By: Carona S.B. No. 1673

A BILL TO BE ENTITLED

AN ACT

relating to the sanitization processes prior to the sale, transfer, or disposal of computers, computer peripherals, and computer software or other Information Technology devices.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 2054, Government Code, is amended by adding Subchapter K to read as follows:

SUBCHAPTER K. INFORMATION TECHNOLOGY DEVICE SANITIZATION PROCESSES

Sec. 2054.401. DEFINITIONS. In this subchapter:

(1) "Clearing" means the process of deleting the data on the media before the media is reused. It is important to note that clearing will allow for the retrieval of information if certain retrieval procedures are used and is not approved for computer equipment or media that contain sensitive and/or confidential data.

(2) "Coercivity" means magnetic media is divided into three types (I, II, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained before executing any degaussing procedure.

(3) "Degauss" means the procedure that reduces the magnetic flux on media virtually to zero by applying a reverse

magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

(4) "Degausser" means the device used to remove data from magnetic storage medium.

(5) "DoD Sanitization Standard (5520.22-M)" means the US Department of Defense standard for clearing and sanitizing data on writable media.

(6) "Dynamic Random Access Memory (DRAM)" means the most common kind of random access memory (RAM) for personal computers and workstations. Unlike firmware chip DRAM loses its content when the power is turned off.

(7) "Electronically Alterable PROM (EAPROM)" is a PROM whose contents can be changed.

(8) "Electronically Erasable PROM (EEPROM)" means user-modifiable read-only memory (ROM) that can be erased and reprogrammed (written to) repeatedly through the application of higher than normal electrical voltage. A special form of EEPROM is flash memory.

(9) "Erasable Programmable ROM (EPROM)" means programmable read-only memory (programmable ROM) that can be erased and re-used. Eraser is caused by shining an intense ultraviolet light through a window that is designed into the memory chip.

(10) "Flash EPROM (FEPROM)" means a non-volatile device similar to EEPROM, but where erasing can only be done in blocks or the entire chip.

(11) "Programmable ROM (PROM)" means read-only memory (ROM) that can be modified once by a user.

(12) "Magnetic Bubble Memory" means a non-volatile memory device for computers that uses magnetic bubbles for recording bits. The technology was used in early 1980s but is obsolete today.

(13) "Magnetic Core Memory" means a random access memory (RAM) system that was developed at MIT in 1951. Magnetic core memory replaced vacuum tubes and mercury delay lines with a much more compact and reliable technology. Semiconductor memories largely replaced magnetic cores in the 1970s.

(14) "Magnetic Plated Wire" means non-volatile memory created by Honeywell in 1960s. Magnetic plated wire consists of a copper conductor covered with a thin layer of highly magnetic material, over which a polyurethane insulating film is enameled.

(15) "Nonvolatile RAM (NOVRAM)" means memory that does not lose its information while its power supply is turned off.

(16) "Oersteds" means the unit of magnetic field strength in the centimeter-gram-second system.

(17) "Overwriting" means a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing; however, the effectiveness of the overwrite procedure may be reduced by several factors, including: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps.

(18) "Overwriting Procedure" means the preferred method to clear magnetic disks is to overwrite all locations three (3) times (the first time with a random character, the second time with a specified character, the third time with the complement of that specified character).

(19) "Read Only Memory (ROM)" means built-in computer memory containing data that normally can only be read, not written to. The data in ROM is not lost when the computer power is turned off. The ROM is sustained by a small long-life battery in your computer.

(20) "Sanitizing" means the process of removing the data on the media before the media is reused in an environment that does not provide an acceptable level of protection for the data. In general, laboratory techniques cannot retrieve data that has been sanitized/purged. Sanitizing may be accomplished by degaussing.

(21) "Static Random Access Memory (SRAM)" means random access memory (RAM) that retains data bits in its memory as long as power is being supplied. SRAM is used for a computer's cache memory and as part of the random access memory digital-to-analog converter on a video card.

Sec. 2054.402. PROCEDURE FOR SALE, TRANSFERRED OR DISPOSED OF COMPUTER SYSTEMS. (a) The following procedures must be followed when a computer system is sold, transferred, or disposed of. This policy does not supersede specific policies, directives or standards required by federal or state agencies pertaining to the disposal of computer equipment. The following procedures also apply to contractor-supplied computers:

(1) before a computer system is sold, transferred, or otherwise disposed of, all sensitive and/or confidential program or data files on any storage media must be completely erased or otherwise made unreadable in accordance with DoD standards (5220.22-M) unless there is specific intent to transfer the particular software or data to the purchaser/recipient;

(2) the computer system must be relocated to a designated, secure storage area until the data can be erased;

(3) hard drives of surplus computer equipment must be securely erased within 60 days after replacement; and

(4) whenever licensed software is resident on any computer media being sold, transferred, or otherwise disposed of, the terms of the license agreement must be followed.

(b) After the sanitization of the hard drive is complete, the process must be certified and a record maintained as specified by the agency's records retention schedule.

Sec. 2054.403. SANITIZATION OF HARD DRIVES. (a) there are three acceptable methods to be used for the sanitization of hard drives:

(1) overwriting;

(2) degaussing; and

(3) physical destruction

(b) The method used for sanitization, depends upon the operability of the hard drive:

(1) operable hard drives that will be reused must be overwritten prior to disposition. If the operable hard drive is to be removed from service completely, it must be physically destroyed

or degaussed; and

(2) if the hard drive is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

(c) Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing state owned hard disk storage media.

Sec. 2054.404. OVERWRITING SPECIFICATION. Overwriting is an approved method for sanitization of hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following specifications:

(1) the data must be properly overwritten with a pattern;

(2) sanitization is not complete until three overwrite passes and a verification pass is completed;

(3) the software must have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data;

(4) the software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors,

blocks, tracks, and any unused disk space on the entire hard disk medium;

(5) the software must have a method to verify that all data has been removed; and

(6) sectors not overwritten must be identified.

Sec. 2054.405. DEGAUSSING SPECIFICATIONS. The following standards and procedures must be followed when hard drives are degaussed:

(1) follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing;

(2) shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing; and

(3) hard disk platters must be in a horizontal direction during the degaussing process.

Sec. 2054.406. PHYSICAL DESTRUCTION. Hard drives must be destroyed when they are defective or cannot be repaired or sanitized for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

Sec. 2054.407. SANITIZATION OF OTHER COMPUTER MEDIA. (a) If there is any risk of disclosure of sensitive data on media other than computer hard drives, the appropriate sanitization methods as outlined in the DoD recommended sanitization procedures should be followed. Particular attention should be paid to floppy disks, tapes, CDs, DVDs, and optical disks.

(b) Memory components should also be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

(c) Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release. Memory components are categorized as either volatile or nonvolatile, as described below:

(1) volatile memory components do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data, i.e. SRAM, DRAM; and

(2) nonvolatile memory components do retain data when all power sources are discontinued. Nonvolatile memory components include Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM) and their variants. Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released; otherwise, DoD Sanitization Procedures must be followed.

Sec. 2054.408. CERTIFICATION OF SANITIZATION. Prior to submitting surplus forms to the agency's appropriate

organizational unit, the sanitizing process must be documented on a form that explicitly outlines the method(s) used to expunge the data from the storage media, the type of equipment/media being sanitized, and the name of the person responsible for the sanitization, as well as the name and signature of their supervisor. The form must be completed and a copy affixed to the hard drive. The completed form must be maintained in a central location designated by the agency.

SECTION 2. This Act takes effect January 1, 2004.