPLIANCE

a. The initial DoD P25 interfaces are the P25 Common Air Interface (CAI) and the Inter-Subsystem Interface (ISSI).

b. DoD Components will ensure that LMR base stations, repeaters, subscriber units, and any LMR support devices are P25 certified for ~~all~~ DoD P25 interfaces prior to procurement or use. Certification information, including Compliance Assessment Program (CAP) test results and the Supplier's Declaration of Compliance (SDoC), may be found on the Department of Homeland Security's Responder Knowledge Base (RKB) ~~Website~~ or its replacement.

2. CYBERSECURITY

a. FIPS-Validated Cryptography

(1) For unclassified but sensitive operations, all cryptographic operations will be implemented in validated module as specified in Reference (l). Symmetric encryption will use 256-bit advanced encryption standard (AES) encryption certified as compliant with Reference (m). Asymmetric cryptography will use public key infrastructure cross certified with the Federal Bridge at Medium assurance or higher.

(2) For classified operations, all LMR systems will be implemented using NSA-approved cryptography.

(3) AES implementations will support the output feedback mode for block encryption of digital communications as specified in Reference (n).

(4) If OTAR is employed, radios will authenticate key messages using AES with cipher-based message authentication code defined in NIST SP 800-38B (Reference (u)).

b. Key Management

(1) For unclassified operations, DoD Components will implement Component-specific written procedures for distributing LMR keys that they obtain from designated authorities, when encryption is required to support joint operations and interoperability exercises.

(2) For classified operations, key management will be completed as approved by NSA.

3. INTEROPERABILITY STANDARDS FOR FIXED AND DEPLOYABLE LMR SYSTEMS. DoD Components will ensure that communications systems that include LMR equipment are in compliance with the interoperability standards for fixed and deployable LMR systems developed by the CDRUSNORTHCOM and CDRUSPACOM as described in paragraph 6a of Enclosure 2.

4. SPECTRUM SUPPORTABILITY. DoD Components will ensure spectrum supportability before acquiring or modifying LMR systems, in accordance with Reference (p).

5. WAVEFORM MODIFICATIONS. If a DoD Component intends to modify LMR system waveforms, the Component will submit a waveform application in accordance with procedures stated in DoDI 4630.09 (Reference (v)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AES	Advanced Encryption Standard <i>advanced encryption standard</i>
CAI	Common Air Interface
CAP	Compliance Assessment Program
CCMD	Combatant Command
CDRUSNORTHCOM	Commander, United States Northern Command
CDRUSPACOM	Commander, United States Pacific Command
CIO DoD	Chief Information Office of the Department of Defense
CJCS	Chairman of the Joint Chiefs of Staff
CNGB	Chief, National Guard Bureau
CTCSS	Continuous Tone Coded Squelch System
DCS	Digital Coded Squelch
DES	data encryption standard
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DoDD	DoD Directive
DoDI	DoD Instruction
FIPS	Federal Information Processing Standards
FM	frequency modulation
HN	host nation
ISSI	Inter-Subsystem Interface
JSC	Joint Spectrum Center
LMR	land mobile radio
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NTIA	National Telecommunications and Information Administration
OTAR	over-the-air-rekeying
OTAZ	over-the-air-zeroization
P25	Project 25
RKB	responder knowledge base <i>Responder Knowledge Base</i>
RF	radio frequency
SDoC	supplier's declaration of compliance
TIA	Telecommunications Industry Association
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
US&P	United States and Possessions
VOIP	Voice over IP <i>Internet Protocol</i>

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this instruction.

installation management activities. Utilities (e.g., electric, water, telephone), physical security, personnel security, transportation, emergency services (including fire), medical services, recreation, and waste management.

LMR. A wireless line-of-sight, handheld, or vehicular communications systems providing netted conventional two-way or trunked, voice and data communications intended for both emergency and non-emergency end users. The system can be either internal or external to DoD, interfacing with public switched telephone network or interfacing with cellular telephone networks.

LMR equipment. One or more devices that are currently employed or intended for use in an LMR system, which includes reconfigurable radio equipment that can support both LMR and non-LMR functionality such as tactical radios that can operate both P25 and other waveforms.

LMR system. A regularly interacting group of base, mobile and associated control and fixed relay stations intended to provide ~~land mobile radio~~ *LMR* communications service over a single area of operation in accordance with section 90.7 of Title 47, Code of Federal Regulations

(Reference (w)). LMR can include at least two subscriber units and typically also includes one or more base stations or repeaters, and console operator positions. The system may also include computers to support configuration and management of devices and related interfaces.

P25-certified. Equipment is P25- certified for a particular P25 interface standard if the LMR equipment manufacturer has published its SDoC on the Department of Homeland Security RKB ~~w~~Website (or its replacement), or has successfully completed testing under the CAP using the corresponding conformance and interoperability test procedures for that interface.