BASIC GUIDE TO INFORMATION SECURITY

MARCH 2015

CDSE

Center for Development of Security Excellence | 938 Elkridge Landing Road | Linthicum, MD 21090

PURPOSE

This guide describes basic security procedures that you should be aware of when handling classified material at your organization. Included are common procedures associated with each particular work environment or task. Be sure to contact your local security office for more detailed information on these and other pertinent procedures. Security managers and officers can also incorporate elements of this guide into their security education and training programs as appropriate.

LAYOUT

This guide is divided into sections by the functional areas commonly found in an organization (See "Contents" below). Within these sections, security procedures or concerns are described. If your job dictates duties other than those described, check with your local security office or look at the "Contents" to see if those other procedures are described in another section. Each area also includes an Organization Requirements section where you can include notes on items concerning local procedures, requirements, etc.

CONTENTS

3 Security Containers
4 Transmission and Transportation
6 Marking Classified Information
7 Classified Reproduction
8 Classified Destruction
9 Classified Information Systems
10 Other Procedures and Requirements

REFERENCES

- DoDM 5200.01, Vol. 1- 4, DoD Information Security Program, February 24, 2012, as amended
- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 28, 2006, as amended

SECURITY CONTAINERS

GENERAL REQUIREMENTS:

- Store all classified in locked containers unless someone is present in the room who has authorized access
- Security containers must be GSA-approved and equipped with an approved combination lock
- Do not share the container's combination with anyone unless they have the appropriate clearance and need-to-know

COMPLETE THE SF 702 (SECURITY CONTAINER CHECK SHEET) EACH TIME YOU:

- Open the container
- Close the container
- Check the container at end of day. Contractors: Use of SF 702 not required under the NISPOM

CHANGE THE COMBINATION:

- When you first put the container into use
- When someone who knows the combination leaves the office (transfer, employment termination, etc.)

- When the combination is compromised
- Use the SF 700 (Security Container Information) to record the combination and mark accordingly
- Change the security container combination to the factory default (50-25-50) when it is removed from service (e.g. disposal, replacement, surplus)

HANDLING CLASSIFIED MATERIALS WHEN THEY ARE NOT IN A SECURITY CONTAINER

- Always ensure classified is under your direct control or that of someone who has the appropriate clearance and is authorized access
- Put the appropriate cover sheet (Orange colored SF 703 for Top Secret; Red SF 704 for Secret; Blue SF 705 for Confidential) on the materials. Contractors can use the SF 703–705 or company-generated equivalent coversheet.

ORGANIZATION REQUIREMENTS

TRANSMISSION AND TRANSPORTATION

RECEIVING CLASSIFIED MATERIAL

- Protect incoming material until it has been determined whether or not classified materials are contained within
- Deliver classified material directly to the addressee or store in designated security container until addressee can receive the material

HOW TO PREPARE CLASSIFIED MATERIALS FOR TRANSMISSION AND TRANSPORTATION

- Double wrap material to be transmitted or transported (use opaque materials)
- Place classification markings on inner layer
- Attach or enclose receipt(s) as required within the inner layer
- Do not indicate classification on outside layer
- Seal package in such a way that tampering can be detected
- Address package to an official address, not to a person (Inner layer can be addressed to a person)

METHODS FOR MAILING AND SHIPPING CLASSIFIED MATERIALS

- Top Secret: Mailing is not authorized (check with your security office for Top Secret transmission information.)
- Secret:
  - U.S. Postal Service (USPS) Registered Mail (within U.S. and Puerto Rico)
  - USPS Registered Mail to APO/FPO, but only if mail will not pass out of U.S. control during the entire mail process
  - USPS Priority Mail Express (formerly USPS Express Mail) within U.S. and Puerto Rico. Do not use to send to APO/FPO address and do not use street-side collection box. Do NOT waive recipient signature requirement.
  - Protective Security Service (PSS) within U.S. boundaries if item is large and bulky
  - GSA contract holder for overnight delivery within U.S. and territories (Contact your security office for additional information)
- Confidential:
  - Methods approved for mailing Secret material
  - USPS Registered Mail (for APO/FPO outside U.S. and Territories; when uncertain if destination within U.S.; to DoD contractor or other Executive Branch agency, when required)
  - USPS First Class Mail between DoD activities within the U.S. and Territories (Outer wrapper shall be endorsed: "Return Service Requested")
  - USPS Certified Mail to DoD contractor or other Executive Branch agency
  - Constant Surveillance Service (CSS) within U.S. boundaries if item is large and bulky

ORGANIZATION REQUIREMENTS

TRANSMISSION AND TRANSPORTATION (CONTINUED)

HAND-CARRYING CLASSIFIED MATERIAL

- Hand-carrying adds additional risks and responsibilities. Use it only after all other transmission methods are inadequate.
- Double wrap the materials
- Keep materials under constant surveillance and in your personal possession
- Do not place in a detachable storage compartment (e.g., auto trailer, etc.)
- Store overnight only at a U.S. Government facility or cleared contractor facility with appropriate storage capability
- Leave an inventory of the materials being hand-carried with your activity
- Receive a hand-carry/courier briefing
- If hand-carrying on a commercial aircraft:
  - Coordinate with the local Transportation Security Administration (TSA) office before leaving
  - Have proper ID and letter of authorization or courier card
  - Allow X-raying but do not allow direct access to the information
- Check with your security office for more information on any additional hand-carrying requirements, (e.g. , Courier Card, etc.)

ORGANIZATION REQUIREMENTS

MARKING CLASSIFIED INFORMATION

MINIMUM MARKING REQUIREMENTS FOR DERIVATIVELY CLASSIFIED DOCUMENTS

- First, mark all portions (paragraphs, drawings, captions, and subject/title lines) with highest level of classification (and dissemination controls) found within that portion. Place marking at beginning of each portion by using approved abbreviations and placing within parentheses.
- Second, conspicuously mark at the top and bottom of each interior page (all pages except the title page, if any, and first page) the highest classification of information (and dissemination controls, if any) contained on that particular page.
- Third, mark the top and bottom of:
  - the front cover, if any,
  - the title page, if any,
  - the first page, and
  - the outside of the back cover, if any, with highest level of classification of information and dissemination controls contained within the document.
- Fourth, place on the front of the document a classification authority block which contains the:
  - "Classified By" line with name/position title or personal identifier of the derivative classifier and agency and office of origin if not otherwise evident
  - "Derived From" line,
  - "Downgrade To" line/ instructions, if applicable,
  - "Declassify On" line

MARKING DOCUMENTS ON COMPUTER MEDIA (E.G., HARD DRIVE, CD, DVD, FLOPPY DISK)

- Mark portions electronically
- Apply interior page markings, overall document markings, and applicable associated markings ("Classified By" line, etc.) electronically, if feasible; otherwise mechanically (either using stamps or a typewriter) place these markings on the hard copy document after it is printed.

MARKING COMPUTER MEDIA

Use the following labels to indicate highest level of classification (and dissemination controls) contained on the media:

- SF 706 (Top Secret)
- SF 707 (Secret)
- SF 708 (Confidential)
- SF 711 (Data Descriptor)
- Contractors may use a company-generated equivalent label

- Affix SF 710 (Unclassified label) on unclassified media that are stored with classified media or used in an environment with classified materials (Contractors may use a company-generated equivalent label).

ORGANIZATION REQUIREMENTS

CLASSIFIED REPRODUCTION

- Use equipment for which classified reproduction has been designated and authorized
- Keep reproduction to the minimum necessary to meet mission requirements
- Limitations and control procedures that apply to the originals must also be applied to the copies
- Always check the copier to be sure that no classified originals or copies are left in it
- Place poor quality or unreadable copies in an authorized container and destroy them as soon as possible
- Contractors: Obtain authorization from contracting activity for Top Secret unless contract requires reproduction. Keep record of reproduction of Top Secret (2 years).

ORGANIZATION REQUIREMENTS

CLASSIFIED DESTRUCTION

REQUIREMENTS

- Check with your security office and/or records management office to identify those files that are considered "record files" and "historical files" for your office
- Destroy document if it is a "non-record" document and there is no longer an operational need for it
- Conduct an annual cleanout day (identify documents no longer needed and destroy)

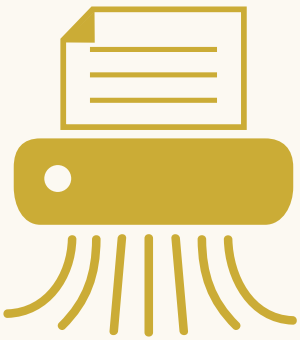
WHO CAN DESTROY CLASSIFIED MATERIALS

- User (or custodian) of the material;
- Designated destruction official(s) for your activity, if applicable

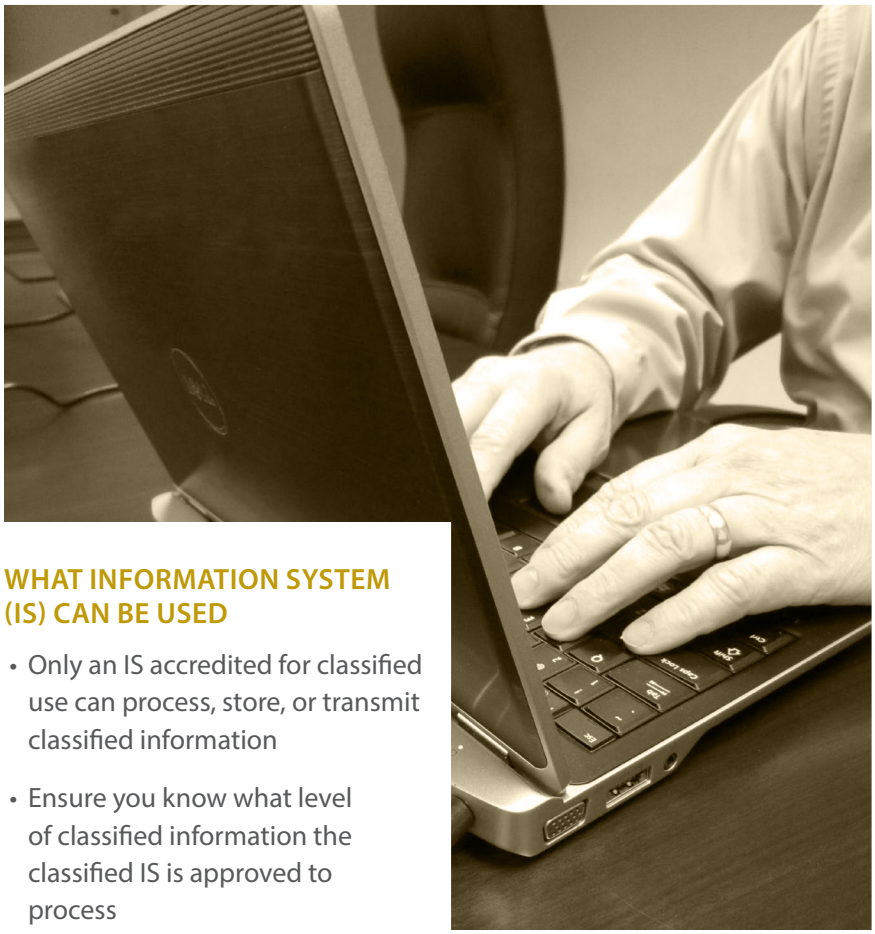
DESTRUCTION METHODS

- Burning
- Shredding
- Pulverizing
- Pulping
- Chemical Decomposition
- Check with your security office for approved destruction methods, procedures, and the location of destruction equipment. Contractors should use approved methods listed in the NISPOM

ORGANIZATION REQUIREMENTS



CLASSIFIED INFORMATION SYSTEMS



WHAT INFORMATION SYSTEM (IS) CAN BE USED

- Only an IS accredited for classified use can process, store, or transmit classified information
- Ensure you know what level of classified information the classified IS is approved to process

WHAT TO DO WITH THE COMPUTER MEDIA

- Indicate on the hard drive, CD, DVD, etc. the classification level of the information on it. (One of the SF 706, 707, 708, 709, or 710 labels can be used to accomplish this.)
- Properly destroy media using approved methods or procedures
- Store the media in an approved security container when:
  - You leave the area and no authorized persons are there
  - You are finished with your classified processing session

WHO CAN HAVE ACCESS

- Only people with appropriate clearance, need-to-know, and a valid user account for the classified IS can have access

ORGANIZATION REQUIREMENTS

OTHER PROCEDURES AND REQUIREMENTS

DISCUSSION OF CLASSIFIED INFORMATION ON THE PHONE

- Use Secure Telephone Equipment (STE) or other authorized secure communication method
- Follow the encryption procedures for that piece of equipment
- Do not discuss classified information at a level higher than the secure connection allows
- Ensure other people are not within hearing range of your voice

FAXING CLASSIFIED INFORMATION

- Use a secure fax unit
- Follow the encryption procedures for that piece of equipment
- Do not transmit classified information at a level higher than the secure connection allows
- Header or cover sheets for classified faxes must be marked with the highest level of classified material transmitted
- Before transmitting, call the receiving office to ensure an authorized person is available to receive the transmission
- Classified documents that are faxed must be marked as a finished document
- Remain with the unit until the transmission or reception is complete

END OF THE DAY SECURITY CHECK

- Check the entire work area for classified materials
- Check the security container to ensure it is locked
- Record this check on SF 701 (Activity Security Checklist)
- Perform the above steps if you work with classified materials during non-working hours

CLASSIFIED ACCOUNTABILITY REQUIREMENTS

- Check with your security office if accountability requirements exist for Top Secret, Secret, and/or Confidential material

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

- CUI is unclassified information requiring safeguarding and dissemination controls in accordance with government policies, regulations, and laws
- CUI includes For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive But Unclassified (SBU), and Privacy Act information
- Only persons with a valid need to know may access CUI (no clearance is required, however.)
- Check with your local security office and/or contract documentation (e.g., DD Form 254) for specific CUI safeguarding and dissemination procedures/ requirements.

ORGANIZATION REQUIREMENTS