OFFICE OF THE SECRETARY OF DEFENSE

1000 DEFENSE PENTAGON
WASHINGTON. DC 20301-1000

September 25, 2002

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Pentagon Area Common Information Technology (IT) Wireless Security Policy

On July 30, 2001, in recognition of the exploitable vulnerabilities that wireless devices introduce to Pentagon area facilities and networks, a moratorium was placed upon the installation of telecommunications network infrastructure to support wireless services. The moratorium continues in effect until security vulnerabilities are fully assessed, a wireless design for the Pentagon is developed, and appropriate policies and procedures are established to support the responsible introduction of wireless technologies into Pentagon and swing space facilities and common IT networks. The attached Pentagon Area Common IT Wireless Security Policy supports the moratorium requirements (which remain in effect) and establishes a balanced approach for mitigating vulnerabilities and security risks while supporting the responsible introduction of new technologies into the workplace.

Given the exploitable vulnerabilities inherent in current wireless products and technologies and the interdependencies of Defense and Pentagon networks, it is essential and expected that all tenants will strictly adhere to this policy. Approval, certification, and accreditation of wireless information systems are responsibilities of the Designated Approval Authorities (DAAs). To support these responsibilities, OSD has tasked the

Director, National Security Agency to develop a Wireless Technology Vulnerabilities Database for the Department. The database will provide an initial assessment of the potential vulnerabilities of specified wireless features and capabilities along with the associated risks and a countermeasures recommendation. Additionally, a DoD Enterprise Wireless Knowledge Management process will be developed by OSD to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department.

The Pentagon Force Protection Agency point of contact is Chief John Jester, Acting Director, (703) 693-3685. The Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD(C3I)) point of contact is Ms. Sarah Smythe, Pentagon Area Common IT Oversight, (703) 604-1489.

Howard G. Becker
Acting Director, Administration
and Management

John P. Stenbit
Assistant Secretary of Defense
(Command, Control,
Communications, and Intelligence)/
DoD Chief Information Officer

Attachments:
Pentagon Area Common IT Wireless Security Policy
Pentagon Area Common IT Wireless Moratorium Provisions

cc:
Administrative Assistant to the Secretary of the Army
Administrative Assistant to the Secretary of the Air Force
Assistant for Administration, Under Secretary of the Navy
Director of Administration and Resource Management, HQ USMC
Director of Communications Operations, HQ USAF/ILC
Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
Deputy Assistant Secretary of Defense, Security and Information Operations
Office of the Secretary of Defense, Chief Information Officer
Vice Director, Joint Staff
Deputy Director for Information Systems and Services, Defense Intelligence Agency
Principal Director for Customer Advocacy, Defense Information Systems Agency
Deputy Director of Real Estate and Facilities, Washington Headquarters Services
Acting Director, Pentagon Force Protection Agency
Program Manager, Pentagon Renovation
Project Manager, Information Management and Telecommunications

Director, Information Technology & Communications
Commander, 1108th USA Signal Brigade
Members, Pentagon Area Information Services: Resource Strategy Board; Operational Requirements and Performance Board; Architecture and Configuration Control Board; Wireless Technology Working Group; Integrated Protection Working Group; and, Consolidated Computer Facilities Working Group

Pentagon Area Common Information Technology (IT) Wireless Security Policy

September 2002

EXECUTIVE SUMMARY

This Pentagon Area Common Information Technology (IT) Wireless Security Policy provides guidelines for implementing wireless technologies in the Pentagon and swing spaces. The guidelines present a balanced approach for mitigating the vulnerabilities and security risks while supporting the responsible introduction of new technologies into the workplace.

Highlights of the Pentagon Area Common IT Wireless Security Policy are as follows:

- Recognizes the pace of technological change and, therefore, requires an annual review to keep pace with the rapidity of technological advances

- Does not apply to Sensitive Compartmented Information Facilities (SCIFs) which are governed by Director of Central Intelligence Directive (DCID) rules

- Excludes Land Mobile, Emergency, and Tactical Radios and one-way receive-only devices (e.g., devices with a wireless receiver and no transmitter)

- Prohibits:
  - Connectivity to a classified network or computer
  - Synchronization with IT devices that are not approved by a Designated Approving Authority

- Allows use of wireless devices (e.g., cellular telephones and Personal Digital Assistants):
  - For unclassified data only
  - In areas where unclassified information is electronically stored, processed, or transmitted
  - In areas where classified information is electronically stored, processed, or transmitted unencrypted when there is a documented operational need; the device's infrared, radio frequency and microphone/audio capabilities are disabled; and DCID rules are followed.

- Requires punitive action for repeated violations of this policy that jeopardize the security of the Pentagon Area common IT Enterprise

PENTAGON AREA COMMON IT
WIRELESS SECURITY POLICY

1.0 INTRODUCTION

The commercial sector has introduced many wireless technologies that support increased productivity and connectivity. Wireless devices are rapidly being deployed in the Department of Defense (DoD) to support mission operations. Although wireless computing devices and infrastructure support systems can provide an increase in connectivity, they also provide an increase in security vulnerabilities and risks to DoD information and operations. While we proceed to assimilate these technologies in the DoD workplace, we also need to ensure a balanced approach is taken regarding the associated vulnerabilities and security risks. Thus, an integrated protection approach must be implemented when deploying wireless technology to support DoD business and mission operations.

This document establishes policy, definitions, and responsibilities necessary to mitigate the vulnerabilities and security risks introduced by wireless technologies and the infrastructure installed to support them. This policy will be reviewed annually and updated, if required, to address technology improvements which may provide practical application for the Pentagon community without introducing additional security risks and vulnerabilities.

1.1 Policy Goals

Information Assurance (IA) is defined as (DoD) information operations that protect and defend information and information systems by ensuring their confidentiality, authentication, availability, integrity, and nonrepudiation (Reference Section 6, Item 7). These IA axioms are described as follows:

- **Confidentiality**- Verify that information is private and therefore seen and accessed only by intended recipients. Confidentiality is created primarily through the use of protocols that use encryption.
- **Integrity**- Verify that information received is the same information transmitted by the originator, unchanged.
- **Authentication**- Identify an individual or computer to ensure access to information is authorized. Authentication goes hand-in-hand with identification and confidentiality.
- **Nonrepudiation**-Ensure that an individual cannot deny sending or receiving information.

- **Availability** - Ensure that information (voice, video, and data) and supporting service resources (e.g., server, local networking infrastructures, and transport medium) are up and running when needed.

Based on the five IA axioms, the goals of this policy are to:

1. Protect DoD information, users, and wireless devices from unauthorized disclosure
2. Ensure that DoD information is protected against an intrusion that could alter, disable, or circumvent the transmission
3. Require centralized oversight, configuration management and control of wireless information systems
4. Ensure protection against physical compromise (e.g., immediate notification of misplaced or missing DoD wireless devices to the appropriate authority)
5. Ensure user authentication of DoD information transferred via wireless computing devices
6. Ensure there will be no adverse impact to DoD critical operations if wireless computing devices and the supporting infrastructure are rendered inoperable

1.2 Applicability and Scope

This policy applies to:

1. Pentagon Area (defined as Pentagon and swing space) tenants (and their on-site contractors) which include Office of the Secretary of Defense (OSD), Joint Staff (JS), Washington Headquarters Services (WHS), the Military Departments, the Defense Agencies, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the Pentagon Area DoD Components/Agencies)
2. Wireless-Information Systems (W-IS) defined as wireless telecommunication or computer-related equipment or interconnected system or subsystem of equipment (includes software, firmware, and hardware) that is used in the Pentagon Area to support DoD business, operations, and missions in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data. W-IS excludes Land Mobile, Emergency, Tactical Radios, and one-way receive-only devices

2.0 POLICY

2.1 All Pentagon Area W-IS shall be:

1. used for Unclassified and Sensitive But Unclassified (SBU)/ For Official Use Only (FOUO) data, only

2. approved, certified, and accredited by the Pentagon Designated Approving Authority (DAA) for Common IT (CIT) or the Component/Agency's DAA based on the supported business or mission operations and in accordance with the DoD Information Technology System Certification and Accreditation Program (DITSCAP) or successor directives
3. compliant with DoD TEMPEST policies and guidelines (NSTISSAM TEMPEST/2-95)
4. compliant with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements
5. compliant with most recent DoD policy for authentication
6. configured with preferences and settings for services approved by the Cognizant DAA (i.e., Pentagon DAA for CIT or the Component/Agency's DAA)
7. configuration managed and controlled

2.2 All Pentagon Area W-IS shall not be:

1. connected to a classified network or computer
2. used where classified information is electronically stored, processed, or transmitted un-encrypted unless all of the following are met:

    a. there is an operational need and the mission cannot be accomplished without the use of the W-IS

    b. the device's Infra Red (IR), Radio Frequency (RF) and microphone/audio capabilities are disabled

    c. Director of Central Intelligence Directive (DCID) rules are followed
3. used as a mission critical system; there shall be no impact to mission operations if the Pentagon Area W-IS fails to sustain medium level outages lasting from seconds to hours
4. used as a primary means of communications for mission operations
5. used to download or load any freeware or shareware enhancements or any extraneous software
6. used to synchronize with a non-Pentagon or non-Component/Agency DAA approved and accredited system or network (including personally-owned home computers or contractor-owned computers or networks)

2.3 Pentagon Area Defense network-capable, wireless computing devices shall employ the following security mechanisms:

1. password protection or strong identification and authentication using techniques such as CAC, PKI and Biometrics for those W-IS that store, process, and transmit

DoD information. Passwords shall not include words found in the dictionary and shall be at least eight (8) characters in length using 3 of the following attributes: upper case alphabet characters, lower case alphabet characters, numeric characters and special characters. The password system will render the device inoperable without the proper authentication

2. features and capabilities to disable IR, RF, and microphone/audio (see definitions)

2.4 Acquisitions of Pentagon Area W-IS that store, process, and transmit DoD information shall require the following features:

1. compliant with most recent DoD policy for authentication
2. intrusion detection, auditing, and monitoring mechanisms
3. encryption via NIST FIPS-approved or NSA-approved encryption mechanisms while in the wireless environment
4. virus protection software or equivalent protections to prevent action of malicious logic
5. digital transmitter/receiver

2.5 The Pentagon Area W-IS common IT transport infrastructure deployed within the Pentagon shall:

1. support Pentagon DAA for CIT and Component/Agency DAA approved, certified, and accredited W-IS
2. support security for voice, data and control channel information via NIST FIPS-approved encryption mechanisms for all modes of operation
3. be under the direct control of the Federal Government
4. be able to monitor and detect the exfiltration of signals from areas where classified information is being electronically stored, processed, or transmitted un-encrypted (e.g., passive RF detector)
5. provide the capability to restrict user options to minimize the amount of traffic related information transmitted
6. provide security mechanisms that are scaleable, manageable, flexible, and standards-based
7. employ security mechanisms that are compatible and inter-operable with those mechanisms used on wired voice and data telecommunications networks and computing devices
8. support strong identification, authentication and auditing if remote administration is employed

3.0 RESPONSIBILITIES

3.1 Pentagon DAA for CIT shall:

1. provide oversight for Pentagon Area wireless policies and implementations
2. provide guidance to Component/Agency DAAs on wireless vulnerabilities, threats, and risks consistent with applicable DoD policies, directives, instructions, and DoD authorized security assessments.
3. provide accreditation procedures to Component/Agency DAAs and have final connection approval authority over W-ISs in the Pentagon Area
4. provide security awareness training guidance to Component/Agency DAAs for Pentagon Area W-ISs
5. recommend to the DoD CIO that a Component/Agency be disconnected from the Pentagon common IT transport infrastructure for repeated violations (i.e., greater than three) of a nature that jeopardizes the security of the Pentagon Area common IT enterprise

3.2 The Component/Agency DAA shall:

1. approve, certify, and accredit all Component/Agency W-IS used in the Pentagon Area (Operational Security and Force Protection concerns must be evaluated)
2. approve, certify, and accredit W-IS systems in accordance with the DITSCAP. The accreditation documentation shall be in accordance with the Pentagon DAA for CIT accreditation procedures
3. conduct an audit at least annually to detect unauthorized W-ISs used within the Pentagon
4. incorporate wireless technology into the Information Assurance training (to reflect changes in technology, and Operational Security and Force Protection concerns) for all affected personnel (i.e., administrators and users)
5. establish disciplinary actions for failure to adhere to W-IS policies and directives
6. report security related events (e.g., the loss or misuse of the W-IS) to the Pentagon DAA for CIT
7. develop recovery and restoration guidance for compromised W-ISs
8. require affirmed acknowledgment that the user shall comply with all DoD applicable policies and directives

3.3 The Pentagon Area W-IS User shall:

1. be trained on the responsible use of accredited Pentagon Area W-IS
2. provide affirmed acknowledgment that they will comply with all DoD applicable policies and directives

3. report lost or stolen Pentagon Area W-IS within 24 hours through the user's chain of command to the Component/Agency DAA
4. report violations to this policy through the user's chain of command to the responsible DAA
5. immediately disable any RF, IR, and microphone/audio features and return any W-IS to the Component/Agency's DAA if the device receives or is used to transmit any classified data

3.4 The Pentagon Area W-IS common IT transport infrastructure Service Provider shall:

1. support Pentagon DAA for CIT and Component/Agency DAA approved and accredited W-IS
2. support security for voice, data and control channel information via NIST FIPS-approved encryption mechanisms
3. be under the direct control of the Federal Government
4. be able to monitor and detect the exfiltration of signals from areas where classified information is being electronically stored, processed, or transmitted un-encrypted and at critical points in the Pentagon (e.g., E-Ring)
5. provide the capability to restrict user options to minimize the amount of traffic related information transmitted
6. provide security mechanisms that are scaleable, manageable, flexible, and standards-based
7. employ security mechanisms that are compatible and inter-operable with those mechanisms used on wired voice and data telecommunications networks and computing devices

4.0 EFFECTIVE DATE

This policy is effective immediately.

5.0 POC

The point of contact for this policy is the DoD CIO.

6.0 REFERENCES

1. DoDD Number O-8530.1, dated January 8, 2001, Subject: Computer Network Defense (CND)
2. DoD Instruction, Number 5200.40, dated December 30, 1997, Subject: DoD Information Security Certification and Accreditation Process (DITSCAP)

3. ASD(C3I)/DoD CIO and the Under Secretary of Defense (Personnel and Readiness) Memorandum, dated Jan 16, 2001, Subject: Common Access Card (CAC)
4. Deputy Secretary of Defense Memorandum, dated May 6, 1999, Subject: Department of Defense (DoD) Public Key Infrastructure (PKI)
5. National Security Telecommunications And Information Systems Security (NSTISSAM) TEMPEST/2-95, 12 December 1995, (FOUO) Red/Black Installation Guidance
6. Policy for Land Mobile Radio Systems (August 1, 2001)
7. National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, January 1999 (Revision 1) (INFOSEC 99)
8. Federal Information Processing Standards Publication 140-2 (Supersedes FIPS PUB 140-1, 1994 January 11), Security Requirements For Cryptographic Modules, Information Technology Laboratory National Institute Of Standards And Technology Gaithersburg, MD 20899-8900, Issued May 25, 2001. Change Notice 1: 10/10/2001
9. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," March 21, 1988
10. DODD 5200.2 Department of Defense Personnel Security Program (DoDPSP), 9 April 1999
11. DODD 5200.2-R DoD Personnel Security Program, January 1987
12. Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems Manual

APPENDIX A
DEFINITIONS

CAC	Common Access Card
DAA	Designated Approving Authority: The official designated by the local authority, who has the power to decide on accepting the security safeguards prescribed for an information system.
Disable IR	The only tape shown to be effective in preventing unauthorized activity through the IR Port is Metallic Tape, such as Aluminum or Copper Foil Tape. The Metallic Tape should extend beyond the IR transceiver's covering to ensure no diffracted light is able to escape or enter around the fringes of the tape. Periodic inspections should be conducted to ensure that no holes or openings are created in the tape due to normal wear and tear.
Disable RF	Based on FCC's Part 15 requirements, no significant RF is transmitted from the device.
Disable microphone/ audio	Turn off the microphone/audio capability
End-to-End	The communications between DoD devices that store, process, and transmit information via a non-DoD network (to include the air and Internet interfaces)
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
One-way receive-only device	Device with a wireless receiver and no transmitter. The device is not capable of transmitting any Wireless RF (i.e., there is no wireless communication between the device and any base station, not even station keeping or "keep alive" signals.)
Pentagon Area	Includes the Pentagon and swing space.
Pentagon Area W-IS common IT transport infrastructure Service Provider	The Operations and Maintenance element under the Army as the Executive Agent for common IT in the Pentagon.
Pentagon DAA for common IT	The Operations and Maintenance security element under the Army as the Executive Agent for common IT in the Pentagon.

PKI	Public Key Infrastructure: A PKI is that portion of the security management infrastructure dedicated to the management of keys and certificates used by public key-based security services. A PKI is a credentials service; it associates user and entity identities with public keys. A well-run PKI is the foundation on which the trustworthiness of public key-based security mechanisms rests.
SBU	Sensitive But Unclassified: Any information, if compromised, could adversely affect the national interest, or the conduct of federal programs, or the privacy to which individuals are entitled, but which has not been specifically authorized to be classified.
swing space	Temporary space for Pentagon occupants, provided by the Renovation Program when it supports vacating Pentagon space for a specific phase of the Renovation. This applies to space outside of and within the Pentagon. Space of this type is assigned to the swing space Integrated Process Team (IPT) for design, construction and management, if it does not fall within an ongoing, specific geographic project.
Wireless	Technology that permits the transfer of information between separated points without physical wire connection. Currently wireless technologies use infrared (IR) and radio frequency (RF) but, as technology evolves, wireless could include other methods of transmission.
W-IS	Wireless-Information System: Any DoD wireless telecommunication or computer-related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. W-IS includes end-systems, user devices, and technologies such as, but is not limited to, Personal Digital Assistant (PDAs), Blackberry, 3G Cellular Telephones, Interactive TV, Wireless/IR Copiers and Faxes, and transport infrastructure components such as, but not limited to, transmitters, receivers, amplifiers, and antennas. W-IS excludes Land Mobile, Emergency, Tactical Radios, and one-way receive-only devices.

Pentagon Common IT Wireless Moratorium Provisions

In accordance with OASD(C3I) memorandum, subject: Wireless Technology Implementation in the Pentagon, July 30, 2001, the following applies during the moratorium:

- No new telecommunications network infrastructure (i.e., hubs, switches, routers, repeaters, cabling or other telecommunications network related devices required to provide wireless services such as cellular telephones, personal digital assistants, pagers and radios) can be installed to support wireless services.

- Support for wireless services already in operation can continue, if such support was previously documented and accredited.

- Contracts for such equipment as cellular phones and pagers can be renewed.

- Deployment of additional wireless end-user devices can continue, if supported by currently installed telecommunications network infrastructure. However, this would be done with some investment risk. When the security vulnerabilities are identified, it is possible that changes to the current wireless infrastructure may be required. In that case, it is feasible that the end-user devices might not be compatible.

OASD(C3I) Point of Contact: Sarah Smythe, (703) 601-2124, sarah.smythe@osd.mil