

## SECURE WIRELESS TECHNOLOGY

- 1. REASON FOR ISSUE:** This directive establishes the Department of Veterans Affairs (VA) policy and responsibilities regarding security for wireless technology for implementation or use across VA.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive establishes the policy for securing wireless technologies in accordance with Federal Information Security Management Act (FISMA) (P.L. 107-347, Title III), December 2002, which requires that Federal Agencies establish and implement appropriate Department-wide wireless technology security based upon Federal requirements and industry best practices.
- 3. RESPONSIBLE OFFICE:** The Office of Information and Technology (OI&T) (005), Information Protection and Risk Management (IPRM) (005R) is responsible for the content of this policy.
- 4. RELATED HANDBOOK:** None
- 5. RESCISSIONS:** None.

**CERTIFIED BY:**

/s/  
Roger W. Baker  
Assistant Secretary for Information  
and Technology

**BY DIRECTION OF THE SECRETARY  
VETERANS AFFAIRS:**

/s/  
Roger W. Baker  
Assistant Secretary for Information  
and Technology

Distribution: Electronic Only.



## SECURE WIRELESS TECHNOLOGY

### 1. PURPOSE AND SCOPE:

a. The purpose of this Directive is to establish policy to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 USC §3541-3549, and P.L. 107-347, Title III, the National Institute of Standards and Technology (NIST), and the Department of Veterans Affairs (VA) Directive and Handbook 6500, *Information Security Program*, with regard to the implementation and risk-based approach for the secure utilization of wireless devices within VA.

b. This directive applies to all VA components and information technology resources, including contracted information technology (IT) systems and services. VA must adhere to the security requirements as set forth in this directive. Wireless technology has many advantages if used in the proper way and, most importantly, in a secure manner.

### 2. POLICY:

a. VA must uniformly establish secure wireless technology configuration requirements and guidance pursuant to existing Federal laws, mandates, and existing VA directives for utilizing wireless devices on any VA equipment used to access all VA services and resources;

b. VA must only utilize wireless technologies conforming to VA secure wireless technology configurations and guidance in accordance with paragraph 2a; and

c. VA sensitive information, as defined by VA Directive and Handbook 6500, must not be transmitted via wireless technologies unless Federal Information Processing Standards (FIPS) 140-2 validated encryption is installed and operating as intended.

### 3. RESPONSIBILITIES:

a. **Secretary of Veterans Affairs:** In accordance with FISMA, the Secretary is responsible for:

(1) Ensuring VA adopts Department-wide wireless security compliance and otherwise complies with FISMA and other related Federal policies and requirements;

(2) Ensuring wireless security and related processes are integrated with strategic and operational planning processes;

(3) Ensuring Under Secretaries, Assistant Secretaries, and Other Key Officials support wireless security with regard to information systems and services under their control; and

(4) Ensuring the Assistant Secretary for Information Technology, in coordination with VA Under-Secretaries, Assistant Secretaries, and Other Key Officials, reports the effectiveness of wireless security to Congress, Office of Management and Budget (OMB), and other entities, as required by law and Executive Branch direction.

b. **Under Secretaries and Assistant Secretaries:** These officials are responsible for:

- (1) Assisting the VA Chief Information Officer (CIO) in implementing wireless security within organizations under their day-to-day operational control or supervision, as appropriate;
- (2) Providing input to the VA CIO to ensure the successful implementation and continuation of securing wireless technology.

c. **Assistant Secretary for Information and Technology as the VA Chief Information Officer:** The VA CIO is responsible for:

- (1) Establishing, maintaining, coordinating, and monitoring Department-wide policies, procedures, and training as elements of wireless technology security;
- (2) Issuing and approving policies, procedures, and guidance for implementing and coordinating wireless technology security among all VA Department organizations; and
- (3) Directing, monitoring, and enforcing Department-wide implementation, maintenance, and compliance of wireless technology security;
- (4) Approving the use of standards-based wireless technologies; and
- (5) Approving mitigation and mitigation plans for transitioning legacy or non-compliant wireless technologies.

d. **The Deputy Assistant Secretary for Information Protection and Risk Management (IP-RM) as the VA Chief Information Security Officer (CISO)** is responsible for:

- (1) Establishing, implementing, communicating, and enforcing minimum security configuration standards on all Departmental wireless systems and networks that process, store, or communicate VA information; and
- (2) Conducting security scanning of VA wireless technologies to ensure appropriate security configuration standards are implemented and operating as intended;

e. **Deputy Assistant Secretary, Enterprise Operations and Field Development (DAS EO&FD) and Deputy Assistant Secretary, Office of Enterprise Development (DAS OED):** The DAS EO&FD and DAS OED are responsible for:

- (1) Ensuring adherence to this policy by VA employees, contractor personnel and other non-Government employees; and
- (2) Establishing reporting and other requirements associated with wireless security to document the status of compliance with this policy.

f. VA System Owners are responsible for approving, documenting, implementing, and maintaining proper wireless technology security practices.

#### 4. REFERENCES

- a. Federal Information Security Management Act (FISMA) (P.L. 107-347, Title III), December 2002;
- b. FIPS 140-2, *Security Requirements for Cryptographic Modules*;
- c. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- d. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- e. IEEE/EIA 12207, *Industry Implementation of International Standard*;
- f. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, *Introduction to Computer Security: The NIST Handbook*;
- g. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*;
- h. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- i. NIST SP 800-48, Rev. 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*;
- j. NIST SP 800-53, Rev.2, *Recommended Security Controls for Federal Information Systems*;
- k. NIST SP 800-60, Rev 1, *Guide for mapping Types of Information and Information Systems to Security Categories*, (2 Volumes). Volume 1: Guide, Volume 2 Appendices;
- l. NIST SP 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers*;
- m. NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i RSN/802.11i*;
- n. NIST SP 111, *Guide to Storage Encryption Technologies for End User Devices*;
- o. NIST SP 800-120, *DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication*;
- p. NIST SP 800-121, *Guide to Bluetooth Security*;

q. Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;

r. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*;

s. OMB Circular A-130, Appendix III, *Transmittal Memorandum #4, Management of Federal Information Resources*; and

t. VA Directive and Handbook 6500, *Information Security Program*.