



Office, Chief Information Officer/G-6

**DEPARTMENT OF THE ARMY  
OFFICE OF THE SECRETARY OF THE ARMY  
107 ARMY PENTAGON  
WASHINGTON DC 20310-0107**

SAIS-AON

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Guidance for Use of Wireless Technologies on the Tactical Network

1. References: See enclosure.
2. Purpose. This memo establishes Army guidance for use of wireless technologies on the tactical network and identifies constraints on independent procurement of wireless solutions.
3. Scope.
  - a. This guidance applies to collateral classified and unclassified cellular or wireless local area network (WLAN) solutions fielded at tactical echelons to communicate between data devices and specially equipped tactical vehicles, other data devices or command posts. Solutions include, but are not limited to, Institute of Electrical and Electronics Engineers (IEEE) 802 family of standards and/or mobile standard technology (Wi-Fi, Bluetooth, WiMAX, 2G/3G/4G/LTE, etc.). This guidance applies to currently fielded end-user devices that may transition to a wireless or cellular capability in the future (i.e., Nett Warrior).
  - b. This guidance does not apply to tactical and Land Mobile Radios.
4. Guidance.
  - a. Acquisition authorities will obtain spectrum supportability and spectrum supportability risk assessments in accordance with the provisions outlined in Army Regulation (AR) 5-12.
  - b. Army organizations will use the minimum number of wireless configurations consistent with operational efficiency.
  - c. Army organizations will reuse existing approved wireless solutions to the maximum extent possible in order to maintain the Army's risk management framework and enhance interoperability in accordance with DoD Instruction 8510.01. Any proposed new materiel solution shall comply with all statutory and regulatory

SAIS-AON

SUBJECT: Army Guidance for Use of Wireless Technologies on the Tactical Network

requirements necessary to obtain an Authority to Operate (ATO) and to negotiate Authority to Connect (ATC) with all designated systems.

d. Army organizations deploying wireless technologies will implement cybersecurity policies and procedures in accordance with reference f. Wireless intrusion detection systems will be implemented commensurate with the required security posture in accordance with reference j and DISA wireless Security Technical Implementation Guides (STIGs).

e. Army organizations using wireless systems that transmit, receive, process or store National Security Information (NSI) must use encryption standards approved by the National Security Agency (NSA) that are commensurate with the level of information classification as defined in Committee on National Security Systems Policy (CNSSP) 15.

## 5. Responsibilities.

a. Army organizations and activities procuring wireless and cellular solutions should:

(1) Ensure that a spectrum supportability determination has been provided by the Army Spectrum Management Office ([usarmy.meade.hqda-cio-g-6.list.asmo-npe-mgt@mail.mil](mailto:usarmy.meade.hqda-cio-g-6.list.asmo-npe-mgt@mail.mil)). Implementations outside the United States, its territories and possessions will comply with AR 5-12 and Combatant Command requirements.

(2) Assess and authorize all wireless technologies and portable electronic devices (PED) with LAN connectivity in accordance with the same risk management and cybersecurity requirements as wired LAN information systems, by following applicable DISA STIGs and references b through h (for DISA STIGs, see [http://iase.disa.mil/stigs/net\\_perimeter/wireless/Pages/index.aspx](http://iase.disa.mil/stigs/net_perimeter/wireless/Pages/index.aspx)).

(3) Ensure that analysis, communications security (COMSEC) monitoring, testing and risk assessments are conducted to determine the risks associated with potential information intercepts or monitoring, TEMPEST emanations, hazards of electromagnetic radiation to ordnance (HERO), and network vulnerability consistent with the minimum information assurance requirements outlined in the references.

(4) Control, monitor and protect wireless access in accordance with applicable regulations.

(5) Fulfill their system needs by purchasing DISA Approved Products List items. Exceptions must be approved by the Chief Information Officer/G-6 (CIO/G-6).

SAIS-AON

SUBJECT: Army Guidance for Use of Wireless Technologies on the Tactical Network

(6) Coordinate with the CIO/G-6 Cybersecurity Directorate for implementation of a National Security Agency commercial solution for classified capability. Liaison with the NSA will be conducted in coordination with CIO/G-6.

b. The Army CIO/G-6 will:

(1) Serve as the certification and accreditation authorizing official (AO) for wireless technologies for the Army tactical network, unless delegated.

(2) Establish a standard approval and implementation process in coordination with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)).

(3) Enforce spectrum management and electromagnetic interference resolution policies in accordance with AR 5-12.

(4) Review the development of specific training and certification requirements for operators and users of tactical wireless solutions.

c. ASA(ALT) should:

(1) Develop system architectures that maintain or enhance interoperability and ensure a common security posture by aligning non-standard wireless communications requirements with existing security architectures and certified configurations to the maximum extent practicable. Deviations from existing architectures or configurations will be coordinated with G-3/5/7 and CIO/G-6 prior to any procurement activity.

(2) Assist programs of record with development of fielding and sustainment funding strategies for any program that is considering implementing a wireless solution.

d. HQDA G-3/5/7 should:

(1) Perform cross-functional coordination, synchronization and integration of requirements, in accordance with Army priorities and senior leader guidance.

(2) Facilitate fielding and training of commercial wireless technologies.

e. HQDA G-2 should:

(1) Provide policy and guidance on the use of Sensitive Compartmented Information (SCI) wireless technologies in an Army-accredited SCI facility (SCIF).

(2) Serve as the AO for all wireless systems within an Army SCIF.

SAIS-AON

SUBJECT: Army Guidance for Use of Wireless Technologies on the Tactical Network

f. Commander, Second Army will:

(1) Develop standards for intrusion detection and intrusion prevention for Army wireless LANs on the tactical network in accordance with AR 25-2.

(2) Enforce and support specifications to support interoperability and net-readiness testing.

(3) Review and recommend updates to DISA STIGs.

6. Policy Review. Within 12 months of this publication, the CIO/G-6 will develop a comprehensive wireless policy to be integrated into the appropriate Army Regulation or Department of the Army Pamphlet.

7. The Army Spectrum Management Office point of contact for spectrum supportability is Ms. Sarah Bauer: (301) 225-3762 or [usarmy.meade.hqda-cio-g-6.list.asmo-npe-mgt@mail.mil](mailto:usarmy.meade.hqda-cio-g-6.list.asmo-npe-mgt@mail.mil).

8. The CIO/G-6 point of contact for this policy is Mr. David J. Davis: (571) 256-8988 or [david.j.davis18.civ@mail.mil](mailto:david.j.davis18.civ@mail.mil).

ROBERT S. FERRELL  
Lieutenant General, GS  
Chief Information Officer/G-6

**DISTRIBUTION:**

Principal Officials of Headquarters, Department of the Army  
Commander

- U.S. Army Forces Command
  - U.S. Army Training and Doctrine Command
  - U.S. Army Materiel Command
  - U.S. Army Pacific
  - U.S. Army Europe
  - U.S. Army Central
  - U.S. Army North
  - U.S. Army South
  - U.S. Army Africa/Southern European Task Force
  - U.S. Army Special Operations Command
- (CONT)

SAIS-AON

SUBJECT: Army Guidance for Use of Wireless Technologies on the Tactical Network

DISTRIBUTION (CONT):

Military Surface Deployment and Distribution Command  
U.S. Army Space and Missile Defense Command/Army Strategic Command  
U.S. Army Medical Command  
U.S. Army Intelligence and Security Command  
U.S. Army Criminal Investigation Command  
U.S. Army Corps of Engineers  
U.S. Army Military District of Washington  
U.S. Army Test and Evaluation Command  
U.S. Army Installation Management Command  
Superintendent, United States Military Academy  
Director, U.S. Army Acquisition Support Center  
Executive Director, Arlington National Cemetery  
Commander, U.S. Army Accessions Support Brigade  
Commandant, U.S. Army War College  
Commander, Second Army

CF:

Director, Army National Guard  
Director of Business Transformation  
Commander, Eighth Army