Martinez

Department of Veterans Affairs

Memorandum

Date: APR 2 0 2004

From: Assistant Secretary for Information and Technology (005)

Subj: Fixed Electronic Media Sanitization

To: Under Secretaries, Assistant Secretaries, Field Facility Directors, and Other Key Officials

1. The Office of Cyber and Information Security (OCIS), in conjunction with the Office of Acquisition and Materiel Management (OA&MM), is in the process of finalizing VA Directive and Handbook 6503, Electronic Media Sanitization. In the interim, all VA organizations, including VA field facilities, are required to follow the media sanitization procedures for fixed electronic media (i.e., hard drives) outlined in this memorandum and its attachment. These procedures ensure that (a) fixed electronic media are appropriately sanitized; (b) the action has been documented; and (c) all VA data is protected to prevent subsequent disclosure when IT equipment containing sensitive data is surplused, donated, or otherwise removed from VA control where the data could be exposed to unauthorized individuals.

2. Storage media must be safeguarded in the manner prescribed for the highest sensitivity of information processed on the computer equipment writing to that media. Until the media is subject to approved purging or clearing actions, there must be continuous assurance that sensitive data is protected, and not allowed to be placed in a situation where the data may be compromised. Officials responsible for performing electronic media sanitization procedures should use the least destructive method for sanitizing information technology (IT) equipment to foster reutilization and minimize the generation of hazardous waste, while ensuring that no data is exposed to unauthorized individuals.

3. If you have any questions concerning the proper procedures for sanitizing electronic media, please have a member of your staff contact Gail Belles, Director, Field Operations and ISO Support Service, at (518) 449-0604, or by email at gail.belles@med.va.gov.

Robert N. McFarland

Attachment

cc:

All VA Information Security Officers

Actions To Be Followed When Sanitizing Fixed Electronic Media

1. **Overwriting.** To satisfy requirements for overwriting, write unclassified characters to all data locations on a media. The number of times overwriting must be performed depends on the storage media and its sensitivity. At a minimum, three passes are required. Data Eraser software by Ontrack has been selected and approved as the VA overwriting technology, and copies of Data Eraser have been distributed Department-wide. If additional copies of the Data Eraser software are required, please send an email request to Suzanne Bucci, Field Operations and ISO Support Service, at suzanne.bucci@med.va.gov. Overwriting is not 100 percent successful when a hard disk contains bad or damaged sectors. Original data written to the damaged sector before it became defective will not be overwritten, and any information previously recorded in these areas can be recovered with specialized tools and techniques. Before media is used, all usable tracks, sectors, or blocks should be identified. For all media found with damaged areas, overwriting is not an acceptable clearing method. In this case, the media shall be degaussed and destroyed. It should be noted that the Data Eraser product may not work effectively on disk arrays; however, a write utility is being tested for use by VA offices, and additional information will be forthcoming.

2. **Degaussing and Destruction.** If sanitization is not possible using VA-approved overwriting technology, media shall be degaussed and destroyed.

a. **Degaussing.** VA-approved degaussers are those that have been tested and approved by the National Security Agency (NSA). NSA publishes a list of evaluated degaussers, the Degausser Products List (DPL). The latest version of the DPL can be found at http://www.dss.mil. In some circumstances, degaussing does not guarantee complete data destruction (e.g., using under strength degaussing equipment will not ensure 100 percent data purging). Always ensure the appropriate degaussing equipment identified on the DPL is matched with the manufacturer's specifications for the media being degaussed. Proper degaussing ensures that there are insufficient remnants to reconstruct data.

b. **Destruction.** To ensure sanitization of sensitive data, fixed electronic media (i.e., hard drives) shall be degaussed before destruction. During the destruction of media, the handling of hazardous materials, if any, shall be in compliance with applicable environmental laws and regulations. The following methods can be used to destroy media:

(1) Destruction by smelting (i.e., to melt or fuse, returning the metal to a liquid state) at an approved metal destruction facility; and

(2) Destruction by pulverization or disintegration (i.e., crushing or grinding, reducing media to very small particles) at an approved metal destruction facility.

3. **Documentation.** VA Form 0751, Information Technology Equipment Sanitization Certificate, must be completed, attached to the proper turn-in documentation, and submitted through proper channels for all information technology (IT) equipment that is

turned-in through the Office of Acquisition and Materiel Management (OA&MM). Other IT equipment and electronic storage media containing sensitive data that is not required to be turned-in through OA&MM is still subject to sanitization procedures prior to disposition or re-use in accordance with NSA's Central Security Service Media Declassification and Destruction Manual procedures.

4. **Office of Cyber and Information Security (OCIS) Media Disposal Services Contract.** OCIS is in the process of establishing an electronic media disposal services contract for use by all VA offices and facilities, nationwide. Procedures for mailing (i.e., securely delivering), tracking, and certifying disposal of media are being evaluated and tested, and will be disseminated VA-wide when finalized.

BRIEFING NOTE

TO: Assistant Secretary for Information and Technology (005)

SUBJECT: Fixed Electronic Media Sanitization (EDMS 268093)

DISCUSSION: The subject memorandum and its attachment describe procedures for ensuring that (1) fixed electronic media are appropriately sanitized; (2) the action has been documented; and (3) all VA data is protected to prevent subsequent disclosure when information technology (IT) equipment containing sensitive data is surplused, donated, or otherwise removed from VA control where the data could be exposed to unauthorized individuals. The memorandum and its attachment will serve as interim guidance until VA Directive and Handbook 6503, Electronic Media Sanitization, is finalized.

IMPLICATIONS: Consistent application of electronic media sanitization procedures across the Department is necessary to prevent disclosure of VA data to unauthorized persons. Based on inquiries received from VA field facilities, current procedures are not widely known or uniformly practiced.

RECOMMENDATION: Sign the memorandum.

Bruce A Brody 4/15/2004

Bruce A. Brody Date
ADAS for Cyber and Information Security
(005S)

4/14/04

Jennifer S. Duncan Date
Director, Office of Management and
Program Support (005B)

APR 20 2004

Edward F. Meagher Date
Deputy Assistant Secretary for Information
and Technology (005)