Committee on National Security Systems

CNSS Policy No. 17
August 2005

National Information Assurance (IA) Policy on Wireless Capabilities

This document prescribes minimum standards. Your department or agency may require further implementation.

CNSS Policy No. 17
August 2005

CHAIR

FOREWORD

1. Wireless capabilities (devices, services, technologies, and networks) have become important elements of the Federal Government's information infrastructure, and are now virtually indistinguishable from the wired segment of that infrastructure. Individuals at all levels within the Federal Government routinely use wireless capabilities to conduct their daily business in support of mission operations. The mobility afforded by wireless capabilities supports increased productivity and connectivity, and the Federal community has responded by deploying these capabilities widely across the Enterprise. However, the advantages that result from the implementation of wireless capabilities also introduce additional risks to information systems and the operations they support. Consequently, the implementation of wireless capabilities or the use of wireless devices within national security systems (NSS), and/or within environments where national security information (NSI) is stored, processed, or transmitted, must be governed by a systematic approach that balances operational gains with the inherent risks associated with the use of these capabilities.

2. This policy establishes the controls necessary to implement wireless capabilities within NSS, and the use of wireless devices where NSI is stored, processed or transmitted, while mitigating the effects of their known vulnerabilities and associated risks.

3. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this policy from the Secretariat.

4. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

//s//

Linton Wells II

CNSS Secretariat (I01C) . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL INFORMATION ASSURANCE (IA) POLICY ON WIRELESS CAPABILITIES

SECTION I – SCOPE

1. This policy applies to all Federal Government departments, agencies, and employees, contractors, and visitors that enter Federal Government facilities, that use wireless capabilities to store, process, or transmit national security information (NSI); and/or have wireless devices operating in environments where NSI is stored, processed, or transmitted. Wireless capabilities include voice and data devices, technologies, services, and networks that form part of a Federal leased, procured, acquired, or operated national security system (NSS). Wireless devices and technologies include Portable Electronic Devices (PED), Wireless LANs (WLAN), and any other wireless capability for storing, processing, or transmitting information.

2. This policy does not apply to receive-only devices or medical devices (e.g. hearing aids, pacemakers or other implanted medical devices). In regards to Section 508 of the Rehabilitation Act, as amended (Reference a), compliance of accessibility devices for the wireless environment will be addressed on a case-by-case basis. A risk assessment shall be conducted prior to introducing emergency radios or wireless personal life support systems into a secure environment.

3. Nothing in this policy should be interpreted as altering or superseding the existing authorities of the Director of National Intelligence.

SECTION II – REFERENCES

4. Referenced documents are listed in Annex A.

SECTION III – DEFINITIONS

5. Definitions in CNSS Instruction No. 4009 (Reference b) apply to this policy. Additional terms are defined in Annex B.

SECTION IV – POLICY

6. Federal Government departments and agencies that use wireless capabilities to store, process, or transmit NSI shall establish a wireless Information Assurance (IA) program that:

a. Establishes responsibilities for control and oversight for the implementation of wireless capabilities within their IA program.

b. Ensures the implementation of wireless information systems meet the same security certification/recertification and accreditation/reaccreditation requirements as wired information systems in accordance with (IAW) Reference c., to include threat, vulnerability, and risk assessment.

c. Requires integrity and non-repudiation controls on wireless information systems IAW Reference c.

d. Implements identification and authentication (I&A) measures for both the wireless device and wireless network IAW Reference c.

e. Controls the implementation of wireless capabilities used for storing, processing, or transmitting NSI.

f. Prohibits the use of wireless functionality while physically connected directly to a wired network unless specifically approved for such operations.

g. Requires encryption of NSI for transmission to and from wireless devices IAW References f and g.

h. Specifies conditions under which wireless devices that store, process, or transmit information are allowed into, and used within, an area where classified and/or sensitive information is discussed or processed.

i. Requires the implementation of a session timeout capability, not to exceed 30 minutes.

j. Considers active (physical and/or electronic) screening for wireless devices where use of wireless capabilities is prohibited.

k. Requires COMSEC monitoring IAW Reference d.

l. Ensures compliance with applicable TEMPEST standards IAW Reference e.

m. Requires that acquisition or procurement of wireless commercial-off-the-shelf (COTS) products comply with published guidance relating to IA/IA-enabled products IAW References f and g.

n. Establishes a process to consider the feasibility and risk of using a wireless system as the sole or principal system for meeting critical or primary mission capabilities.

o. Incorporates security best practices (e.g. Security Technical Implementation Guides [STIGs]) when implementing wireless capabilities.

p. Establishes configuration management and controls for hardware and software life-cycle management of IA within wireless capabilities.

q. Includes an inventory management control plan for new and existing devices, repairable devices, recovery of lost, stolen or destroyed devices, and disposal of devices.

r. Develops and implements a remediation strategy for the inadvertent storage, processing, or transmission of information/data of a higher classification than the device is authorized.

s. Mandates adherence to published department or agency spectrum management and supportability guidance.

t. Incorporates wireless topics into IA training, education, and awareness, as appropriate.

u. Requires a yearly review of existing wireless policies to ensure compliance with this policy.

v. Ensures that legacy systems comply with this policy within eighteen months of its issuance.

w. Ensures that all new acquisitions comply with this policy within six months of its issuance.

7. Federal Government departments and agencies that do not use wireless capabilities to store, process, or transmit NSI, but are likely to have wireless devices operating in environments where NSI is stored, processed, or transmitted, shall establish a wireless IA program that incorporates at a minimum, items f., h., j., k., l., r., s. and t. from paragraph 6 above. The NSS will need to be reviewed IAW Reference c.

SECTION V – RESPONSIBILITIES

8. Heads of Federal departments, agencies, programs, projects, and initiatives for which this policy applies shall:

a. Develop, fund, and manage programs necessary to implement this policy.

b. Ensure that a Designated Approval Authority (DAA) is identified for each system under their operational control, and that DAAs have the ability to influence the application of resources to comply with the objectives of this policy.

Encls:
ANNEX A - References
ANNEX B - Definitions

ANNEX A

REFERENCES

The following documents are referenced in this policy:

a. Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998.

b. CNSSI No. 4009, “National Information Assurance (IA) Glossary,” dated May 2003.

c. NSTISSI No. 1000, "The National Information Assurance Certification and Accreditation Process (NIACAP)," dated April 2000.

d. NTISSD No. 600, “Communications Security (COMSEC) Monitoring” dated 10 April 1990.

e. CNSSP No. 300, “National Policy on Control of Compromising Emanations,” dated April 2004.

f. NSTISSP No. 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,” dated June 2003.

g. Federal Information Processing Standard Publication (FIPS) 140.2, “Security Requirements for Cryptologic Modules,” dated May 25, 2001.

ANNEX B

DEFINITIONS

Terms used in this policy have the following meanings:

a. Identification & Authentication (I&A). The process of accepting a claimed identity and establishing the validity of that claimed identity.

b. Portable Electronic Device (PED). Any non-stationary electronic device with the capability of processing, storing, and/or transmitting information. This definition includes, but is not limited to Blackberry devices, PDAs (with wireless transmit or receive capability), cellular phones, two-way pagers, e-mail devices, wireless keyboards and mice, audio/video recording devices, and hand-held/laptop computers.

c. Wireless. The absence of a physical connection.

d. Wireless Capabilities. Wireless devices, services, technologies, and networks acquired and/or procured to satisfy an operational need.

e. Wireless Device. Hardware that provides wireless capabilities.

f. Wireless Information System. Includes the wireless transmission medium, stationary integrated devices, firmware, supporting services, and protocols.

g. Wireless Technology. A technology that permits the active or passive transfer of information between separated points without physical connection. Active information transfer may entail a transmit and/or receive emanation of energy, whereas passive information transfer entails a receive-only capability. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.