OUTLINE SHEET 5.2

Destruction

REFERENCES

SECNAV M-5510.36, Chapters 2 and 10
IA Pub P-5239-26, Remanence Security Guidebook

OUTLINE

A. Basic Policy (ISP 10-17)

1. Destruction of unneeded classified information is essential to an effective command security program

2. Benefits of reducing classified holdings

   - Allows for better protection
   - Reduces storage needed
   - Reduces administrative workload
   - Better prepared for emergency

3. Classified records "Clean out" day – COs should establish to destroy unneeded classified and controlled unclassified holdings

B. Destruction Procedures (ISP 10-19)

1. Use only authorized means and personnel cleared to level of information being destroyed

2. Destruction records **(CNO ltr 5510 ser N09N2/9U223112 of 7 May 09, Interim Policy Changes, Reminders and Clarifying Guidance to SECNAV M-5510.36)**

   a. Secret and Confidential information – require no record of destruction except for special types of classified information or removable storage devices (i.e., removable hard drives; however administrative procedures for recording destruction must be established

      (1) See applicable instructions for destruction requirements for special types of classified information

(2) Removable storage devices (Classified (non-SCI) and CUI unclassified hard drives (internal and removable) connected to Navy networks **(NTD 12-08, Disposition of Navy Hard Drives)**

- Use one of 2 approved disposition methods: Ship to National Security Agency for degaussing and crushing. For guidance see www.nsa.gov/cmc (for OCONUS shipments follow ISP, Chapter 9)*or* Use a NSA certified service

- Upon immediate removal from network, working with IAM, ensure accurate records are maintained for each hard drive being disposed of – must associate hard drive to a specific computer/component

- Final disposition – Not considered destroyed until command receipt of CMC Record of Destruction of Classified Material (or similar form from approved destruction facility if not done by CMC) and matched with local command records

NOTE: All classified and CUI hard drives within NNPI and NCIS will not be turned over to EDS during tech refresh.

b. For Top Secret, record required - Can use:

(1) OPNAV Form 5511/12, Classified Material Destruction (see Student CD for form) or any other record (e.g., log book or computerized log) that:

- Fully identifies material
- Shows number of copies destroyed
- Is signed by 2 cleared witnesses
- Shows date of destruction

(2) Retain Top Secret record 5 years **(ISP 2-3)**

NOTE: Record of destruction not required for Top Secret waste products (TS working papers are not considered "waste products"

3. Burn bags – Used if classified information cannot be immediately destroyed at the command. Ensure adequate

storage in GSA approved storage facilities prior to destruction

a. Striped burn bags (although not required), marked and stored according to classification level until actually destroyed, are useful in that they identify contents as classified; other types of bags should be properly marked so as to not be mistaken for trash

b. Seal and safeguard bags awaiting destruction at level of classified information they contain

c. Use an enclosed vehicle to transport burn bags for destruction

4. Requirements for destruction detail personnel

- Cleared
- Familiar with regulations and procedures
- Trained (equipment operating procedures, emergencies, cleanup)
- Rotated periodically

C. Methods of Destruction (ISP 10-18)

1. Use method that prevents later recognition or reconstruction

2. Methods

a. Burning

b. Crosscut shredder

(1) Shreds to no greater than 5 square millimeters

NOTE: Must be purchased from NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders (see www.navysecurity.navy.mil for latest information on crosscut shredders)

(2) Some special programs require more stringent control of shred residue, e.g., burning, mixing with soap/water, or mixing with unclassified residue.

c. Pulverizers and disintegrators – Residue shall not exceed 5 square millimeters in size

d. Mutilation - Rendering the information permanently destroyed

e. Chemical Decomposition - Using chemicals to render the information permanently destroyed

f. Pulping (wet process) 1/4″ or smaller security screen - used for water-soluble material

3. Selecting destruction equipment

Does it meet shred size specs?
Does it meet safety standards?
Does it meet local pollution standards?
What are maintenance requirements?
Is it simple to use?
Will it meet requirements?
Can you substantiate/justify cost?

D. Destruction of Non-Paper Classified information

1. IT media **(IT Pub P-5239-26, Remanence Security Guidebook)**

a. Hard drives (see NTD 12/08)

b. Floppy disks - Destroy by incineration, or remove outer cover and shred the internal disk with cross cut shredder or pulverizer. Mix material with paper to lessen the chance of clogging machine

NOTE: May also use Degausser/Eraser equipment

c. Magnetic tapes - Remove classified information by degaussing (exposing tape to a magnetic force) Degaussing devices are approved by National Security Agency and available through the National Supply System

2. Equipment - Remove the classified component and store in security container until properly destroyed

3. Film and negatives – Incinerate, shred through an approved crosscut shredder, or pulverize

4. CD Media **(IA Pub P-5239-26)**

a. Approved equipment can be purchased off the GSA schedule for destruction of CDs

NOTE: Only an approved CD declassifier may be used to remove classified data bearing surfaces. Classified CDs may not be broken up.

b. CDs can also be transmitted to NSA for destruction

See website http://www.nsa.gov\cmc for guidance on shipping, receipt requirement (CMC Procedures and Forms) and other services provided by NSA'S Classified Material Conversion

E. Destruction of Controlled Unclassified Material (ISP 10-20)

1. Destroy CUI, DOD UCNI, DOE UCNI, FOUO, and technical documents by any means approved for the destruction of classified information or by any means that would make it difficult to recognize or reconstruct the information – Records of destruction not required

2. IT storage media containing digital FOUO, CUI and unclassified technical documents shall, at a minimum, be reformatted prior to reuse within a DOD IT system

3. Destroy unclassified NNPI in same manner approved for classified information

F. Commands Removed from Active Status (ISP 10-21)

1. Dispose of classified information by approved means or store at approved facility if status is temporary

2. CO will certify to accepting command that:

a. Security Inspection conducted and all classified information has been removed, and

b. Provide documentation for information left aboard

G. Emergency Destruction Supplement (ISP Exhibit 2B Part Two)

1. Required for command emergency plans for commands located outside the U.S. and its territories and deployable units. Any reasonable means of ensuring that classified information cannot be reconstructed is authorized for emergency destruction

NOTE: For COMSEC information, refer to CMS/EKMS program guidance

2. Factors to be considered in planning

- Volume and sensitivity of information held
- Proximity to hostile forces
- Need to remain operational

3. Formalizing an Emergency Destruction Supplement

    a. Be specific - list procedures and methods to be used (e.g., document shredders, weighted bags, etc.)

    b. Identify exact locations of classified information, including specific drawers, shelves, sections of security containers

    c. Establish destruction priorities

    Priority 1 - Top Secret (includes all categories; destroy any special program material first, then GENSER)

    If time allows, destroy Priority 2 (Secret) special program then GENSER, and Priority 3 (Confidential) special program then GENSER

    NOTE: Jettisoning or sinking are methods that can be used in an emergency

    d. Be specific in tasking - Use billet designations; e.g., Admin Officer will...

    e. Establish reporting requirements to account for material destroyed/not destroyed; make report to CNO (N09N2) and Admin chain of command

    f. Conduct drills as necessary to train personnel

4. Naval surface noncombatant vessels operating in hostile areas without escort shall have appropriate equipment on board prepared for use

5. Measures to precede emergency destruction planning

    a. Reduce amount of classified information to minimum

    b. Store infrequently used information at a more secure command

    c. Transfer to digital media to reduce volume needed to be transferred or destroyed