

Department of Defense Security Institute

and

Joint Industry-Government
Security Awareness Group



THE LAYMAN'S GUIDE TO SECURITY

March 1997

Defense Security Institute
Information Security Team
8000 Jefferson Davis Highway
Richmond, Virginia 23297-5091

DSN 695-4893
COMM (804) 279-4893
FAX (804) 279-5239



"KILROY IS BACK" graphics by Chip Beck

Purpose

This booklet describes some of the basic security procedures that you should be aware of when handling classified materials in your work environment. The procedures described within are not all encompassing. We have included only those that are commonly associated with each particular office environment. Be sure to contact your local security office for more detailed information on these and other pertinent procedures. Use this booklet as an introduction to security or as a security refresher/reminder.

Layout

The booklet is divided into sections by the functional duties (see "Contents" below) commonly found in an organization. Within these sections, the more likely 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 "Index" to see if those other procedures are described in another section.

Contents

Distribution Courier
Reproduction Services
Typist/Word Processing Personnel
Mail Room
Administrative Support Personnel
Secretary
Other Information

NOTE: U.S. government activities and their contractors may reproduce this booklet.

Distribution Courier
Procedures to follow when reproducing classified materials

Who can have access

- Give access to classified only to people with appropriate clearance and need-to-know.

What to do while distributing classified materials

- Keep materials in your personal possession at all times until you can hand it directly to someone else who has a clearance and is authorized access to it.
- Never leave classified materials unattended while delivery is being made.

What to do when no one is in the office to receive the mail

- Keep the materials in your possession.
- Take it back to the distribution point and hand it to an authorized person or put it in an approved container,
or
- Deliver it to the office at a later time and hand it to an authorized person.



Organization Requirements

Reproduction Services

- Use machines for which classified reproduction has been authorized and so designated.
- Ensure latent images will not cause compromise.
- 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 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).

Who can have access

- Give access to classified only to people with appropriate clearance and need-to-know.



Organization Requirements

Organization Requirements

Reproduction Services (continued)

Using your security container

- Store all classified in locked container unless someone is present in the room who is authorized access.
- Fill out SF 702 (Security Container Check Sheet) each time you:
 - open
 - close
 - or
 - checkthe container. [SF 702 not required under NISPOM.]
- Change your combination:
 - when you first put the container into use.
 - when someone who knows the combination leaves the office (transfer, extended absence, etc.).
 - when the combination is compromised.
 - when there is an open container security violation.



Handling classified materials when they are not in a security container

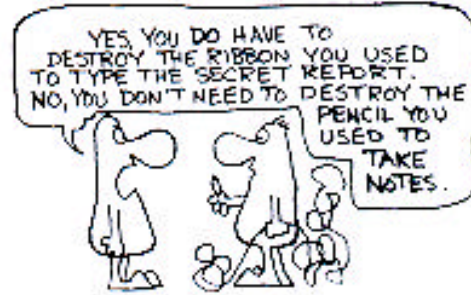
- Always ensure classified is under your direct control or that of someone who has the appropriate clearance and is authorized access.
- Put the appropriate cover sheet (Orange colored SF 703 for Top Secret; Red SF 704 for Secret; Blue SF 705 for Confidential) on the materials. [Not required under NISPOM .]

Organization Requirements

Typist/Word Processing Personnel

What to do with the typewriter/printer ribbon

- Indicate on the cartridge/cassette the classification level of the information on it. (One of the SF [706, 707, 708, 709, 710] labels can be used to accomplish this.) Properly destroy the cartridge/cassette as soon as feasible.
- Store the cartridge/cassette in an approved security container when:
 - you leave the area and no authorized persons are there (if there is an authorized person around, be sure to tell them that the classified ribbon is there).
 - you are finished with your typing.



What to do with the disk

- Place the proper classification label on the diskette.
- Store the diskette in a proper security container when:
 - you leave the area and no authorized persons are there (if there is an authorized person around, tell them that the classified diskette is there).
 - you are not using the diskette.

What to do with the materials while typing

- Do not leave the classified materials alone. If you must leave:
 - ensure that an authorized person is there (tell them about the materials), or
 - lock the materials in an authorized security container.

What to do with the drafts/notes/etc.

- Store the classified drafts/notes/etc. in an authorized security container.
- Give it to whoever wrote it or to someone with appropriate clearance and need-to-know.

Who can have access

- Give access to classified only to people with appropriate clearance and need-to-know.

Organization Requirements

Organization Requirements

Mail Room

Using your security container

- Store all classified in locked container unless someone is present in the room who is authorized access.
- Fill out SF 702 (Security Container Check Sheet) each time you:
 - open,
 - close, or
 - check the container. (SF 702 not required under NISPOM.)
- Change your combination:
 - when you first put the container into use.
 - when someone who knows the combination leaves the office (transfer, extended absence, etc.).
 - when the combination is compromised.
 - when there is an open container security violation.



Handling of mail

- Protect mail until it has been determined whether or not classified materials are contained within.
- For DoD contractors: Ensure only cleared personnel receive and sign for all certified and registered mail.

Handling classified materials when they are not in a security container

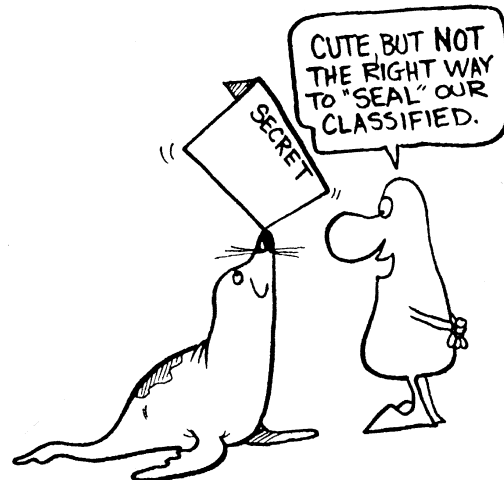
- Always ensure classified is under your direct control or that of someone who has the appropriate clearance and is authorized access.
- Put appropriate cover sheet (Orange colored SF 703 for Top Secret; Red SF 704 for Secret; Blue SF 705 for Confidential) on materials. [Not required under NISPOM.]

Who can have access

- Give access to classified only to people with appropriate clearance and need-to-know.

How to prepare classified materials for movement

- Double wrap (use opaque materials).
- Place classification markings on 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.



Mail Room (continued)

Methods for mailing classified materials

- Top Secret: mailing not authorized.
- Secret:
 - Registered mail (within U.S. and Puerto Rico).
 - Registered mail to APO/FPO but only if mail will not pass out of U.S. control during entire mail process.
 - Protective Security Service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service).
 - U.S. Postal Service 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. Use only as a last resort.
 - GSA contract holder for overnight delivery (currently FedEx) (within US & territories). (See your security office for limitations and procedures.)
- Confidential:
 - Registered mail (for APO/FPO outside U.S. and Territories; for NATO outside U.S.; when uncertain if destination within U.S.; to DoD contractor or other Executive Branch agency, when appropriate).
 - First Class mail between DoD activities within the U.S. and Territories.
 - Certified mail to DoD contractor or other Executive Branch agency.
 - Constant Surveillance Service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service).



Using distribution systems

- Ensure classified materials are not left alone in distribution boxes.
- Ensure only authorized personnel (with appropriate clearance and need-to-know) pick up the classified materials.

End of the day security check

- Check the entire work area for classified materials.
- Check the container to ensure it is locked.
- Record this check on SF 701 (Activity Security Checklist). [701 not required under NISPOM.]
- Perform the above steps if you work with classified materials during non-working hours.

Organization Requirements

Administrative Support Personnel

Minimum marking requirements for paper products

- First, mark all portions (paragraphs, drawings, captions, and subject/title lines) with highest level of classification [and restrictive warning notices/caveats] found within that portion. Place marking at beginning of each portion (except subject/title lines are marked after the portion) by using 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 restrictive caveats, if any) contained on that particular page.
- Third, mark the top and bottom of 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 contained within the document.
- Fourth, for a derivatively classified document, place on the front of the document the:
 - "derived from" line,
 - "declassify on" line,
 - downgrading instructions, if any,
 - restrictive caveats, if any,
 - originating office and date

[Check with your security office for how to mark an originally classified document.]

How to mark documents on disks

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

How to mark disks

- Use:
 - SF 706 (Top Secret label)
 - SF 707 (Secret label)
 - SF 708 (Confidential label)
 - SF 711 (Data Descriptor label)to indicate highest level of classification contained on disk. [SFs not required under NISPOM.]
- Place SF 710 (Unclassified label) on unclassified disks that are stored with classified disks or used in an environment with classified materials. [SF not required under NISPOM.]

Administrative Support Personnel (continued)

Faxing classified information

- Use a secure FAX unit.
- Follow the encryption procedures for that piece of equipment.
- Before transmitting, call the receiving office to ensure an authorized person is available to receive the transmission.
- Remain with the unit until the transmission or reception is complete.

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. [Not required under NISPOM.]

Using your security container

- Store all classified in locked container unless someone is present in the room who is authorized access.
- Fill out SF 702 (Security Container Check Sheet) each time you:
 - open,
 - close, or
 - check the container. [SF 702 not required under NISPOM.]
- Change your combination:
 - when you first put the container into use.
 - when someone who knows the combination leaves the office (transfer, extended absence, etc.).
 - when the combination is compromised.
 - when there is an open container security violation.



End of the day security check

- Check the entire work area for classified materials.
- Check the container to ensure it is locked.
- Record this check on SF 701 (Activity Security Checklist). [701 not required under NISPOM.]
- Perform the above steps if you work with classified materials during non-working hours.

Administrative Support Personnel (continued)

Who can have access

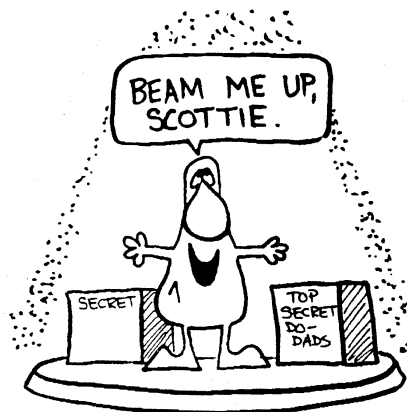
- Give access to classified only to people with appropriate clearance and need-to-know.

Transporting from office to office

- Do not attract attention to yourself when carrying classified materials from one office to another. Place the materials in a nondescript envelope or container.
- Place cover sheet (SF 703, 704, or 705) on materials prior to placing into envelope to remind yourself and recipient that materials are classified. [SFs not required under NISPOM.]

How to prepare classified materials for movement

- Double wrap (use opaque materials).
- Place classification markings on 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.



Organization Requirements

--

Secretary

Minimum marking requirements for paper products

- First, mark all portions (paragraphs, drawings, captions, and subject/title lines) with highest level of classification [and restrictive warning notices/caveats] found within that portion. Place marking at beginning of each portion (except subject/title lines are marked after the portion) by using 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 restrictive caveats, if any) contained on that particular page.
- Third, mark the top and bottom of 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 contained within the document.
- Fourth, for a derivatively classified document, place on the front of the document the:
 - "derived from" line,
 - "declassify on" line,
 - downgrading instructions, if any,
 - restrictive caveats, if any,
 - originating office and date

[Check with your security office for how to mark an originally classified document.]



How to mark documents on disks

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

How to mark disks

- Use:
 - SF 706 (Top Secret label)
 - SF 707 (Secret label)
 - SF 708 (Confidential label)
 - SF 711 (Data Descriptor label)

to indicate highest level of classification contained on disk. [SFs not required under NISPOM.]

- Place SF 710 (Unclassified label) on unclassified disks that are stored with classified disks or used in an environment with classified materials. [SF not required under NISPOM.]

Secretary (continued)

Faxing classified information

- Use a secure FAX unit.
- Follow the encryption procedures for that piece of equipment.
- Before transmitting, call the receiving office to ensure an authorized person is available to receive the transmission.
- Remain with the unit until the transmission or reception is complete.

Who can have access

- Give access to classified only to people with appropriate clearance and need-to-know.

Using your security container

- Store all classified in locked container unless someone is present in the room who is authorized access.
- Fill out SF 702 (Security Container Check Sheet) each time you:
 - open,
 - close, or
 - checkthe container. [SF 702 not required under NISPOM.]
- Change your combination:
 - when you first put the container into use.
 - when someone who knows the combination leaves the office (transfer, extended absence, etc.).
 - when the combination is compromised.
 - when there is an open container security violation.

End of the day security check

- Check the entire work area for classified materials.
- Check the container to ensure it is locked.
- Record this check on SF 701 (Activity Security Checklist). [701 not required under NISPOM.]
- Perform the above steps if you work with classified materials during non-working hours.

Organization Requirements

Secretary (continued)

Transporting from office to office

- Do not attract attention to yourself when carrying classified materials from one office to another. Place the materials in a nondescript envelope or container.
- Place cover sheet (SF 703, 704, or 705) on materials prior to placing into envelope to remind yourself and recipient that materials are classified. [SFs not required under NISPOM.]

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. [Not required under NISPOM.]



How to prepare classified materials for movement

- Double wrap (use opaque materials).
- Place classification markings on 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.

What to destroy

- Check with your records management office to identify those files that are considered "record files" and "historical files" for your office.
- Destroy document if it's a "non-record" document and no operational need for it.
- Conduct annual cleanout day (identify documents no longer needed and destroy).
- Contractors: Recommend you check with contracting agency prior to destruction.

Organization Requirements

Secretary (continued)

How to destroy classified materials

- Burning, (if allowed by your local environmental control agency).
- Shredding (particle size must meet standard set by your component).
- Pulverizing (standard for equipment set by your component).
- Pulping (standard for equipment set by your component).

Check with your security office for location of equipment and information on other methods.

Contractors: Approved methods listed in NISPOM.



Accountability systems

- Check with the security office for your activity's accountability requirements for Top Secret, Secret, and Confidential materials.

Organization Requirements

Other Information

Discussion of classified information on the phone

- Use a STU-III or some other authorized secure communication method.
- Follow the encryption procedures for that piece of equipment.
- Ensure that other people are not within hearing range of your voice.

Who can destroy classified materials

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

Methods for transmitting classified materials

- Top Secret:
 - Defense Courier Service.
 - Department of State courier system.
 - Authorized component courier service.
 - Authorized electronic system, e.g., a STU-III.
 - Handcarrying (with proper authorization).
- Secret:
 - Authorized component courier service.
 - Authorized electronic system, e.g. a STU-III.
 - Handcarrying (with proper authorization).
 - Defense Courier Service (not routinely but under certain circumstances).
 - Registered mail (within U.S. and Puerto Rico).
 - Registered mail to APO/FPO but only if mail will not pass out of U.S. control during entire mail process.
 - Protective Security Service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service).
 - U.S. Postal Service Express Mail (within U.S. and Puerto Rico). Do not use to send to an APO/FPO address and do not use street-side collection box. Use only as a last resort.
 - GSA contract holder for overnight delivery (currently FedEx) (within US and territories). (See your security office for limitations and procedures.)
- Confidential:
 - Authorized component courier service.
 - Authorized electronic system, e.g., a STU-III.
 - Handcarrying (with proper authorization).
 - Defense Courier Service (not routinely but under certain circumstances).
 - Registered mail (for APO/FPO outside U.S. and Puerto Rico; for NATO outside U.S.; when uncertain if destination within U.S.; to DoD contractor or other Executive Branch agency, when appropriate).
 - First Class mail between DoD activities within the U.S. and Territories.
 - Certified mail to DoD contractor or other Executive Branch agency.
 - Constant Surveillance Service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service).



Other Information (continued)

Handcarrying

- Use handcarrying as your last means for transmitting classified materials. Use it only after all other transmission methods have been found inadequate.
- Double wrap the materials.
- Keep materials under constant surveillance and personal possession.
- Do not place in detachable storage compartment, e.g., auto trailer, luggage rack, etc.
- Store overnight only at a U.S. government facility or cleared contractor facility with storage capability.
- Leave with your activity a list of the materials being handcarried.
- Get briefed.
- If using a commercial airline:
 - coordinate with the airline before leaving.
 - have ID and letter of authorization.
 - allow X-raying but do not allow direct access to the information.



Check with your security office for more information on handcarrying.

