U. S. ELECTION ASSISTANCE COMMISSION
Voting System Testing and Certification Program
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Wiping Election Equipment before Disposal, Sale, or Destruction

In today's world, everyone needs to be cognizant of the security risks associated with the disposal, sale, or destruction of computer equipment and storage devices. Election officials, specifically, need to perform their due diligence to make sure that any proprietary information, such as voting system software or firmware, election data, such as ballot selections and vote totals, and any personal information, such as voter registration data, has been properly sanitized from those devices before they dispose of, sell, or destroy election equipment. This equipment can include everything from voting devices to electronic pollbooks, and servers.

The EAC is aware that many jurisdictions are currently looking to procure new election technologies. Therefore, those same jurisdictions will have a need to dispose of the currently owned equipment. This document is focused on providing guidance and best practices for steps to take prior to the disposal or sale and the destruction of voting equipment that may contain proprietary data and/or non-confidential, but sensitive records such as vote totals, ballot definitions, and audit logs.

For other election systems and election technologies that do contain personal identifiable information, you may also want to take additional precautions. Therefore, for more detailed information on determining how to sanitize any election technology, see the attached Clearing and Sanitization Matrix from Defense Security Service and/or refer to NIST Special Publication 800-88 Revision 1.

Before you dispose, sell, or destroy any voting equipment or election technology, make sure that you perform all necessary back-ups.

Disposal or Sale of Voting Equipment

Prior to the disposal or sale of any voting system, all equipment should be wiped of all data. Solely deleting the files on the device is not sufficient, since deleting files does not remove the files from memory. Deleted files remain on the disk and can still be recovered. Therefore, all equipment should be taken back to the condition of a non-functioning piece of hardware with no software or firmware remaining on the equipment.

First, determine if your Information Technology/Information Security Department has a process for wiping data from memory before disposing or selling equipment. Follow all of the requirements set forth by your jurisdiction for fulfilling this process. Second, confirm the process with your voting system manufacturer (vendor) to make sure it is sufficient for meeting the requirements of the technology and equipment to which it is applied. Third, make sure that you verify that there are no legal or contractual obligations that you must meet before disposing or selling any of the voting equipment.

For computer equipment, you may be able to do this on your own by using a tool that overwrites every sector of the hard drive multiple times. There are tools, both free and for purchase, that meet the Department of Defense security standards for wiping the data (DOD 5220.22-M, Data Wipe Method).

Destruction of Voting Equipment

Your jurisdiction may determine that it would be best to outsource the disposal and destruction of the voting equipment. When exercising this option, it is recommended that the jurisdiction should exercise due diligence, including only using a disposal company that is certified by a recognized trade association or similar third party. Also, the jurisdiction should request a certificate of destruction stating that all of the data stored on the voting equipment has been properly erased and all hardware has been appropriately discarded.

14.1.16 Clearing and Sanitization Matrix

Media	Clear					Sanitize														
Magnetic Tape																				
Type I	a						b									l				
Type II	a						b									l				
Type III	a						b									l				
Magnetic Disk																				
Bernoulli	a	c					b									l				
Floppy	a	c					b									l				
Non-Removable Rigid Disk		c				a			d							l				
Removable Rigid Disk	a	c				a			d							l				
Optical Disk																				
Read Many, Write Many		c														l				
Read Only																l	m			
Write Once, Read Many (Worm)																l	m			
Memory																				
Dynamic Random Access Memory (DRAM)		c	g					c				g				l				
Electronically Alterable Programmable Read Only Memory (EAPROM)				h										i		l				
Electronically Erasable PROM (EEPROM)				h						f						l				
Erasable Programmable ROM (EPROM)					j			**c**							**k**	l				**k then c**
Flash EPROM (FEPROM)				h				**c**					**h**			l				**h then c**
Programmable ROM (PROM)		c														l				
Magnetic Bubble Memory		c				a		c								l				
Magnetic Core Memory		c				a			d							l				
Magnetic Plated Wire		c						**c**		**e**						l				**c and e**
Magnetic Resistive Memory		c														l				
Non-volatile RAM (NOVRAM)		c						c								l				
Read Only Memory (ROM)																l				
Synchronous DRAM (SDRAM)		c	g					c				g				l				
Static Random Access Memory (SRAM)		c	g					c				g				l				
Other Media																				
Video Tape																l				
Film																l				
Equipment																				
Monitor			g																p	
Impact Printer			g									**g**						**o**		**o then g**
Laser Printer			g									**g**					**n**			**n then g**

INSTRUCTIONS FOR READING THE MATRIX:

A letter in black in the above table indicates the procedure is a complete, single option. For example, to sanitize EEPROM: Perform either procedure f or l (refer to indices below) and the media/memory is completely sanitized. Letters in bold indicate the procedures must be combined for a complete sanitization. For example, to sanitize a Laser Printer: n must be performed, followed by g.

NOTE: When a combination of two procedures is required, the far right hand column indicates the order of the procedures (e.g., o then g).

MATRIX INDEX:

a. Degauss with Type I, II, or III degausser.
b. Degauss with same Type (I, II, or III) degausser.
c. Overwrite all addressable locations with a single character utilizing an approved overwrite utility.
d. For spills only, overwrite with a pattern, and then its complement, and finally with another unclassified pattern (e.g., "00110101" followed by "11001010" and then followed by "10010111" [considered three cycles]). Sanitization is not complete until three cycles are successfully completed. Once complete, verify a sample. If any part could not be written to the disk, the disk must be destroyed or degaussed. This option does not apply to disks used on a system accredited for classified processing.
e. Each overwrite must reside in memory for a period longer than the classified data resided.
f. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones utilizing an approved overwrite utility.
g. Remove all power to include battery power.
h. Perform a full chip erase as per manufacturer's data sheets.
i. Perform h above, then c above, a total of three times.
j. Perform an ultraviolet erase according to manufacturer's recommendation.
k. Perform j above, but increase time by a factor of three.
l. Destruction (see below.)
m. Destruction required only if classified information is contained.
n. Run 1 page (font test acceptable) when print cycle not completed (e.g., paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.
o. Ribbons must be destroyed. Platens must be cleaned.
p. Inspect and/or test screen surface for evidence of burn-in information. If present, screen must be destroyed.