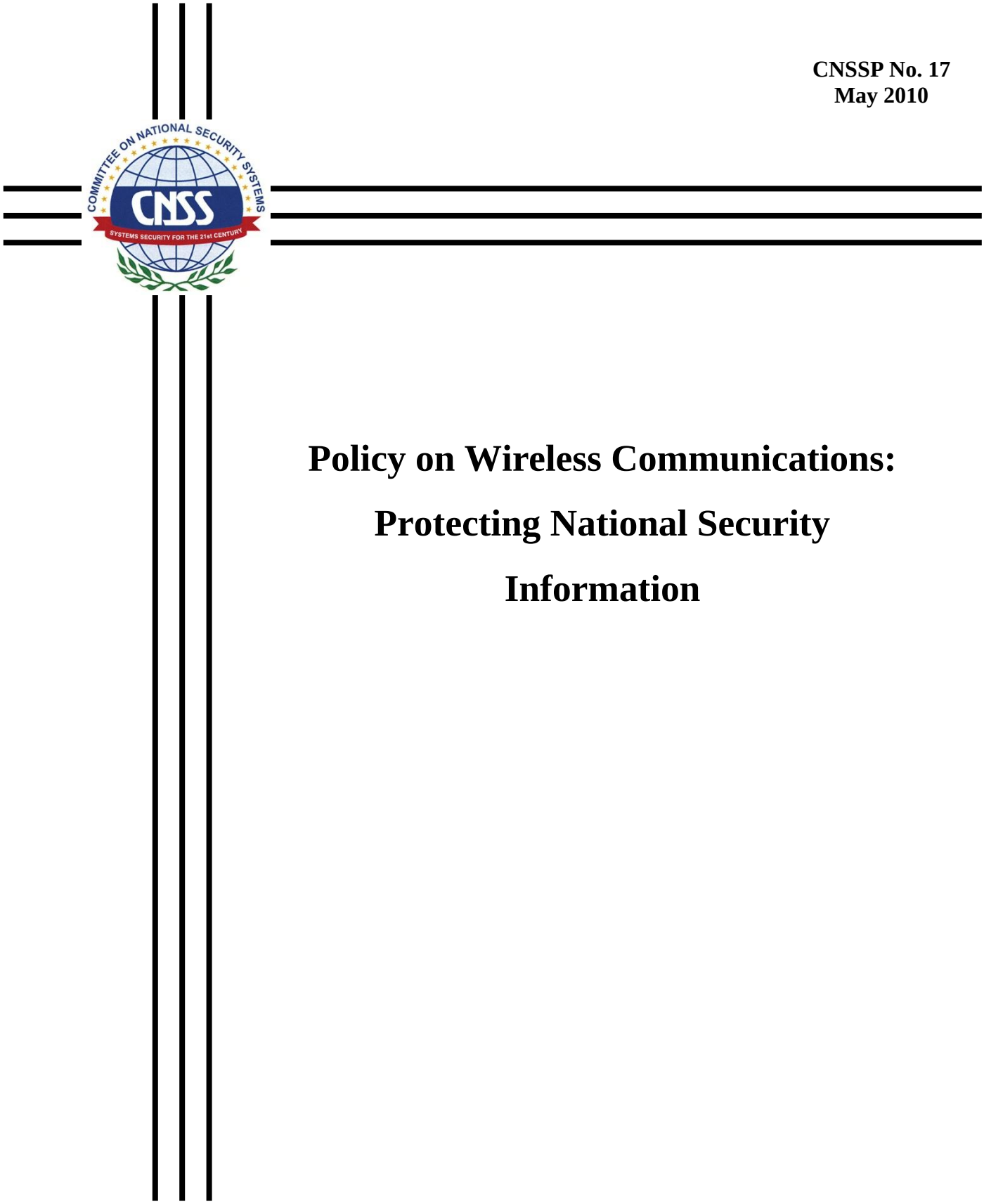
Committee on National Security Systems



CNSSP No. 17
May 2010

Policy on Wireless Communications: Protecting National Security Information

CHAIR

FOREWORD

1. The Committee on National Security Systems (CNSS) is issuing this policy to help agencies better safeguard National Security Information (NSI) during wireless transmission and delivery, while stored on mobile systems, and while stored on fixed systems that can be accessed by wireless media. It addresses the use of wireless technologies in areas where NSI is discussed or processed. It also assigns responsibilities for improving the security posture of the Executive Departments and Agencies (D/A), and provides references for a minimum set of security measures required for the use of wireless technologies in a national security environment.

2. This policy supersedes the Committee on National Security Systems Policy (CNSSP) No. 17, "National Information Assurance (IA) Policy on Wireless Capabilities," August 2005.

3. The heads of D/As are ultimately responsible for protecting NSI that is transmitted, received, processed, or stored using wireless technologies. D/As shall ensure that all wireless national security systems (NSS) and their components, to include new acquisitions, legacy systems, and upgrades, comply with this policy.

4. The CNSS has the authority to request the information and technical support necessary from the heads of D/As to ensure that NSS meet the minimum requirements set forth in this policy, and will review and assess D/A wireless NSS communications programs for compliance. Specifically, the CNSS Secretariat tracks the status of the Member and Observer organizations' implementation of new/revised CNSS Issuances in order to create an Issuance Compliance Report. The Secretariat will oversee and administer this reporting process, which will be initiated six months following approval of this policy.

5. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: www.cnss.gov

//s//
CHERYL J. ROBY

Committee on National Security Systems

CNSSP No. 17

Policy on Wireless Communications:
Protecting National Security Information

SECTION I – SCOPE

1. This policy derives its authority from the National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems* (Reference A) and applicable sections of the Federal Information Security Management Act (FISMA) of 2002 (Reference B)**.**

2. This policy applies to all D/A employees, contractors, and visitors that use or plan to use wireless equipment, software, services, and interdependent technologies in areas where NSI is transmitted, received, processed, or stored. It also applies to the processes that enable the D/As to oversee the planning, design, development, acquisition, implementation, use, control, operation, maintenance, and disposition of existing and future NSS wireless capabilities within their scope of authority. The term D/A shall be interpreted to include Federal bureaus and offices. NSS wireless capabilities include wireless technologies acquired and/or procured to satisfy an operational need.

SECTION II – REFERENCES

3. References for this policy are listed in ANNEX A. Additionally, informational references are provided in ANNEX B to assist D/As in establishing a wireless communications program for NSS or incorporating wireless communications guidelines into an existing NSS program.

SECTION III – DEFINITIONS

4. Terms defined in CNSS Instruction No. 4009: *National Information Assurance Glossary* (Reference C) applies to this policy.

SECTION IV – POLICY

5. The following security controls shall be incorporated into D/A NSS programs where NSI is transmitted, received, processed, or stored using wireless technologies or where wireless technologies are used in the proximity of NSI. In those instances where a D/A NSS program does not exist, the D/A shall establish a wireless NSS program. Wireless controls shall address the complete lifecycle of information technologies consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 Revision 2: *Security Considerations in the System Development Life Cycle* (Reference D). These include the planning, design,

development, acquisition, implementation, use, operation and control, maintenance, and disposition of existing and future wireless capabilities.

a. At a minimum, D/As shall issue policies that include the following management controls:

i. When implementing standalone wireless capabilities for the transmission of NSI, or integrating wireless devices, services, and technologies into existing NSS, D/As shall implement a risk management process that adheres to the guidelines found in CNSS Policy No. 22: *Information Assurance Risk Management Policy for National Security Systems* (Reference E) and the principles set forth in National Security Decision Directive 298: *National Operations Security Program* (Reference F).

ii. The procurement of wireless technologies for the transmission of NSI shall be prohibited unless a risk assessment is completed and accepted (this includes the procurement of wireless technologies for tests, pilots, prototypes, and feasibility studies).

iii. Wireless risk assessments shall address the protection of NSI from the point of origin; during transmission; when received; while processed using wireless hardware and software; while stored on wireless media; and when using a wireless system as the sole or principal system for meeting critical or primary mission essential functions.

iv. A configuration baseline shall be established that defines the organization's minimum requirements for compliance with this policy, and ensures that wireless hardware, firmware, software, and documentation are adequate to protect NSI. In those instances where a D/A has an existing Information Technology Configuration Control Board (ITCCB) for NSS; the ITCCB shall incorporate the wireless requirements referenced above.

v. All information systems that employ wireless technologies used for the transmission, receipt, processing, and storage of NSI shall complete a security control assessment and be granted authorization to operate by the D/A Authorizing Official (AO).

vi. A TEMPEST countermeasure requirements review for the implementation of wireless technologies in the facilities under consideration shall be completed by a Certified TEMPEST Technical Authority (CTTA) in accordance with CNSS Policy No. 300: *National Policy on Control of Compromising Emanations*

(Reference G) and CNSS Instruction No. 7000: *Tempest Countermeasures for Facilities* (Reference H):

1. Prior to acquiring wireless NSS solutions; and

2. On wireless technologies in proximity to where NSI is discussed or processed.

vii. Periodic inspections shall be performed to identify deviations from the D/A-approved configuration baseline of wireless devices located in areas where NSI is discussed or processed, regardless of whether wireless devices are powered on or off, and; all deviations shall be reported to the AO.

viii. Where practicable, wireless technologies shall support interoperability through the adoption of commercially available, standards-based wireless products certified to transmit, receive, process, or store NSI in accordance with the requirements of this policy.

ix. A current inventory of wireless equipment, software, and services used for transmission of NSI shall be maintained.

x. Restrictions for the use of wireless technologies that transmit NSI shall be promulgated throughout the organization.

xi. Basic education, training, and awareness regarding the use of wireless technologies to transmit NSI shall be administered to all D/A managers, technical support personnel, and users of wireless technologies before they can be authorized to operate on wireless NSS. The content of this policy and procedures for its implementation shall be incorporated into training and awareness materials.

xii. The AO or Cognizant Authority can terminate wireless network operations in the event of an emergency or security breach.

b. At a minimum, D/As shall implement the following technical controls:

i. Confidentiality, integrity, and availability controls as well as authentication and non-repudiation measures on wireless information systems, per National Security Telecommunications and Information Systems Security Instruction No. 1000: *National Information Assurance Certification and Accreditation Process* (Reference I) and CNSS Instruction No. 1253: *Security Categorization and Control Selection for National Security Systems* (Reference J).

ii. Authentication employing the Extensible Authentication Protocol (EAP) shall implement cryptographic modules validated under the NIST Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140 (Reference K) and NIST SP 800-120: *Recommendation for EAP Methods Used in Wireless Network Access Authentication* (Reference L) commensurate with the level of risk.

iii. Wireless systems used to transmit, receive, process, or store NSI shall utilize NSA-approved encryption Suite A or Suite B Type 1 standards or NIST FIPS 140 commensurate with the level of information classification as defined in CNSS Policy No. 15: National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (Reference M).

iv. Wireless and wired intrusion detection systems shall be used to monitor for unauthorized access to the network and to detect malicious wireless activities.

v. There shall be configuration controls to govern modifications.

vi. Adherence to applicable TEMPEST standards in accordance with CNSS Policy No. 300 (Reference G) and CNSS Instruction 7000 (Reference H) prior to the acquisition of a wireless technology or solution in an area where NSI information is discussed and/or processed in an adjacent area.

SECTION V – RESPONSIBILITIES

6. Heads of D/As shall:

a. Report compliance with this policy to the CNSS Secretariat on an annual basis.

b. Ensure resource adequacy.

i. Maintain a staff of cleared personnel with current credentials and adequate training to manage wireless NSS programs; and

ii. Sustain a level of funds to adequately operate and maintain wireless NSS capabilities in accordance with this policy.

Encl:
ANNEX A - References
ANNEX B – Best Practices

ANNEX A

References

A. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems,* July 5, 1990.

B. Federal Information Security Management Act of 2002, December 17, 2002.

C. CNSS Instruction No. 4009, *National Information Assurance Glossary,* June 2006.

D. NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.

E. CNSS Policy No. 22, *Information Assurance Risk Management Policy for National Security Systems*, February 2009.

F. National Security Decision Directive 298, *National Operations Security Program,* January 22, 1988.

G. CNSSP No. 300, *National Policy on Control of Compromising Emanations,* April 2004.

H. CNSS Instruction No. 7000, *Tempest Countermeasures for Facilities*, May 2004.

I. National Security Telecommunications and Information Systems Security Instruction No. 1000, *National Information Assurance Certification and Accreditation Process*, April 2000.

J. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.

K. Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

L. NIST SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication,* September 2009.

M. CNSS Policy No. 15, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information,* June 2003.

ANNEX B

Best Practices

Federal guidelines that deal with NSS, but are not specifically addressed in this policy, are included here for informational purposes:

A. CNSS Policy No. 15, Fact Sheet No. 1, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, June 2003.

B. Defense Information Systems Agency, *Wireless Security Technical Implementation Guide Version 6, Release 1*, September 2009.

C. Intelligence Community Policy Memorandum 2005-700-1, Annex D, December 1, 2005.

D. National Institute of Science and Technology Special Publication (NIST SP) 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

E. NIST SP 800-37 Revision 1, DRAFT *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, November 17, 2009.

F. NIST SP 800-39, DRAFT *Managing Risk from Information Systems: An Organizational Perspective*, April 3, 2008.

G. NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

H. NIST SP 800-48 Revision 1, *Guide to Security Legacy IEEE 802.11 Wireless Networks*, July 2008.

I. NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

J. NIST SP 800-63 Revision 1, DRAFT *Electronic Authentication Guideline*, December 12, 2008.

K. NIST SP 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.

L. NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, April 2007.

M. NIST SP 800-121, *Guide to Bluetooth Security*, September 2008.

N. NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008.

O. NIST SP 800-127, DRAFT *Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies*, September 2009.