DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON, DC 20310-1000

DAMI-CDS

14 January 2008

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Wireless Microphones

1. The purpose of this memorandum is to provide security guidance on the use of wireless microphones for discussion of classified national security information.

2. Wireless is defined in DODD 8100.2 as technology which permits the active transfer of information involving emanations of energy between separated points without physical connection. Currently wireless technologies use infrared (IR), acoustics, Radio Frequency (RF), and optical but, as technology evolves, wireless could include other methods of transmission.

3. National, Department of Defense, and Army Policy specifically require the use of National Security Agency (NSA) approved encryption for the transmission of classified information. These specific references are cited as an enclosure to this memorandum.

4. Wireless microphones are designed to transmit information and do not take into consideration the intended recipient or the classification of the transmitted information. Because of this design, a wireless microphone used to transmit classified information requires an encryption system approved by the National Security Agency.

5. My POC is Mr. Richard Niederkohr, DSN 225-2644 or commercial 703-695-2644, email address is Rick.Niederkohr@us.army.mil

Encl

JAMES H. BONNES
Acting Director, Counterintelligence,
Human Intelligence, Disclosure &
Security Directorate

DIISTRIBUTION:
Administrative Assistant to the Secretary of the Army
CIO/G-6
DISTRIBUTION: (CONT)

DAMI-CDS
SUBJECT: Wireless Microphones

U.S. Army Material Command
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Central (USARCENT)
U.S. Army North (USARNORTH)
U.S. Army South (USARSOUTH)
U.S. Army Europe (USAREUR)
U.S. Army Pacific (USARPAC)
Eighth United States Army (EUSA)
U.S. Army Special Operations Command (USASOC)
Military Surface Deployment and Distribution Command (SDDC)
U.S. Army Space and Missile Defense Command (SMDC)
Director, Army National Guard
U.S. Army Intelligence and Security Command (INSCOM)
U.S. Army Network Command (NETCOM)
U.S. Army Medical Command (MEDCOM)
U.S. Army Criminal Investigation Division Command (CID)
U.S. Army Corps of Engineers (COE)
U.S. Army Test and Evaluation Command (TECOM)
Military District of Washington
U.S. Army Military Academy (USAMA)
U.S. Army Reserve Command (USARC)
U.S. Army Acquisition Support Center
U.S. Army Installation Management Agency (IMA)
902nd Military Intelligence Group

DAMI-CDS
SUBJECT: Wireless Microphones

References:

1. Committee on National System Security (CNSS) Policy No 17, National Information Assurance (IA) Policy on Wireless Capability, August 2005. Paragraph 6 g, requires encryption of National Security Information for transmission to and from wireless devices IAW NSTISSP 11 and FIPS 140-2.

2. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 101, National Policy on Securing Voice Communications, September 1999. In order to improve U.S. communications security, and specifically to reduce the vulnerability of government voice communications to exploitation, it is national policy that:

a. all military voice radio systems be secured;

b. Civil government voice systems, which carry traffic of significant intelligence value, be secured.

3. Department of Defense Directive C 5200.5 - Communications Security, April 1990. Paragraph D2 - Only National Security Agency (NSA) - endorsed COMSEC products and services shall be use to secure classified telecommunications of DoD Components and their contractors.

4. Department of Defense Instruction 8523.AA (DRAFT). Will replace DOD C 5200.5. Paragraph 6.1 - Only National Security Agency/Central Security Service approved COMSEC products and services shall be used to secure classified information.

5. AR 25-2, Information Assurance, October 2007. Paragraph 6-1 requires that classified national security information be protected in transmission by NSA approved cryptography.