Department of Defense
DIRECTIVE

NUMBER 8100.*0*2
April 14, 2004
Certified Current as of April 23, 2007

ASD(NII)

SUBJECT: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

References: (a) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(b) Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 18, 2002[1]
(c) Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 5, 1999[1]
(d) DoD Directive 8500.*0*1*E*, "Information Assurance (IA)," October 24, 2002
(e) through (m), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG) (reference (a)). Hereafter, the term "wireless" means commercial wireless devices, services, and technologies.

1.2. Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense.

1.3. Promotes joint interoperability using open standards throughout the Department of Defense for commercial wireless services, devices, and technological implementations.

[1] Limited Distribution. Contact the Office of the Intelligence Community Chief Information Officer.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of 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").

2.2. Applies to all DoD personnel, contractors, and visitors that enter DoD facilities or that have access to DoD information.

2.3. Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of the DoD GIG, or as part of DoD non-GIG Information Technology (IT) (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and Portable Electronic Devices (PED) such as laptop computers with wireless capability, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDA), and any other commercial wireless devices capable of storing, processing, or transmitting information.

2.4. Does not apply to Information Systems (IS) and/or Sensitive Compartmented Information Facilities (SCIF) to which Director of Central Intelligence Directive (DCID) 6/9 (reference (b)) and DCID 6/3 (reference (c)) apply; i.e., Sensitive Compartmented Information (SCI) and special access programs for intelligence under the purview of the Director of Central Intelligence.

2.5. Does not apply to receive-only pagers, Global Positioning System receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems. The detection segment of a PED (e.g., the laser used in optical storage media; between a barcode and a scanner head; or Radio Frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator) does not require encryption.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoD Directive 8500.01E (reference (d)) and DoD Instruction 8500.02 (reference (e)) and be certified and accredited in accordance with DoD Instruction 5200.40 (reference (f)). In addition:

4.1.1. For data, strong authentication, non-repudiation, and personal identification is required for access to a DoD IS in accordance with published DoD policy and procedures. Identification and Authentication (I&A) measures shall be implemented at both the device and network level. I&A of unclassified voice is desirable; voice packets across an Internet protocol (e.g., Voice over Internet Protocol (VoIP)) shall implement I&A in accordance with published DoD policy and procedures.

4.1.2. Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the Designated Approving Authority (DAA) for the wireless connections under their control. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (reference (g)).

4.1.2.1. Encrypting unclassified voice is desirable; voice packets across an Internet protocol (e.g., VoIP) shall use encryption that is validated as meeting FIPS 140-2 requirements.

4.1.2.2. For data at rest, PEDs shall use file encryption that is validated as meeting FIPS 140-2 requirements. Individual exceptions may be granted on a case-by-case basis as determined by the DAA.

4.1.3. Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit written approval of the cognizant DAA. If approved by the DAA, only assured channels employing National Security Agency (NSA)-approved encryption shall be used to transmit classified information. Classified data stored on PEDs must be encrypted using NSA-approved encryption consistent with storage and treatment of classified information.

4.1.4. Measures shall be taken to mitigate denial of service attacks. These measures shall address not only external threats, but potential interference from friendly sources.

4.1.5. Introduction of wireless technologies in DoD ISs, including those creating an external interface to non-DoD systems (or allowing use of DoD wireless devices on non-DoD wireless networks) can have a significant adverse effect on the security posture of the IS and requires security review and documentation in accordance with reference (d).

4.2. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).

4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

4.4. Pursuant to subparagraph 4.1.2., DAAs shall ensure that Wireless Personal Area Network (WPAN) capability is removed or physically disabled from a device unless FIPS PUB 140-2-validated cryptographic modules are implemented (reference (g)). Exceptions may be granted on a case-by-case basis as determined by the DAA.

4.5. The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ongoing accreditation agreement (reference (f)).

4.6. Mobile code shall not be downloaded from non-DoD sources. Downloading of mobile code shall only be allowed from trusted DoD sources over assured channels.

4.7. PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.

4.8. Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data, in accordance with reference (e). The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency.

4.9. The DoD Components shall seek and follow spectrum supportability guidance from the Military Communications-Electronics Board (MCEB) prior to assuming any contractual obligations for the full-scale development, production, procurement, or deployment of spectrum dependent (i.e., wireless) devices or systems, in accordance with DoD Directive 4650.01 (reference (h)).

4.10. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.

4.10.1. The KM process shall be utilized by DAAs to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.

4.10.2. DAAs shall submit alternative mitigating techniques for inclusion in the KM database. The DoD Components shall use the KM process to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices.

4.10.3. Information on vulnerability assessments shall be considered for classification in accordance with DoD 5200.1-R (reference (i)) and handled appropriate to that classification.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer, shall:

5.1.1. Monitor and provide oversight and policy development of all DoD wireless activities.

5.1.2. Establish a formal coordination process with the Intelligence Community (IC) Chief Information Officer (CIO) to ensure proper protection of IC information in implementing this Directive.

5.1.3. Ensure information interoperability of wireless capabilities in support of joint operations in accordance with DoD Directive 4630.05 and DoD Instruction 4630.08 (references (j) and (k)).

5.1.4. Direct the development of acquisition strategies and assess potential architectures (e.g., wireless application frameworks) to minimize costs of wireless development, services and systems, achieve economies of scale, and promote interoperability and security. As necessary, coordinate these activities with the Under Secretary of Defense for Acquisition, Technology, and Logistics.

5.1.5. Direct the development and implementation of a DoD wireless KM process to promote increased sharing of DoD wireless information.

5.1.6. Evaluate and approve specific implementation timelines for compliance of legacy systems to this Directive.

5.1.7. Ensure that the Director, Defense Information Systems Agency, shall:

5.1.7.1. Incorporate wireless considerations in its DoD-wide Information Assurance (IA) initiatives such as computer emergency response, vulnerability alerting, and enterprise anti-virus and file/data store encryption software.

5.1.7.2. Provide analytical and standards support to the DoD Components concerning proper employment of wireless devices.

5.1.7.3. Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.

5.1.7.4. Ensure that wireless capabilities are appropriately integrated into the Defense Information Systems Network.

5.1.7.5. Promote research and development of spectrum-efficient technologies.

5.2. The Under Secretary of Defense for Intelligence shall:

5.2.1. Ensure that the Director, Defense Intelligence Agency, provides intelligence support and guidance on the use of wireless technologies for Defense Intelligence Agency-accredited SCIFs.

5.2.2. Ensure that the Director, Defense Security Service, includes monitoring and assessment of wireless IS security practices while conducting regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (l)).

5.2.3. Ensure that the Director, National Security Agency shall:

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

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

5.2.3.3. Serve as the DoD focal point for IA wireless technologies research and development in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. As necessary, coordinate these activities with the Director, Defense Research and Engineering.

5.3. The OSD Principal Staff Assistants shall:

5.3.1. Ensure end-to-end protection and joint interoperability in their functional areas by guiding investments and other actions relating to wireless technologies.

5.3.2. Ensure wireless requirements for ISs and functional applications developed under their cognizance are fully coordinated at the DoD cross-Component level.

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Develop, coordinate, and promulgate wireless policies and procedures applicable to Joint operations.

5.4.2. Review, confirm, and certify the security and sufficiency of wireless-related interoperability requirements for ISs using wireless capabilities supporting Joint operations.

5.4.3. Ensure the appropriate review and confirmation of the sufficiency of wireless-related interoperability key performance parameters and information exchange requirements for all capstone requirements documents and operational requirements documents.

5.5. The Commander, U.S. Strategic Command, shall develop defensive actions necessary to detect, deter, or defeat unauthorized wireless activity up to and including computer network attacks against DoD computer networks and to minimize impact from such activities.

5.6. The Heads of the DoD Components shall:

5.6.1. Submit to the DoD CIO, within 180 days of this Directive, specific implementation timelines for compliance of legacy systems to this Directive.

5.6.2. Ensure that all new commercial wireless procurements comply with this Directive immediately. 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., wireless) systems:

5.6.2.1. Seek and conform to guidance from the MCEB concerning the licensing and use of wireless systems.

5.6.2.2. Comply with the evaluation and validation requirements of enclosure 3 of reference (e).

5.6.3. Ensure use of the wireless KM process when evaluating potential wireless solutions.

5.6.4. Ensure that activities evaluating wireless technology provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques, and related security procedures.

5.6.5. Ensure that DAAs, in accordance with reference (f):

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

5.6.5.2. Include intrusion detection methodologies for the wireless systems.

5.6.5.3. Incorporate wireless topics into annual IA training.

5.6.5.4. Review risk assessment results to make an informed and affirmative decision about the risk before granting an exception to this policy.

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 8500.02, "Information Assurance (IA) Implementation," February 6, 2003
(f) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997 (supplemented by DoD 8510.1-M, "Application Manual," July 2000)
(g) Federal Information Processing Standard (FIPS) 140-2, May 25, 2001[2]
(h) DoD Directive 4650.01, "*Policy for Management and Use of Electromagnetic Spectrum*," *June 6, 2004*
(i) DoD 5200.1-R, "Information Security Program," January 1997
(j) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology and National Security Systems *(NSS)*," *May 5, 2004*
(k) DoD Instruction 4630.08, "Procedures for Interoperability and Supportability of Information Technology *(IT)* and National Security Systems *(NSS)*," *June 30, 2004*
(l) DoD 5220.22-M, "National Industry Security Program Operating Manual," *February 28, 2006*
(m) Section 11103(a) of title 40, United States Code

[2] Available via internet at http://www.itl.nist.gov/fipspubs/

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality, and data integrity, and employs U.S. Government-approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements for an assured channel carrying unclassified data: Internet Protocol Security, Secure Sockets Layer v3, Transport Layer Security, and Secure Multipurpose Internet Mail Extension. Assured channels for classified data must use an NSA-approved protection mechanism commensurate with the classification level of the data.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

E2.1.3. Commercial Wireless. Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands.

E2.1.4. Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with Committee on National Security Systems-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

E2.1.5. Designated Approving Authority (DAA). The official authorized to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

E2.1.6. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

E2.1.7. End-to-End. IS from the end-user device up to the security border of a DoD network and/or between two user devices connected by a DoD/non-DoD network (to include the wireless infrastructures air interface).

E2.1.8. External Interfaces. Interfaces, including commercial systems (such as a cellular/PCS or pager network not under control of the DAA), capable of carrying traffic between systems under control of the DAA (e.g., the DoD IS and a DoD wireless device).

E2.1.9. Federal Information Processing Standards (FIPS). The standards issued by the National Institute of Standards and Technology for Federal computer systems (http:www.itl.nist.gov/fipspubs/).

E2.1.10. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in 40 U.S.C. 11103(a) (formerly section 5142 of the Clinger-Cohen Act of 1996) (reference (m)).

E2.1.10.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.1.10.1.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.1.10.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.1.10.1.3. Processes data or information for use by other equipment, software, and services.

E2.1.10.2. Non-GIG IT -- Stand-alone, self-contained, or embedded IT that is not or shall not be connected to the enterprise network.

E2.1.11. Heads of the DoD Components. For purposes of this policy guidance, the Heads of the DoD Components include: the Office of the Secretary of Defense Principal Staff Assistants, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies and DoD Field Activities, and the Inspector General of the Department of Defense, and all other organizational entities in the Department of Defense.

E2.1.12. Identification & Authentication (I&A). Process of accepting a claimed identity and establishing the validity of that claimed identity.

E2.1.13. Information Assurance (IA). Measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.14. Information System (IS). The entire infrastructure, organization, personnel, and components used to collect, process, store, transmit, display, disseminate, and dispose of information.

E2.1.15. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by a DoD Component directly or used by a contractor under a contract with the DoD Component that:

E2.1.15.1. Requires the use of such equipment; or

E2.1.15.2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract (reference (a)).

E2.1.16. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.17. Personal Digital Assistant (PDA). A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

E2.1.18. Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

E2.1.19. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.20. Spectrum Supportability. The assessment as to whether the electromagnetic spectrum necessary to support the operation of spectrum-dependent equipment or a spectrum-dependent system during its expected life cycle is, or will be, available (that is, from system development, through development and operational testing, to actual operation in the electromagnetic environment). The assessment of "spectrum supportability" is based upon, at a minimum, receipt of equipment spectrum certification, reasonable assurance of the availability of sufficient frequencies for operation, and consideration of electromagnetic compatibility (EMC).

E2.1.21. Synchronize. The process of communicating with a host or another PED to upload, download, merge, or swap information (Hot-Synch).

E2.1.22. Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.

E2.1.23. Wireless Personal Area Network (WPAN). A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either RF (e.g., Bluetooth) or IR technology.