Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6601
Transmittal Sheet
February 27, 2007

REMOVEABLE STORAGE MEDIA

1. REASON FOR ISSUE: To establish policy for The Department of Veterans Affairs (VA) removable storage media.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: To implement information security requirements relating to removable storage media.

3. RESPONSIBLE OFFICE: The Office of Information and Technology (OI&T), 810 Vermont Avenue, NW, Washington, DC 20420, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

Certified By:

Robert T. Howard
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

Gordon H. Mansfield
Deputy Secretary

Distribution: Electronic

REMOVEABLE STORAGE MEDIA

1. PURPOSE AND SCOPE

a. This directive establishes Department of Veterans Affairs (VA) policy towards the uncontrolled use of all removable storage media, especially Universal Serial Bus (USB) devices, throughout the Department. The provisions of this directive are applicable VA-wide.

b. Information contained on such devices can be easily compromised if the device does not have adequate protective features. In addition, removable storage media, such as USB thumb drives, MP3 PLAYERS (e.g., iPods and Zunes, and external hard drives), can introduce malicious code to the VA network via USB ports, consequently their use must be better controlled.

c. The overall intent of this Directive is to limit the use of removable storage devices through USB ports to connect to VA information technology or access to VA sensitive information.

2. POLICY

a. All VA employees, contractors, business partners, and any person who has access to and stores VA information must have permission from a supervisor and Information Security Officer (ISO) to use such devices, and if used to store sensitive information, the device must contain protective features that have the approval of the local senior Office of Information and Technology (OI&T) official.

b. In addition, all Department staff, contractors, business partners, or any person who has access to and stores VA information must have written approval from their respective VA supervisor and ISO before sensitive information can be removed from VA facilities. VA sensitive information must be in a VA protected environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed.

c. Among USB devices, “thumb drives” clearly pose one of the highest data security risks. To further enhance the VA security posture, only USB thumb drives that are Federal Information Processing Standards (FIPS) 140-2 certified can be utilized. This requirement is applicable to all VA employees, contractors, business partners, or any person who has access to and stores VA information. Utilization of personally-owned USB thumb drives within the Department is prohibited. Transition to this posture must occur over the next sixty (60) days. The OI&T community, under the direction of the Chief Information Officer (CIO), will effect this transition.

d. FIPS 140-2 certified USB thumb drives will be procured with VA funding for VA employee utilization if the need to utilize a thumb drive as an external storage device

exists. This must be approved by the individual's supervisor and must be provided by the local OI&T senior representative.

e. The procurement will be accomplished under the direction and control of OI&T.

f. VA employees are not authorized to access or store any VA information using a thumb drive that has not been procured by the VA.

g. Non-VA personnel (contractors, business partners, etc.) supporting VA must furnish their own FIPS 140-2 certified USB thumb drives that conform to the published listing of VA approved USB thumb drives. Further, permission must be obtained from a designated VA supervisor before they can be utilized.

h. The listing of VA approved USB thumb drives is derived from the *National Institute of Standards and Technology (NIST) FIPS 140-2 Validation Lists for Cryptographic Modules.* This listing is also posted on the VA Intranet under the Office of Information and Technology, Office of Information Technology Operations.

3. RESPONSIBILITIES. All Under Secretaries, Assistant Secretaries, and Other Key Officials are responsible for the following:

a. Communicating this policy to all employees in their organizations and evaluating the security and privacy awareness activities of each organization in order to set clear expectations for compliance with security and privacy requirements and to allocate adequate resources to accomplish such compliance.

b. Developing mechanisms for communicating, on an ongoing basis, each workforce member's role and responsibilities specific to data security and privacy policies and practices that will enhance our security and privacy culture.

4. DEFINITIONS

Thumb Drive: A USB Flash Drive is essentially NAND-type flash memory integrated with a USB 1.1 or 2.0 interface used as a small, lightweight, removable data storage device. This hot swappable, non-volatile, solid-state device is usually compatible with systems that support the USB version that the drive uses.

Sensitive Information: VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and

personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

5. REFERENCES:

a. 40 U.S.C. Section 11101, Definitions

b. 44 U.S.C. Section 3544

c. VA Directive 6504, Restrictions on Transmission, Transportation, and Use of and Access to VA Data Outside VA Facilities.

d. 5 U.S.C. Section 552a

e. 45 C.F.R. Parts 160 and 164.