Exhibit B

DSS Clearing and Sanitization Matrix
(Updated June 28, 2007)

NISPOM paragraphs 5-704 and 5-705 set out requirements for the destruction of classified material that is no longer required, including media, memory, and equipment. The appropriate procedure to be used is based on the classification sensitivity of the information and the type (size, capacity and coercivity) of the media. There is currently no overwriting product or process that has been evaluated in accordance with the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

Therefore, in accordance with NISPOM paragraph 8-301, DSS will apply the guidance in the NSA CSS Policy Manual 9-12, "NSA/CSS Storage Device Declassification Manual", dated 13 Mar 2006, to sanitization, declassification, and release of IS storage devices for disposal or recycling. Effective immediately, DSS will no longer approve overwriting procedures for the sanitization or downgrading (e.g. release to lower level classified information controls) of IS storage devices (e.g., hard drives) used for classified processing.

The matrix provides guidance regarding clearance, sanitization (destruction) and disposition of the most common media, memory and equipment used for classified processing.

Clearing and Sanitization Matrix[1]

Media	Clear					Sanitize															
Magnetic Tape																					
Type I	a						b									l					
Type II	a						b									l					
Type III	a						b									l					
Magnetic Disk																					
Bernoullis	a	c					b									l					
Floppy	a	c					b									l					
Non-Removable Rigid Disk		c				a										l					
Removable Rigid Disk	a	c				a										l					
Optical Disk																					
Read Many, Write Many		c														l					
Read Only																l	m				
Write Once, Read Many (Worm)																l	m				

[1] In addition, NIST Special Publication 800-88, Guidelines for Media Sanitization, dated Sep 2006, can assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information, ensuring cost effective security management of their IT resources, and mitigate the risk of unauthorized disclosure of information.

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					
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, e.g. EEPROM sanitization: Perform either procedure f or l (refer to indices below) and the media/memory is completely sanitized. Letters in ***red*** indicate the procedures must be combined for a complete sanitization, e.g., Laser Printer sanitization**:** **n** must be performed, then **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.
d. Overwrite all addressable locations with a character, its complement, then a random character.
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.
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.

Destruction Methods for Classified Media and Equipment:

A. NISPOM Paragraph 5-705 reflects requirements for destruction of classified material, including classified media and equipment. DSS recommends methods and procedures for destroying classified media and equipment should be reflected in the System Security Plan and reviewed/approved in connection with the information system certification and accreditation process. The following summary information is provided for contractor facilities in updating system security procedures for destruction of classified media:

- Incineration is the most common and recommended method for removing recording surfaces.

- Applying an abrasive substance to completely remove the recording surface (e.g. emery wheel, disk sander, belt sander, sand blaster) from the magnetic disk or drum. Make certain that the entire recording surface has been thoroughly destroyed before disposal. Ensure proper protection from inhaling the abraded dust.

- Degaussing or destruction using government approved devices. NSA publishes guidance on the sanitization, declassification, and release of Information Systems (IS) storage devices for disposal or recycling in the NSA CSS Policy Manual 9-12, NSA/CSS Storage Device Declassification Policy Manual, dated 13 Mar 2006. It is recommended that prior to performing any process for disposal, recycling or release of storage, media, or equipment that users review the manual and/or check for any updates to the guidance. NSA publishes on a recurring basis, updated Evaluated Products Lists (EPL) for High Security Crosscut Paper Shredders, High Security Disintegrators and Optical Media Destruction Devices. Contractors may utilize NSA evaluated destruction devices for destruction of classified media and hardware without prior authorization from DSS. For use of non-NSA approved devices or procedures, prior approval of the CSA is required.

- Smelting, disintegrating, or pulverizing hard disks or drums at an approved metal destruction facility. Prior approval of the CSA is required.

- Destroying by the use of chemicals (e.g. application of concentrated hydriodic acid (55 to 58 percent solution). Chemical destruction is hazardous and should only be done by trained personnel in a proper environment (e.g. licensed facility, well-ventilated area, safety equipment and procedures, etc.) Prior CSA approval is required.

- Due to the proliferation, wide spread use, interoperability, low cost of USB technologies throughout the Global Information Grid (GIG), USB media and equipment no longer required to store or process classified information must be destroyed.

B. The National Security Agency (NSA) Classified Material Conversion (CMC) destruction facility may be utilized by qualified and registered contractors. NSA CMC will accept all COMSEC hardware and materials (regardless of ownership), classified Government Furnished Equipment (GFE) (including media), and Special Access Program (SAP) information from contractor facilities, with the prior endorsement of a government contracting officer (CO) or contracting officer representative (COR) in accordance with NSA CMC contractor registration procedures reflected in NSA guidance "Contractor Request for NSA CDC Services". Guidance for registration for NSA destruction services is also available on the DSS website.