DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA DIRECTIVE 6512
Transmittal Sheet
October 12, 2017

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, in concert with VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500*, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* establishes VA policy for securing wireless technologies in accordance with Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014, 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), Office of Information Security (005R), Office of Cybersecurity (OCS) (005R2) is responsible for the content of this policy.

4. **RELATED HANDBOOK:** None

5. **RESCISSIONS:** VA Directive 6512, *Secure Wireless Technology*, November 4, 2009.

CERTIFIED BY:

/s/
Dat P. Tran
Acting Assistant Secretary for
Office of Enterprise Integration

BY DIRECTION OF THE SECRETARY VETERANS AFFAIRS:

/s/
Scott R. Blackburn
Executive in Charge
for Information & Technology

Distribution: Electronic Only.

This page is intentionally blank for the purpose of printing front and back copies.

SECURE WIRELESS TECHNOLOGY

1. PURPOSE AND SCOPE

a. The purpose of this Directive is to establish Department of Veterans Affairs (VA) policy and assign responsibilities to ensure security of wireless technology as required by the Federal Information Security Management Act of 2002 (FISMA), 44 USC §3541-3549, and P.L. 107-347, Title III and Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014; the National Institute of Standards and Technology (NIST); the Department of Veterans Affairs (VA) Directive 6500, *Managing Information Security Risk: VA Information Security Program;* and VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA 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.

2. POLICY

a. VA must uniformly establish secure wireless technology configuration standards 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 One-VA Technical Reference Model (TRM) One-VA Technical Reference Model (TRM), and the OIT Enterprise Infrastructure Baselines managed by IT Operations and Services (ITOPS) Enterprise Systems Engineering.

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; and

d. The policies and responsibilities outlined in this Directive are to be used in conjunction with all policies and responsibilities mandated in VA Directive and Handbook 6500.

3. **RESPONSIBILITIES**

a. **Secretary of Veterans Affairs** is responsible for designating the Department's Chief Information Officer (CIO) as the senior agency official responsible for the Department's Information Technology program.

b. **Assistant Secretary for Information and Technology**, as the VA CIO, is **responsible for:**

(1) Establishing VA Department-wide policy to ensure effective and secure control over wireless technology and compliance as it relates to 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) Reporting the effectiveness of wireless security to Congress, Office of Management and Budget (OMB), and other entities, as required by law and Executive Branch direction. Establishing, maintaining, coordinating, and monitoring Department-wide policies, procedures, and training as elements of wireless technology security;

(5) Issuing and approving policies, procedures, and guidance for implementing and coordinating wireless technology security among all VA Department organizations; and

(6) Directing, monitoring, and enforcing Department-wide implementation, maintenance, and compliance of wireless technology security;

(7) Approving the use of standards-based wireless technologies; and

(8) Approving mitigation and mitigation plans for transitioning legacy or non-compliant wireless technologies.

c. **Under Secretaries and Assistant Secretaries** 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; and

(2) Providing input to the VA CIO to ensure the successful implementation and continuation of securing wireless technology.

d. The **Deputy Assistant Secretary for Information Security (OIS)** 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 Chief Information Officer (DCIO) for IT Operations and Services (ITOPS)**, responsible for:

(1) Ensuring adherence to this policy by VA employees, contractor personnel and other non-Government employees who access VA data; and

(2) Establishing reporting and other requirements associated with wireless security to document the status of compliance with this policy.

f. **Deputy Chief Information Officer for Architecture, Strategy, and Design** is responsible for ensuring the information security requirements necessary to protect the organizational missions/business functions are adequately addressed in all aspects of enterprise architecture (EA) including; reference models, segment and solution architectures, and resulting information systems supporting those missions and business processes.

g. **Information Security Officers (ISO)** are agency officials who OI&T Field Security Service has assigned responsibility to ensure the appropriate operational security posture is maintained for an information system or program. VA ISOs are responsible for:

(1) Providing official guidance on information security matters to local management and staff;

(2) Verifying and validating, in conjunction with the Information System Owners and managers, appropriate security measures are implemented and functioning as intended; and

(3) Mitigating security issues in within their facilities.

h. **Local/Facility Chief Information Officers (CIO)** are responsible for identifying and mitigating security issues within their facilities. Local/Facility CIOs are also responsible for coordinating with Biomedical Engineering staff, Information System Owners, and facility personnel to ensure the use of wireless technology does not interfere with the safe operation of any medical devices.

i. **Local/VISN Biomedical Engineering staff** is responsible for:

(1) Coordinate with the Local CIO and ISO to ensure that any wireless technologies proposed for a facility will not interfere with the safe operation of any approved medical device;

(2) Ensuring that the Health Information Security Division (Under the Field Security Services) access controls are used; and

(3) Coordinating with the Local CIO to ensure that all areas where wireless technology use is prohibited are clearly marked.

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

4. REFERENCES

a. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014;

b. Office of Management and Budget (OMB) Memorandum M-16-04, Cyber*security Strategy and Implementation Plan (CSIP) for Federal Civilian Government,* October 2015;

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

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

e. Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*;

f. NIST SP 800-48, Rev. 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*;

g. NIST SP 800-97*, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i RSN/802.11i*;

h. NIST SP 800-120*, DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication;*

i. NIST SP 800-121 Rev. 1*, Guide to Bluetooth Security*;

j. NIST SP 800-153*, Guidelines for Securing Wireless Local Area Networks (WLANs)*

k. NIST SP 800-167*, Guide to Application Whitelisting;*

l. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program;*

m. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*;

n. Health Insurance Portability and Accountability Act of 1996 (HIP AA) Security Rule, *Security Standards for the Protection of Electronic Protected Health Information*