



INTELLIGENCE

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

JUL 20

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DIRECTOR, FORCE TRANSFORMATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, ADMINISTRATION AND
MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy and Procedures for Sanitization of Department of Defense
(DoD) Classified or Controlled Unclassified Information Prior to
Public Release

REFERENCE: (a) DoD 5200.1-R "Information Security Program," January 1997
(b) DoD Directive 5230.29 "Security and Policy Review of DoD
Information for Public Release," August 6, 1999

Recent events have highlighted the need to reinforce the policy and procedures for consistent sanitization of DoD classified or controlled unclassified information.

In accordance with references (a) and (b), the attached procedures are mandatory when sanitizing information from either hard copy or electronic documents that are intended for release. It is imperative that personnel who are performing sanitization duties understand the vulnerabilities surrounding the process, as well as the importance of performing this activity consistently and reliably using only approved procedures, products, and software.



These procedures are necessary because information can be recovered if not correctly sanitized. We are coordinating with NSA and ASD/NII about the suitability of COTS products to perform sanitization functions in a seamless, integrated fashion. Until such solutions are identified, tested, and approved, rigorous adherence to the attached procedures is essential. Organizations that have already established electronic redaction methods in which the text is replaced by solid black or white (pixel replacement) technologies may continue to utilize this software and upload the resulting sanitized products to information systems for electronic release.

A handwritten signature in black ink, appearing to read "S. Cambone", with a long horizontal flourish extending to the right.

Stephen A. Cambone

Attachment
As stated

SANITIZATION PROCEDURES

A. Hard-copy sanitization options:

(1) Conduct security review and physically remove information with an Exacto-style razor knife or scissors. Photocopy sanitized document, and distribute as required.

(2) Conduct security review and black-out or tape over the information using one of the following approved products:

- Charpak Graphic Tape (black plastic tape);
- Post-it Correction and Cover-up Tape (white paper tape, 2-line, id #652, from 3M);
- Pres-a-ply correction tape (white-1 line), id #43 161, from Dennison or,
- Liquid Paper Dryline (white) from PaperMate.

(3) After the process is complete, create black and white photocopy and review the final product to verify that no deleted information is visible. When complete, distribute as required.

B. Electronic sanitization options:

(1) Conduct security review and black-out information intended for sanitization. If approved by an Activity or Command Information System Security Officer, Commercial Off-the-Shelf (COTS) products may be used to create a sanitized camera-ready version of a document. Print a hard copy sanitized version. Manually rescan the sanitized document and convert it to a graphics format (e.g., TIF or .pdf). Upload to appropriate information system, conduct any additional format conversions to facilitate distribution (e.g., .pdf) and release (e-mail, website posting, or via hard copy) as required.

(2) The photocopy sanitized product described in paragraph A(2) above may also be scanned, converted to a graphics format, uploaded, and further processed as described above.