



United States
Department of Agriculture

Office of the Chief Information Officer

DN 3300-013

**Commercial Wireless Technologies in USDA –
Unclassified Security Requirements for Wireless Devices**



TABLE OF CONTENTS

| | Page |
|--------------------------------------------------|------|
| <u>1</u> <u>PURPOSE</u> | 1 |
| <u>2</u> <u>POLICY</u> | 1 |
| <u>3</u> <u>BACKGROUND</u> | 1 |
| <u>4</u> <u>APPLICABILITY AND SCOPE</u> | 2 |
| <u>5</u> <u>REFERENCES</u> | 2 |
| <u>6</u> <u>DEFINITIONS</u> | 4 |
| <u>7</u> <u>ROLES AND RESPONSIBILITIES</u> | 6 |
| <u>8</u> <u>INQUIRIES</u> | 9 |

DEPARTMENTAL NOTICE

Number:
3300-013

SUBJECT:
Commercial Wireless Technologies in USDA - Unclassified Security
Requirements for Wireless Devices

DATE:
April 20, 2005

OPI: Office of the Chief Information
Officer, Telecommunications Policy
and Planning Division

CODIFICATION/EXPIRATION:
This Notice will expire one year from the date it is signed, unless rescinded or canceled earlier.

PURPOSE



This Departmental Notice (DN) instructs USDA agencies and staff offices to establish processes and procedures for the secure use of wireless devices for data transmission (non-voice). It also requires that processes and procedures be established by agencies and staff offices for the proper management of wireless devices, including conformance to the National Institute of Standards and Technology (NIST) standards.

POLICY



USDA agencies and staff offices will establish baseline processes and procedures for the management and secure use of wireless devices capable of non-voice data transmissions. Agency and staff office processes and procedures must conform to NIST standards in addition to USDA policies for telecommunications training, acquisitions, and asset management. All existing USDA security policies for information technology and telecommunications shall be applied to wireless technologies, which includes wireless devices. Unencrypted analog or digital voice transmissions are vulnerable to interception and should be treated as open, non-secure communications.

BACKGROUND



Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed. Sensitive data may be corrupted during improper synchronization. Malicious entities may deploy unauthorized client devices to surreptitiously gain access to sensitive information. Handheld devices are easily stolen and can reveal sensitive information. Data may be extracted without detection from improperly configured devices. Viruses or other malicious code may corrupt data on a wireless device and subsequently be introduced to a wired network connection. Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities. Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations. Internal attacks may be possible via ad hoc transmissions. [NIST]

Wireless hackers can download access point software onto an unsecured handheld device and masquerade as a legitimate access point. After a client has been hijacked, the device will forward the connection to the hacker's IP address.

USDA agencies and staff offices have requested guidance on how to minimize security risks associated with wireless data communications that could adversely affect their operations and resources. Although this guidance is directed specifically to non-voice, wireless data communications, it is important to note that unencrypted digital voice transmissions are vulnerable to interception and should be treated as open, non-secure communications.

APPLICABILITY AND SCOPE



This notice applies to all USDA Agency and Staff Office personnel. This directive has precedence over Agency and Staff Office policies, procedures or other Agency and Staff Office guidance.

It applies to all commercial wireless devices, services and technologies that transmit non-voice data. This includes portable electronic devices (PED) such as laptop computers with wireless capability, cellular/personal communications system (PCS) devices, personal digital assistants (PDA), paging devices, Global Positioning System (GPS) receivers, Radio Frequency Identification Devices (RFID), fixed telemetry devices, and any other commercial wireless devices capable of storing, processing, or transmitting information. This policy does not address classified communications.

REFERENCES

National Federal Oversight Guidelines



Committee on National System Security Systems (CNSS). *National Information Assurance (IA) Policy on Wireless Capabilities*, CNSS Secretariat (IO1C). National Security Agency. Ft. Meade, Maryland. August 11, 2004

Iorga, Michaela, Gavrilă, Serban, Jansen, Wayne, Karygiannis, Tom, Korolev, Vlad. *Policy Expression and Enforcement for Handheld Devices*. National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Federal Register. *Executive Order 13011: Federal Information Technology*. July 16, 1996

Karygiannis, Tom, Owens, Les. *Wireless Network Security, 802.11 Bluetooth and Handheld Devices*. National Institute of Standards and Technology: Special Publication 800-48. Computer Security Division, Technology Administration, U.S. Department of Commerce. November 2002.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 197: Specification for the Advanced Encryption Standard (AES)*. Information Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce. November 26, 2001.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 140-2: Security Requirements for Cryptographic Modules*. Information

Technology Laboratory, National Institute of Standards and Technology, US Department of Commerce. December 3, 2002.

Office of Management and Budget. *OMB Circular A-130, Transmittal Memorandum #4Memorandum for Heads of Executive Departments and Agencies: Management of Federal Information Resources*. November 28, 2000.

US Congress. *Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)) (also known as: Division E: Information Technology Management Reform Act): Section 5002*. United States Code. 1996.

US Congress. *Defense Authorization Act: The Government Information Security Reform Act: Public Law 106-398*. October 30, 2000.

US Congress. *Government Paperwork Elimination Act, 44 USC 3504*. October 21, 2003

Federal Agency Guidelines



Defense Intelligence Agency. *Regulation No. 50-23: Security: DIA Information Systems Security (INFOSEC) Management*. SYS: Defense Intelligence Agency. March 1, 2002

Department of Defense. *802.11 Wireless LAN Security Framework*. Department of Defense: Defense Information Systems Agency Wireless Security Support Program. January 2004.

Department of Defense. *Directive Number 81002.2*, April 14, 2004, ASD (NII)

Department of Homeland Security. *Suggested Enhancements: Management Directive 4300A: Policy Directive for Sensitive Systems: Section 2.8 – Designated Accrediting Authority: Section 3.11.5 – Wireless Security Working Groups: Section 4.6 – Wireless Communications: 5th Draft*. Wireless Management Office. May 2004.

Department of Veterans Affairs. *VA Wireless and Handheld Device Security Guideline, Version 2.1*. September 25, 2003.

DISA. *Wireless Security Technical Implementation Guide, Version 3, Release 1*. DISA Field Security Operations. DISA for DOD. April 15, 2004.

General Services Administration. : *CIO 2161.1: Wireless Personal Digital Assistants (PDAs)*. General Services Administration. February 6, 2004

USDA Guidelines



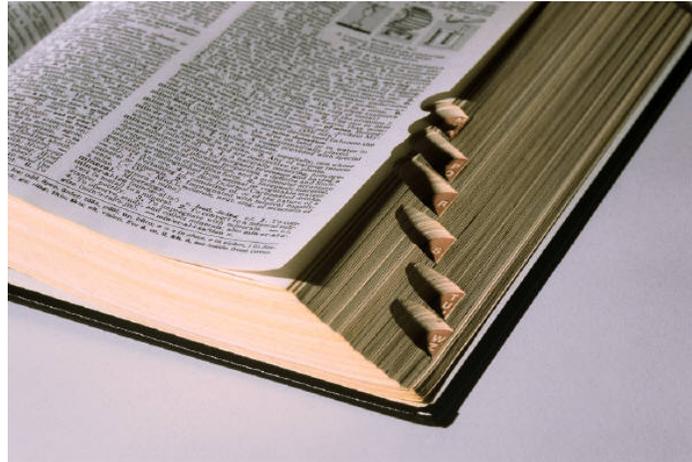
Bull, Barre, Cramer, Chuck. *USDA Personal Electronic Device (PED), Security Assessment Guide*. Science Applications International Corporation. September 6, 2001.

Telecommunications Advisory Sub Council. *Technical Recommendations for Wireless Data Network Deployments Within the United States Department of Agriculture*. Strategy Team: Wireless Working Group: Telecommunications Advisory Sub Council. US Department of Agriculture. November 1, 2004.

USDA. *Cyber Security Manual, Series 3500 DRAFT Chapter 10, Information Technology Systems, Part 3, Portable Electronic Devices (PED) and Wireless Technology*. U.S. Department of Agriculture. September 28, 2004.

USDA. *Disposition of Excess Personal Property and Donation of Surplus Personal Property*. Agricultural Property Management Regulations Chapters 110-36 and 110-37. U.S. Department of Agriculture. Codified version of the Federal Property Management Regulations appear in 41 Code of Federal Regulations, Chapters 101 and 102.

DEFINITIONS



- a. Commercial Wireless: Devices, Services, and Technologies commercially procured and intended for use in commercial and unlicensed frequency bands.
- b. Devices: See "Wireless Devices"
- c. Emergencies: An emergency is any unplanned event that can cause death or significant injury to employees or the public; that can shut down or disrupt operations; or that can cause physical or environmental damage, such as national or declared emergencies, fire emergencies, hazardous materials incidents, storms, communications failure, disaster recovery, and similar emergencies. Note: Failure to plan for a requirement does not constitute an emergency.
- d. Media Access Control (MAC): A hardware address that uniquely identifies each node of a network. MAC related information in the header of a datagram is sent in the clear so it is possible that the MAC address can be obtained by eavesdroppers and spoofed in an attempt to gain access to the WLAN.
- e. Peer-to-Peer: WLANs may be configured into a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly. This type of implementation can be as basic as two laptops with wireless Network Interface Cards (NICs) transmitting data back and forth where an access point is required. Peer-to-peer WLAN communications can bypass required encryption and authentication mechanisms, making transmissions vulnerable to interception and unauthorized access from outsiders.
- f. Personal Digital Assistant (PDA): A generic term for a class of small, easily carried electronic devices used to store and retrieve information.
- g. Poison Pill: An application that when sent to a wireless device, it automatically removes all data and applications from the device. The poison pill can only be sent by the cellular/PCS carrier and only certain models of wireless devices are compatible with the technology.

- h. Teleworking: (Also known as flexiplace, flexible workplace, and telecommuting). Performance of official duties at an alternative work site (i.e. home, telecenter, or other satellite work location).
- i. Vulnerability: Weakness or fault in a system or protection mechanism that exposes information to attack or damage.
- j. Wireless: Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF and optical but, as technology evolves, wireless could include other methods of transmission.
- k. Wireless Device: Hardware that provides wireless capabilities. This definition includes, but is not limited to wireless handheld devices like PDAs, cellular/PCS phones, two-way pagers; wireless audio/video recording devices; telemetry devices with wireless integrated technologies; electronic tablets and laptop computers.
- l. Wireless Handheld Device: Handheld wireless devices include a range of PDA's and digital cellular or personal communications system (PCS) phones capable of transmitting text messages. PDA's act as small computers often capable of synchronizing with a PC on specific software applications. Many handheld devices are capable of "beaming" data with the use of Infrared (IR) technologies that may combine the capabilities of a traditional PDA, digital cellular telephone with voice services as well as e-mail, text messaging, Web access, voice recognition and any number of applications that serve as productivity tools. Throughout this document, wireless handheld devices will be termed "devices".
- m. 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. Wireless technologies use IR, acoustic, RF and optical transmission mediums, however, as technology evolves wireless could use other transmission mediums as well.
- n. Wireless Local Area Network (WLAN): WLANs use radio waves for transmission and are generally connected through access points to an existing wired infrastructure, although they may be standalone as well. They provide authorized users access to resources that are not physically connected to their client device.

ROLES AND RESPONSIBILITIES



Agencies and Staff Offices will:

- (1) Comply with the USDA Enterprise Architecture standards.
- (2) Follow Departmental acquisition processes for the purchase of devices. See DN 3300-14 on wireless acquisitions.
- (3) Keep a central inventory of all wireless devices and their associated Media Access Control (MAC) addresses. See DN 3300-15 on wireless asset management.
- (4) Route all Internet access through the authorized USDA network protected by USDA owned and maintained firewalls and prohibit wireless access from USDA-owned devices directly to the Internet from any location.
- (5) Determine whether devices should be granted privileges on the USDA enterprise network, and if so, notify the OCIO ISSPM to invoke the proper procedures at the Department level.
- (6) Establish a configuration management process to ensure that all devices capable of transmitting data, meet Federal, Departmental and Agency or Staff Office security requirements for non-voice data transmission.
 - (a) At a minimum, devices should be configured to be consistent with landline devices such as desktop computers including:
 1. Anti-virus software.
 2. Password settings enabled at "power-on" and enabled to prompt users for a password based on a "time-out" mechanism requiring the user to log in after a period of inactivity.
 3. Software to enable the installation of software patches.
 4. Authentication software for network access.

5. Robust encryption software enabled for all data transmissions.

6. Disable peer-to-peer data exchange capabilities. Exceptions will be made for continuity of operations (COOP) or emergency response operations. All purchases of wireless devices for the purpose of engaging in peer-to-peer data exchange require that a waiver be submitted to the Associate CIO for Telecommunications by agency or staff office COOP representatives.

(b) Non-voice data services must be discontinued for devices that do not have data encryption capabilities, including those available on cellular and PCS phones. Note that unencrypted text messages transmitted from cellular telephones are not secure and may be vulnerable to interception.

(c) The configuration management process should include periodic security assessments of all devices to ensure that they meet minimum-security configuration requirements.

(7) Label devices with the names of the individuals to whom the devices were issued along with the Agency or Staff Office contact information. If devices are shared, labels should include that name(s) of individuals responsible for tracking and maintaining the devices along with the Agency or Staff Office contact information.

(8) Protect information system infrastructure from unauthorized device access by means of a physical barrier, and use of physical access cards or locks to access the Agency or Staff Office facility.

(9) Ensure that only authorized users are permitted to use government devices.

(10) Conduct annual training for all employees on the security vulnerabilities and proper use of devices. See DN 3300-16 on wireless training.

(11) Develop an internal policy regarding the use of wireless handheld devices with cameras. Establish an internal waiver process to review requests to purchase cameras in wireless handheld devices on a case-by-case basis, requiring users to provide a sound business justification for operational need.

(12) Establish a process for handling lost or stolen devices per the Federal Information Security Management Act (FISMA) guidelines. At a minimum:

(a) The Agency or Staff Office personnel should notify the commercial service provider to suspend or discontinue service; and request that the provider transmit a "poison pill" to the device if it supports the technology.

(b) Network administrators should be notified to remove or suspend the remote device account, block the Media Access Control MAC from the network access list, monitor the network for activity originating from the lost or stolen device.

(c) Agency or Staff Office Information System Security Program Managers

(ISSPM)s or Security Officers should be notified.

(d) The Agency or Staff Office Property Manager should be notified.

(13) Establish procedures for the disposition of wireless assets according to Agricultural Property Management Regulations Chapter 110-36, *Disposition of Excess Personal Property* and Chapter 110-37 *Donation of Surplus Personal Property*. Prior to disposition:

(a) Use DoD approved software to delete all sensitive files and data.

(b) Clear configuration settings.

USDA employees will:



(1) Ensure that when not in use, wireless devices are secured or in the physical possession of the user.

(2) Secure devices with Passwords for non-voice data transmissions.

(a) Passwords for non-voice data transmissions should begin with an alpha character and contain at least one special character. The special characters are the dollar sign (\$), the number sign (#), the numbers 0 through 9, and the underscore (_).

(b) The password should consist of a combination of letters and numbers (or special characters) and be 8 characters in length. Avoid passwords that are either all numbers or all letters to the greatest extent possible.

(c) Never select a password that is related to your personal identity, history, or environment. Never select a word that can be found in a dictionary. Never use your social security number.

(d) Passwords should be changed every 90 days.

(3) Synchronize their devices with their corresponding personal computers (PC)s monthly.

- (4) Archive sensitive data onto a PC, and delete from the device when no longer needed.
- (5) Turn off communication ports during periods of inactivity.
- (6) Submit a waiver to their agency or staff office for the purchase of wireless handheld devices with cameras.
- (7) Immediately report lost or stolen devices to their supervisors.
- (8) Follow USDA disposition policies.

USDA employees will not:



- (1) Alter or disable network security controls unless authorized by Agency and Staff Office management.
- (2) Share logon or password information with others unless authorized by Agency or Staff Office management.
- (3) Engage in "peer-to-peer" WLAN data exchange. Policy for peer-to-peer data exchange in a Bluetooth WPAN environment can be found in DN -12 on wireless networks.

NOTE: Exceptions will be made for continuity of operations (COOP) or emergency response operations. All purchases of wireless devices for the purpose of engaging in peer-to-peer data exchange require that a waiver be submitted to the Associate CIO for Telecommunications by agency or staff office COOP representatives.

INQUIRIES



Direct all questions concerning this notice to the Telecommunication Policy and Planning Division, Telecommunications Services and Operations, Office of the Chief Information Officer at (202) 694-5980.