



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240



JUL 29 2005

OCIO Directive 2005-012

To: Bureau Chief Information Officers
Bureau Deputy Chief Information Officers

From: W. Hord Tipton 
Chief Information Officer

Subject: Wireless Network Security

Purpose:

As part of the strategic planning needed for implementation of wireless networking technology, security must be addressed from the planning stages through deployment. Risks must be identified and the impact on existing systems and information must be determined before the technology is deployed.

This directive outlines the security requirements for wireless networking devices within the Department of the Interior (DOI). Specifically, this directive applies to all devices transmitting DOI data or interfacing with the DOI network infrastructure including major applications, general support systems, or any other DOI information technology (IT) resource using the Institute of Electrical and Electronics Engineers (IEEE) 802.11xx or Bluetooth standards.

At a high level, this directive helps to ensure the confidentiality, integrity, authenticity, and availability of data transmitted across DOI wireless networks, in accordance with *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48: Wireless Network Security, 802.11, Bluetooth and Handheld Devices.*

Scope:

This directive applies to all Departmental offices and bureaus and covers all 802.11xx and Bluetooth wireless networks and networking devices, and handheld devices (e.g. Internet-enabled Personal Digital Assistant (PDA), Blackberry wireless internet services) connected to any of DOI's resources.

Wireless devices such as cellular communications and other Wireless Local Area Network (WLAN) standards that do not implement the IEEE 802.11 and Bluetooth standards are not addressed by this directive and must not be implemented until they are able to conform to this directive and the applicable Security Technical Implementation Guides (STIG). The only exception to this directive is for standard cellular communications which this directive does not govern, except to the extent that cellular features supporting IEEE 802.11 and Bluetooth features and functionality. In such

instances, those features must either be disabled or securely configured in accordance with this directive and applicable STIGs. In all cases the password function must be enabled on these devices.

Timeframe:

This directive is effective immediately.

Directive:

Before wireless networking is deployed in DOI, research and strategic planning must be performed. The following requirements must be implemented for planned and existing wireless networks:

Security

All wireless networks must be implemented according to the requirements set forth in version 2 of the DOI Wireless STIG available via Command Center at <https://www.cmd-ctr.com/login>.

Inventory

All network devices must be accounted for in the bureau system inventory. The inventory must include all wireless access points, wireless enabled laptops, wireless enabled PDAs, and Blackberry's. The inventory must specify the FIPS 140-2 compliant encryption modules, algorithms, and strength of the encryption implemented. Wireless access point inventories must be made current effective immediately. CIOs must submit a current inventory of wireless access points accompanied with a memorandum certifying that there are no other wireless access points in operation other than what is identified on the inventory by August 12, 2005. Inventory of wireless laptops, PDAs, Blackberry, and all other types of Bluetooth enabled devices (including, but not limited to, keyboards, cell phones, etc.) must be completed by November 01, 2005.

Transmittable Information

Sensitive but Unclassified (SBU) data/information (e.g. Privacy Act information, financial, Indian Trust data, etc.) may be transmitted across approved wireless connections that meet the requirements of this directive and that are configured in accordance with the STIGs as long as:

1. An approved DOI network resource transmitting the data/information initiates the encryption and the encrypted session terminates at an approved DOI network device (e.g., approved wireless PDA, Blackberry device, remote laptop, etc.) so as to prevent potential sniffing or monitoring that might lead to any sensitive information being exploited/compromised; and
2. Those portable devices that may be used outside of DOI facilities implement encryption to ensure the confidentiality of any sensitive data/information received by the device.

Authority to Operate

All DOI wireless networks must be fully certified and accredited prior to becoming operational. Any system with a FIPs 199 category impact assessment of moderate or high should also be penetration tested consistent with guidance in NIST 800-42.

The risk assessment must address specific issues related to wireless technology.

Routine site surveys must be conducted to ensure that signal boundaries are limited to planned distances.

Encryption

The built-in security features of Bluetooth or 802.11 (data link level encryption and authentication protocols) must be used as part of an overall defense-in-depth strategy. Although these protection mechanisms have weaknesses described in this publication, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, is mandatory and binding for Federal agencies having determined certain information be protected via cryptographic means. As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard. In the above-mentioned instances, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPSec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect that information, regardless of whether the non-validated data link security protocols are used. DOI policy directs that when a determination has been made that encryption is a requirement to protect the confidentiality of any SBU data, for either transmission or storage on a device, the encryption modules must implement the Advanced Encryption Standard with cipher key lengths of 256 bits (AES-256) at a minimum.

Training

Personnel involved in wireless technologies must receive annual training on the risks of the technology as well as the planning, installing, implementing, controlling, and securing of wireless networks.

Usability

DOI resources must not be connected to non-DOI networks or resources in a manner where SBU data/information may become inadvertently or intentionally stored/copied unencrypted on a non-DOI resource (e.g., laptops, PDAs, cellular phones must never be connected to any public/personally owned kiosk, computer, etc. that might be available in such places as airports, hotels, libraries, cafes/restaurants, etc.).

Only authorized DOI systems may be used for wireless connections.

Each bureau Chief Information Officer (CIO) bears responsibility for the approval of WLAN and wireless personal area network (WPAN) implementations within their bureau once authority is delegated. A waiver is required for wireless installations until each bureau provides a certified inventory of all wireless applications and receives approval authority. Systems/devices not listed on a bureau's certified inventory must be confiscated by the bureau/office CIO and turned in to the DOI property and acquisition office. Procurement and installation of wireless equipment in violation of this directive will be considered an inappropriate expenditure of appropriated funds and repayment to the U.S. Treasury by the responsible party will be expected. Additional liability and disciplinary action may be administered should rogue installation serve as a back door leading to hacking between networks.

Adherence to this directive will be examined during compliance reviews.

Delegation of Authority and Responsibility:

The individual having responsibility and authority for a given wireless network is the CIO of the bureau in which the network resides over once their certified inventory is submitted and approved by the Department. The CIO provides direction, leadership, and accountability for the wireless network through development, implementation, and ultimately, operation. The bureau CIO is in charge of all network security functions and will have the authority to delegate or appoint other individuals and/or create teams as necessary. This person also has ultimate responsibility of ensuring that proper security measures for the network have been deployed, and is the official with the utmost accountability for compliance with this directive.

Each bureau CIO will maintain a current inventory capturing the location, system owner, users, range of IP addresses being utilized, and the date of last risk assessment for each wireless network residing in their bureau.

An annual compliance report must be completed by the bureau/office CIO's by July 31st of each year and submitted to the Departmental CIO.

Contact:

Questions concerning this directive should be directed to the Office of the Chief Information Officer, Cyber Security Division.

cc: Heads of Bureaus and Offices
Bureau Information Technology Security Managers