U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: DR 3505-002
SUBJECT: Wireless Networking Security Policy	DATE: August 11, 2009
	OPI: Office of the Chief Information Officer

1. PURPOSE

a. This policy establishes the requirements for the secure implementation of wireless networking technology within the United States Department of Agriculture (USDA) information systems and data environments. This policy applies to all wireless networking equipment, software and services used for official USDA purposes.

b. This policy does not include wireless devices that do not directly connect to a general support system access point (e.g., Bluetooth, wireless keyboards, wireless mice, personal digital assistant (PDA).)

c. This policy adheres to the guidance identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Appendix F as:

Identifier	Family	Class
AC-1	Access Control	Technical
AC-17	Access Control	Technical

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This regulation supersedes Departmental Manual (DM) 3550-003, Chapter 10, Part 3, "Portable Electronic Devices and Wireless Technology," dated February 8, 2006.

b. USDA Telecommunications Management DR 3300-1-C "Wireless Communications" is still valid.

3. BACKGROUND

a. Wireless networking technology has become part of the evolving business landscape. Wireless networking technologies are increasingly used by USDA employees, customers and business associates in business meetings, while on business travel, in public areas and in USDA locations.

b. Wireless networking technology includes any electronic device capable of receiving, storing or transmitting information using any format (e.g., radio, infrared, network or similar connections) without a permanent or physical link to Federal networks.

4. POLICY

a. Only enterprise-class wireless (see Appendix A - Definitions) network devices will be employed within USDA networks. Consumer-class wireless (see Appendix A - Definitions) network devices are strictly prohibited.

b. Agencies will ensure that all wireless network devices are configured in accordance with applicable Federal Information Processing Standards (FIPS) and NIST Special Publications. (See Appendix C – Authorities and References.)

c. Agencies will implement NIST best practice guidance as outlined in NIST 800-97 "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf) .

d. All wireless networking devices configuration changes will be implemented using the agency's change control process.

e. USDA agencies will adhere to all Departmental IT architectural standards (DR 3100 series) and to the USDA Information Technology System Development Life Cycle Guide (http://www.ocio.usda.gov/e_arch/doc/USDA_SDLC_GUIDEv1.0_011507.pdf).

f. Agencies will maintain an up-to-date inventory of all wireless access points and a current wireless network diagram. A report of the agency's wireless network inventories and diagram will be submitted to the Department's Chief Information Officer (CIO) annually by September 30th, or when changes occur to the agencies network that involve a wireless network.

g. Sensitive but unclassified (SBU) data and personally identifiable information (PII) residing on or transmitted by wireless technology must be encrypted using FIPS 140-2 approved and validated cryptographic algorithms

h. Exceptions that are approved will be interim in nature and expire at the end of each fiscal year. Agencies will submit all policy exception requests directly to the Deputy Chief Information Officer (DCIO) for Policy and Architecture.

5. PROCEDURES AND GUIDANCE

The policies in this regulation establish the overarching framework for wireless technology usage and will be further shaped by other USDA regulations and manuals that contain clarifying procedures. The USDA Departmental regulations and manuals can be found at: http://www.ocio.usda.gov/directives/index.html. For additional procedures and guidance see Appendix C – Authorities and References.

6. RESPONSIBILITIES

a. The DCIO for Policy and Architecture is responsible for:

(1) Establishing policy for security over wireless networks; and

(2) Enforcing the policy through compliance reviews, automated tools, and other means as necessary.

b. Agency CIOs are responsible for:

(1) Implementing this policy within their respective agency and/or office; and

(2) Providing proper evidence of compliance as necessary and upon request.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

Departmental Regulation (DR) 4070-735-001 *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of Computers and Telecommunications Equipment. In addition, Section 21, Disciplinary or Adverse Action, states:

a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.

b. Disciplinary or adverse action will be effected in accordance with applicable law and regulations.

-END-

APPENDIX A

DEFINITIONS

a. Consumer-Class Wireless - A commercial off-the-shelf wireless device that has not been architected as part of a general support system and is not FIPS 140-2 compliant.

b. Enterprise-Class Wireless - A centralized deployment of a wireless network utilizing wireless access points that are FIPS 140-2 compliant and have been architected as part of a general support system.

c. Portable Electronic Device (PED) - Any electronic device that is capable of receiving, storing or transmitting information using any format (e.g., radio, infrared, network or similar connections) without a permanent link to Federal networks. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless email, Web browsing, and Internet access.

d. Wireless Access Point - A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network.

e. Wireless Communication - Anything that supports communications between mobile, portable, or fixed facilities through the use of the electromagnetic spectrum. Examples are: AM and FM broadcasting, UHF and VHF television, satellite, microware, land mobile radio (used for public safety, commercial, and private use), citizen’s band, trunked radio, paging, cellular telephone, wireless Local Area Networks (LANs), wireless telephone PBXs, and Personal Communications Services (PCS).

APPENDIX B

ABBREVIATIONS

CIO	Chief Information Officer
DCIO	Deputy Chief Information Officer
DM	Departmental Manual
DR	Departmental Regulation
FIPS	Federal Information Processing Standard
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PII	Personally Identifiable Information
SBU	Sensitive But Unclassified
SP	Special Publication
USDA	United States Department of Agriculture

APPENDIX C

AUTHORITIES AND REFERENCES

Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

FIPS PUB 140-2 Annex A Draft, *Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, October 2008.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, Rev. 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.

NIST SP 800-53, Revision 3, DRAFT *Recommended Security Controls for Federal Information Systems*, February 2009.[1]

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008.

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

Office of Management and Budget (OMB) M-06-16, *Protection of Sensitive Agency Information*, June 2006.

USDA, DR 3100 Series "Management of Information Resources, Planning, standards, approvals, security, review and evaluation"

USDA, DR 3300-1-C "Wireless Communications," March 23, 1999.

USDA Departmental Regulation (DR) 4070-735-001, "Employee Responsibilities and Conduct," October 4, 2007.

NOTE: The references in this appendix reflect the current guidance as of the writing of this policy. Agencies must employ the most current guidance available.

[1] The current version at the time of issuance.