INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

August 23, 2007

INSPECTOR GENERAL INSTRUCTION 4630.4

WIRELESS LOCAL AREA NETWORK (LAN)

FOREWORD

This Instruction provides the policies, procedures, standards and guidelines for the use of Wireless Local Area Networks on the Department of Defense Office of Inspector General networks and assigns the responsibilities for control and oversight.

The office of primary responsibility is the Information Systems Directorate. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

Stephen D. Wilson
Assistant Inspector General for
Administration and Management

2 Appendices

A. Purpose. This Instruction establishes the Department of Defense Office of Inspector General (DoD OIG) Wireless Local Area Network (LAN) Policy.

B. References. See Appendix A.

C. Applicability and Scope. This Instruction applies to the Offices of Inspector General, the Deputy Inspectors General, the Assistant Inspectors General who report to the Inspector General, the General Counsel, and the Director, Equal Employment Opportunity, hereafter referred to collectively as the OIG Components. This Instruction does not cover mobile computing devices, which may be referred to as personal digital assistants, palm tops, hand-held computers and workstations, web-based enhanced cell phones, two-way pagers, and wireless e-mail devices. Use of these devices is covered in IGDINST 7950.3, *Mobile Computing Devices*, May 3, 2007.

D. Definitions. See Appendix B.

E. Policy

1. Due to the ease with which traffic may be intercepted, OIG employees shall not create, send, or receive sensitive or controlled unclassified information to include For Official Use Only (FOUO) or higher through wireless LANs without approval of the Designated Approving Authority (DAA). All classified data transfers shall be performed only on accredited, classified systems. It is permissible to use a wireless connection to remotely connect (i.e. hotel, home) to the OIG network via the standard OIG Virtual Private Network (VPN) connection. There will be no wireless access points on the OIG networks.

2. If pilot and fielded wireless LANs cannot meet the same security requirements as wired LANs, they shall not be used for the same level of data.

3. The OIG employees do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time. To the extent that employees wish that their private activities remain private, they should avoid using office equipment such as the computer, Internet, or electronic mail (e-mail). By using government office equipment, employees imply their consent to disclosing the contents of any files or information maintained or passed-through government office equipment. By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of wireless information technology is made with the understanding that such use is generally not secure, private, or anonymous.

4. Wireless solutions shall be configured in accordance with references (a) through (e).

5. Wireless LANs must be thoroughly analyzed, tested, and assessed for risk to determine the danger of information interception/monitoring and network intrusion. Therefore, wireless technology is not standard hardware or software until the Chief Information Officer (CIO) establishes it as such in reference (f).

6. No wireless LAN shall be connected in any way to the OIG LAN or Wide Area Network (WAN) or used in a secure facility (Sensitive Compartmented Information Facility, Special Access Program, or Special Access Requirement).

F. Responsibilities

1. The **DAA** shall approve for the OIG any use of wireless LANs. This will include certification of analysis, testing, and risk assessment of the danger of information interception/ monitoring and network intrusion.

2. **Employees** shall:

a. Read, understand, and abide by this policy and its provisions.

b. Access and use wireless LANs only in accordance with established laws, procedures, and guidelines. Those include, but are not limited to, references (a) through (g).

c. Refrain from any practices that might jeopardize, compromise, or render useless any OIG information, system, or network.

d. Not send secure or classified information through any electronic communications system not certified by the DAA.

3. The **Information Systems Directorate (ISD)** shall:

a. Develop security policies, standards, and procedures.

b. Ensure wireless LAN use complies with applicable security laws, guidelines, regulations, and standards, both internal and external. That includes, but is not limited to, public laws and the OIG, the General Services Administration, and the Office of Management and Budget publications.

c. Coordinate the administration of wireless LANs in the OIG and perform the technical analysis, testing, and risk assessment of the danger of information interception/monitoring and network intrusion.

d. Make decisions on and assist employees with security safeguards for wireless LAN use.

e. Perform the duties delegated by the DAA.

4. The **Workforce Relations Division** shall advise and assist management on appropriate administrative action(s) if misuse occurs.

APPENDIX A
REFERENCES

a. DoD Directive 8500.01E, *Information Assurance (IA),* October 24, 2002

b. IGDINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000, with changes 1 and 2

c. DoD Directive 8100.01, *Global Information Grid (GIG) Overarching Policy*, Sept 19, 2002

d. 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

e. DoD Memorandum on the *Pentagon Area Common Information Technology Wireless Security Policy*, Sept 25, 2002

f. IGDINST 7950.2, *Hardware and Software Management Program*, May 3, 2007

g. DoD 5200.1-R, *Information Security Program*, January 1997

APPENDIX B
DEFINITIONS

1. **Chief Information Officer (CIO).** The senior official appointed by the Inspector General who is responsible for developing and implementing information resources management in ways that enhance the OIG mission performance through the effective, economic acquisition and use of information. The CIO is the Assistant Inspector General for Administration and Management.

2. **Designated Approving Authority (DAA).** The official appointed by the Inspector General who has the authority to accept the security safeguards prescribed for an information system. The DAA issues an accreditation statement that records the decision to accept those standards. The DAA is the Director, Information Systems Directorate.

3. **Employee.** An OIG employee or contractor who uses computer hardware or software to perform work-related tasks.

4. **Information Technology.** 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.

5. **Internet.** The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

6. **Local Area Network (LAN).** A system of connected computers utilizing nodes which are processing locations. A node may be a computer or some other device.

7. **Sensitive or Controlled Unclassified Information.** This is information in which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, U.S.C., *The Privacy Act*, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, U.S.C., *The Computer Security Act of 1987*. This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following: For Official Use Only (FOUO), Sensitive but Unclassified (SBU), Drug Enforcement Administration (DEA) Sensitive, DoD Unclassified Controlled Nuclear (DoD UCNI), Sensitive Information (*Computer Security Act of 1987*), and Technical Documents.

8. **Wide Area Network (WAN).** A physical or logical network that provides data communications to a larger number of independent users than are served usually by a local area network (LAN) and is spread usually over a larger geographic area than that of a LAN. Typically, a WAN consists of two or more LANs.

9. **Wireless LAN.** A local area network that uses high frequency radio waves rather than wires to connect between nodes.