



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

January 30, 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 08-039 – Commercial Wireless
Metropolitan Area Network (WMAN) Systems and Technologies

References: See Attachment 1

Purpose. This DTM establishes policy for the acquisition, implementation, and operation of Institute of Electrical and Electronics Engineers (IEEE) 802.16-based wireless technologies. It focuses primarily on ensuring that appropriate security controls are applied to DoD-owned and -operated WMANs implemented in tactical environments. Specifically, this DTM addresses the use of WMAN technologies, based on the current IEEE Standard 802.16, that are modified to meet DoD requirements. The current IEEE 802.16 body of standards includes amendments IEEE Std 802.16-2004 (formerly 802.16d) and IEEE 802.16e-2005 (formerly 802.16e). This DTM is effective immediately; it incorporates and cancels Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Memorandum (Reference (a)) and shall be converted to a DoD Instruction within 180 days.

Applicability. This DTM:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).


b. Does not supersede the authority for the Intelligence Community (IC) or Office of the Director of National Intelligence to implement policy or authority with purview over Secure Compartmented Information communications.

Policy. See Attachment 2.

Responsibilities. See Attachment 3.

Procedures. See Attachment 4.

Releasability. This DTM is approved for public release and is available on the Internet from the DoD Issuances Web Site at <http://www.dtic.mil/whs/directives>.


John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Attachments:

1. References
 2. Policy
 3. Responsibilities
 4. Procedures
- Glossary

ATTACHMENT 1

REFERENCES

- (a) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "DoD Moratorium on Advanced Wireless Services (AWS) in the 3.4-3.65 GHz Frequency Band," February 26, 2007 (hereby canceled)
- (b) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
- (c) DoD Instruction 6055.11, "Protection of DoD Personnel from Exposure to Radiofrequency Radiation and Military Exempt Lasers," February 21, 1995
- (d) Committee on National Security Systems Policy 300, "National Policy on Control of Compromising Emanations," April 10, 2004
- (e) DoD Regulation 5200.08-R, "Physical Security Program," April 9, 2007
- (f) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- (g) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
- (h) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
- (i) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (j) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- (k) Committee on National Security Systems Policy, 15 Fact Sheet No.1, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," June 30, 2003
- (l) DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009
- (m) DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004
- (n) DoD Instruction 4630.09, "Wireless Communications Waveform Development and Management," November 3, 2008
- (o) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004

ATTACHMENT 2

POLICY

It is DoD policy that:

a. For tactical environments, WMAN systems shall implement:

(1) Strong identification and authentication (i.e., two factors, at a minimum) at the device and network levels.

(2) End-to-end protection of data-in-transit by implementing validated encryption, in accordance with paragraph 1 of Attachment 4.

(3) Federal Information Processing Standards (FIPS) validated encryption that ensures message confidentiality, or a cryptographic hashing function that ensures message authenticity for radio management and control frames, in accordance with paragraph 1 of Attachment 4.

(4) Transmission security (TRANSEC) vulnerability mitigation techniques that limit the risks of signal exploitation, in accordance with paragraph 2 of Attachment 4.

(5) The capability to actively screen for unauthorized WMAN devices, in accordance with paragraph 3 of Attachment 4.

b. For all non-tactical WMAN systems and technologies, DoD Components shall ensure compliance with existing commercial wireless policy, per DoD Directive (DoDD) 8100.02 (Reference (b)). Non-tactical WMAN systems that are subsequently repurposed and deployed for use in tactical environments must be made fully compliant with paragraphs a.(1) through a.(5) of this attachment. Conversely, tactical WMAN systems that are subsequently repurposed and deployed for use in non-tactical environments must be made fully compliant with existing commercial wireless policy, per Reference (b).

c. All WMAN usage in the 3.30-3.65 gigahertz (GHz) spectrum band shall be prohibited due to potential interference issues. Exceptions will be evaluated in accordance with paragraph 4 of Attachment 4.

d. All WMAN equipment shall comply with all applicable human exposure to radio frequency (RF) safety standards, in accordance with DoD Instruction (DoDI) 6055.11 (Reference (c)).

e. All WMAN equipment shall comply with all applicable TEMPEST standards for national policy on compromising emanations, in accordance with Committee on National Security Systems Policy (CNSSP) 300 (Reference (d)).

ATTACHMENT 3

RESPONSIBILITIES

1. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO, in addition to the responsibilities in paragraph 6 of this attachment, shall:

a. Monitor and provide oversight and policy development for all DoD WMAN activities.

b. Coordinate with the Under Secretary of Defense for Intelligence (USD(I)) to establish a coordination process with the IC Chief Information Officer and Security Officer to ensure proper protection of IC information in implementing this DTM. Coordinate with the USD(I) Security Directorate where wireless devices or networks impact physical security equipment, active or passive systems, technologies, and devices, as described in DoD 5200.08-R (Reference (e)).

c. Assess potential architectures. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics, to ensure that DoD acquisition systems and processes of WMAN systems are clear and understandable. Address acquisition in accordance with DoDD 5000.01 and DoDI 5000.02 (References (f) and (g)).

d. Identify common spectrum band for WMAN use that permits joint operations, in coordination with the Defense Spectrum Organization.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO and in addition to the responsibilities in paragraph 6 of this attachment, shall:

a. Incorporate WMAN in its DoD-wide information assurance (IA) initiatives such as computer emergency response and vulnerability alerting.

b. Ensure that WMAN capabilities are appropriately integrated into the Defense Information Systems Network.

c. Develop security technical implementation guide on WMAN.

d. Ensure that standards cited in this DTM are maintained current in the DoD IT Standards Registry.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in paragraph 6 of this attachment, shall provide intelligence support and guidance on the use of WMAN technologies for DIA-accredited sensitive compartmented information facilities.

4. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in paragraph 6 of this attachment, shall include assessment of WMAN information system (IS) security practices while conducting regular inspections of DoD contractors processing classified information, in accordance with DoD 5220.22-M (Reference (h)).

5. DIRECTOR, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE (NSA/CSS). The Director, NSA/CSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in paragraph 6 of this attachment, shall:

a. Implement a capability to assess the risks and vulnerabilities associated with WMAN technologies that are responsive to DoD requirements.

b. Develop and disseminate threat information regarding the capabilities and intentions of adversaries to exploit WMAN technologies used by the DoD Components.

c. Conduct research and development in support of IA requirements for WMAN technologies to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. Coordinate these activities with the Director, Defense Research and Engineering.

d. Develop TRANSEC mitigation options.

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Ensure that all new commercial WMAN procurements immediately comply with this DTM. Ensure all entities within their organization and/or under their control that are involved in acquiring (e.g., either developing or procuring) spectrum-dependent (i.e., WMAN) systems:

(1) Seek and conform to guidance from the Military Communications Electronics Board (MCEB) concerning the licensing and use of WMAN systems.

(2) Comply with the evaluation and validation requirements of Enclosure 3 of DoDI 8500.2 (Reference (i)).

(3) Comply with the procedures identified in Attachment 4.

b. In accordance with Reference (i) and DoDI 8510.01 (Reference (j)):

(1) Control WMAN access to ISs under their cognizance to ensure that the WMAN systems (including external interfaces to commercial WMAN services) do not introduce WMAN vulnerabilities that undermine the assurance of the other interconnected systems.

(2) Include intrusion detection methodologies for the WMAN systems.

(3) Incorporate WMAN topics into annual IA training.

(4) Review risk assessment results to make an informed decision about the risk before granting an exception to this policy, in accordance with paragraph 5 of Attachment 4.

c. Using NSA developed options (see paragraph 5.d. of this attachment), conduct a comprehensive TRANSEC vulnerability analysis for tactical environments, and implement TRANSEC vulnerability mitigation techniques in accordance with paragraph 2 of Attachment 4.

d. Conduct a comprehensive TEMPEST vulnerability analysis for tactical and non-tactical environments, and develop mitigation techniques that limit the risks of compromising emanations, in accordance with paragraph 3 of Attachment 4.

7. COMMANDER, U.S. STRATEGIC COMMAND (CDRUSSTRATCOM).

CDRUSSTRATCOM shall, in addition to the responsibilities in paragraph 6 of this attachment, develop defensive actions necessary to detect, deter, or defeat unauthorized WMAN activity up to and including computer network attacks against DoD computer networks and to minimize impact from such activities.

ATTACHMENT 4

PROCEDURES

1. DUAL-LAYER DATA-IN-TRANSIT ENCRYPTION. WMAN systems used in the tactical environment represent NSS; therefore, the implementation of advanced encryption standards (AEs) in WMAN systems must be reviewed and certified by NSA prior to acquisition and use, in accordance with CNSSP 15 (Reference (k)).

a. For WMAN systems that store, process, or transmit unclassified information, make the following determinations regarding the use of International Organization for Standardization (ISO) open systems interconnect (OSI) Layer 2 and Layer 3 encryption:

(1) Whenever possible, FIPS 140 validated IEEE 802.16e-2005 Security SubLayer AES-CCM encryption (based on IETF RFC 3610) shall be provided to protect ISO OSI Layer 2 radio data frames. If not available, then another FIPS 140 validated and NSA certified AES encryption mechanism shall be provided to protect ISO OSI Layer 2 radio data frames.

(2) Implement FIPS 140 validated and NSA certified overlay AES encryption at ISO OSI Layer 3 to protect data packets.

b. For WMAN systems that store, process, or transmit classified information:

(1) Whenever possible, FIPS 140 validated IEEE 802.16e-2005 Security Sublayer AES-CCM encryption shall be provided to protect ISO OSI Layer 2 radio data frames. If this is not available, then another FIPS 140 validated or NSA certified encryption mechanism shall be provided that protects ISO OSI Layer 2 radio data frames.

(2) Implement NSA Type 1 certified High Assurance Internet Protocol Encryptor (HAIPE), other NSA Type 1 certified, or NSA approved Suite B overlay encryption at ISO OSI Layer 3 to protect data packets.

2. TRANSEC VULNERABILITY ANALYSIS

a. DoD Components shall evaluate TRANSEC vulnerabilities mitigation options developed and maintained by the NSA. DoD Components shall select and implement the appropriate TRANSEC vulnerabilities mitigation techniques. Evaluations will be conducted to determine whether the system requires a low probability of exploitation (LPE) for the signal in space. If LPE is required, mitigation techniques such as spreading, transmission flow security, frequency hopping, or emulation by dynamic spectrum access techniques shall be used.

b. Designated accrediting authorities (DAAs) shall approve and document the comprehensive TRANSEC vulnerability analysis during the DoD Information Assurance

Certification and Accreditation Process (DIACAP) certification and accreditation of the system, in accordance with Reference (j).

3. ACTIVELY SCREENING FOR UNAUTHORIZED WIRELESS. DoD Components shall monitor their WMAN systems within all areas where WMAN coverage exists, to detect and prevent unauthorized access, jamming, or electromagnetic interference.

a. Screening shall be periodically performed to ensure compliance with ongoing accreditation agreement in accordance with References (b) and (j).

b. Reporting of unauthorized access, jamming, or electromagnetic interference identified during active electromagnetic sensing shall be appropriately handled and integrated into existing computer or network incident response process and plans.

c. WMAN coverage areas shall be constrained to the extent possible to the area(s) in which the WMAN is intended for use.

d. DoD Components shall establish standard operating procedures to address intrusion, jamming, or electromagnetic interference, when detected.

e. The WMAN's coverage area shall be appropriately sized during RF design and initial implementation.

4. WMAN SPECTRUM SUPPORTABILITY. DoD Components shall assure spectrum supportability prior to acquiring spectrum-dependent WMAN systems in accordance with DoDD 4650.1 (Reference (l)), and ensure compliance with the DoD Electromagnetic Environmental Effects Program in accordance with DoDD 3222.3 (Reference (m)).

5. INDUSTRY STANDARD WAVEFORM MODIFICATIONS. To ensure system and network interoperability, communications waveforms that are not in full compliance with Industry standards shall be subject to review and assessment by ASD(NII)/DoD CIO. Waveform development and modifications (such as spectrum, power output level, symbol, throughput modulation, or coding modifications) must be submitted for review and assessment in accordance with the procedures specified in DoDI 4630.09 (Reference (n)).

6. WMAN SECURITY EXCEPTIONS. In instances where WMAN devices, systems, or technologies cannot be used in accordance with this DTM due to unavailable technology solutions, DAAs are authorized to grant exceptions. The exception must be documented and made available during the DIACAP certification and accreditation of the system in accordance with Reference (j).

7. WMAN BACKHAUL EXCEPTIONS. WMAN technologies that are deployed solely to establish backhaul or site-to-site connectivity (links that are not used at the edge of the network and therefore do not directly interconnect with user devices) via point-to-point or point-to-multipoint links are exempt from the standards set forth in this DTM. DoD Components shall acknowledge that these links must be protected in accordance with Reference (b) and protect backhaul data-in-transit with FIPS 140 validated encryption modules for unclassified information, or NSA Type 1 certified HAIPE encryption for classified information.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CDRUSSTRATCOM	Commander, United States Strategic Command
DAA	designated accrediting authority
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
FIPS	Federal Information Processing Standards (FIPS) 140-2, May 2001
GHz	gigahertz
GIG	Global Information Grid
HAIPE	High Assurance Internet Protocol Encryptor
IA	information assurance
IC	Intelligence Community
IEEE	Institute of Electrical and Electronics Engineers
IEEE Std. 802.16-2004 (formerly 802.16d)	IEEE WiMAX Standard/ETSI HIPERMAN Air Interface for Fixed Broadband Wireless Access Systems
IEEE Std. 802.16e-2005 (formerly 802.16e)	IEEE WiMAX Standard/Mobile WiMAX Air Interface for Fixed and Mobile Broadband Wireless Access Systems.
IEEE Std. 802.20-2008	IEEE Standard for Local and Metropolitan Area Networks Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility
IETF	Internet Engineering Task Force
IETF RFC 3610	Counter with CBC-MAC (CCM), September, 2003

IP	Internet Protocol
IS	information system
ISO	International Organization for Standardization
JSIR	Joint Spectrum Interference Resolution
Km/h	kilometers per hour
LPE	low probability of exploitation
MCEB	Military Communications Electronic Board
NSA/CSS	National Security Agency/Central Security Service
NSS	national security systems
OSI	open systems interconnection
RF	radio frequency
RFC	request for comments
TRANSEC	transmission security
USD(I)	Under Secretary of Defense for Intelligence
WiMAX	Worldwide Interoperability for Microwave Access
WMAN	Wireless Metropolitan Area Network(s)

PART II. DEFINITIONS

Unless otherwise noted, the following terms and their definitions are for the purpose of this DTM.

AES-CCM. An encryption algorithm that utilizes the 128-bit block ciphers to provide authentication and privacy.

backhaul communications. The transmitting of information from a remote site or network to a central network or main site.

defense-in-depth IA. A multiple layer security approach that ensures the confidentiality, integrity, and availability of a network and its resources.

IEEE 802.16. A body of standards established by the IEEE to facilitate point to multipoint broadband wireless transmission. The 802.16 body of standards is comprised of multiple sub groups (e.g., a/b/c/d/e/f/g/k/m) that supports line of sight, non-line of sight, and quality of service. It operates in the 2-11 GHz spectrum.

IEEE 802.20. An IEEE standard for the deployment of mobile broadband wireless access networks. The 802.20 standard was designed to provide a packet based air interface for the wireless transportation of IP-based traffic, in licensed bands > 3.5GHz, to mobile users at vehicular speeds of up to 250 Km/h.

interoperability. Defined in DoDD 4630.05 (Reference (o)).

overlay encryption. A defense-in-depth approach that utilizes a combination of various types of encryption techniques. It is referred to as “overlay encryption” because it does not operate as part of the underlying radio system. Overlay encryption systems are external to the radio equipment, and typically include two or more hardware devices that provide bulk network data traffic encryption and decryption. Overlay bulk encryption devices will encrypt the network data stream prior to its being transmitted by the radio system, and decrypt the network data stream after it has been received by the radio system.

point-to-multipoint. Communication achieved from a singular point to multiple points.

point-to-point: Communication achieved from a singular point to one other singular point.

strong authentication. A method used to secure computer systems, and/or networks by verifying a user’s identity by requiring two factors in order to authenticate (something you know, something you are, or something you have).

tactical environment. Environments where military actions, battles, and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities in this environment focus on the ordered arrangement and maneuver of combat elements in relation to each other, and to the enemy, to achieve combat objectives.

transmission flow security. The measures taken to prevent an adversary from deriving indications and warnings by monitoring activity on a channel.

WiBRO. A IEEE 802.16e-based wireless broadband technology developed by the South Korean telecommunications industry.

WiMAX. A standards-based technology that has been independently certified for interoperability by the WiMAX Forum, enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL. It is a technology based on IEEE standards 802.16-2004 (formerly 802.16d) and/or 802.16e-2005 (formerly 802.16e). WiMAX technology implies

that a product based on these standards has passed WiMAX Forum interoperability testing and is listed in the WiMAX Forum Certified product list.

WMAN. A wireless network that spans a geographical area the size of a small city or village (a single radio can cover a span of approximately 5 kilometers).

WMAN technologies. Wireless technologies categorized as WMANs include IEEE 802.16 standards and a body of addendums (also known as WiMAX), WiBRO, IEEE 802.20 Mobile Wireless Broadband Access, and other proprietary microwave technologies. WMAN technologies can be configured in either point-to-point or point-to-multipoint configurations. WMANs can be used as backhaul technologies interconnecting segments of the network at the distribution layer, or provide end-user connectivity working at the network edge. While WMAN technologies can be used as backhaul technologies, this DTM focuses on their use for providing end-user connectivity.