Defense Security Service

"SURVIVAL HANDBOOK"

The Basic Security
Procedures Necessary For
Keeping You Out of Trouble

June 2002

Defense Security Service Academy
938 Elkridge Landing Rd
Linthicum, MD 21090

DSN 283-8171
COMM 410-865-3171
FAX 410-865-2704, DSN 283-7704

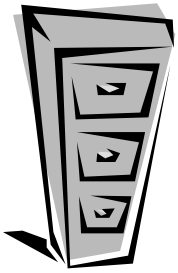
Security Points of Contacts		
Name:	Security Program/ Subject Matter:	Phone Number:

Pertinent Security Regulations	
Number:	Subject/Title:

As we are well aware, there are a multitude of security practices and procedures that must be followed in order to protect classified materials. The sheer volume of procedures can be intimidating to anyone. This pamphlet describes the basic security procedures that we should know to keep us out of trouble when handling classified materials on a daily basis. Be sure to contact your local security office for more detailed information on these and other pertinent security procedures.

Contents

- Using your security container
- How to handle classified materials when it is outside of the container
- How to derivatively classify
- How to mark your documents
- How to transmit classified materials
- How to destroy classified materials
- Procedures to follow when typing classified
- Using the phone/FAX for classified
- Rules for taking classified home to work on
- End of the day security check



Using Your Security Container

SF 700 (Security Container Information) is used:

- to record the names of personnel to recall if there is a problem with the security container.
- to record the combination.

SF 702 (Security Container Check Sheet) is used:

- to record the opening and closing of the container.
- to record the action of someone checking the container to ensure that it is locked.

When choosing combinations:

- Do not use the factory setting of 50-25-50.
- Do not use a combination where all numbers end in 0 or 5.
- Do not use numbers that are peculiar to you or to your activity (e.g., phone numbers, birthdays, etc.).
- Do not use sequential number sets such as 11-22-33.
- Do not use numbers of one container to build on another (e.g., container #1 is 10-20-30 and container # 2 is 10-20-31).

Handle your combination as classified information (at the same classification level as the materials that the container protects).

You should be using a GSA approved security container to store your classified materials. To verify that your container is a GSA approved one, call your local security office. A GSA approved security container:

- has a label that indicates it is an approved container. (This label is located on the face of the top drawer.)
- has a second label inside the container that is called a test certification label. (It will be found on the locking drawer.)
- cannot be locked if one of the non-locking drawers is in the open position.

Contact your local security office for exceptions and further details concerning the above.

How to Handle Classified Materials When It Is Outside of a Container

Whenever you have a classified document outside of a container, it must always be under your direct control. If you are not actively using that document, place a cover sheet over it.

Cover sheets [SF 703 (Top Secret - Orange colored), 704 (Secret - Red colored), and 705 (Confidential - Blue colored)]:

- warn you, the holder or custodian of the document, that you have a classified document in your immediate possession.
- hide the information when you are not using the document.

Before you give classified information to anyone, you (the holder of the information) must ensure that the person to whom you are giving the information has the proper level of clearance (TS for TS information, etc.) and has the "need-to-know" (the person must have access to the information to perform an official duty). If you are unsure, contact your local security manager.

How to Derivatively Classify Information

Derivative classification is the process of deciding that an item of information is classified and marking it with the level of classification.

Anyone who does derivative classification is responsible for ensuring that the proper classification level (and downgrading and declassification instructions) are assigned to the information.

When you derivatively classify information, you are identifying an original classification authority's previous decision pertaining to that information and you are carrying forward that decision in terms of the information's classification and its length of classification.

How do we know that information is classified?

The classification of the information may be identified in three ways.

1. Classified source documents. Through their markings, classified documents provide classification instructions about the information they contain. But, because we must keep marking requirements reasonable, the instructions are almost always less specific then those found in the following two types of guidance.
2. Security classification guides. Almost always, a well-prepared security classification guide (SCG) is the most accurate source of classification instructions.

Most DoD SCGs are listed in the DoD Index of Security Classification Guides, DoD 5200.1-I.

SCGs are available from the Defense Technical Information Center (DTIC) and from the preparing office.

3. Other classification guidance. Classification guidance is often found in directives, exercise plans, memoranda, etc. In the National Industrial Security Program, sources of guidance are placed on a DD Form 254, Contract Security Classification Specification.

Do not depend upon your memory or general impressions when derivatively classifying information.

How do I determine how long the information should remain classified when I'm doing derivative classification?

Our goal is to protect information at the appropriate level for as long as necessary, and to try our best to not protect it when it is no longer needed.

You will find that classified source documents carry only a single marking showing the duration of classification. SCGs and other guidance, however, will specify the duration for individual items of information.

When you are determining how long to keep the classification for your derivatively classified document:

- If a single declassification instruction (date, event, or EO 12958 exemption marking) applies to all the classified information in your document, use it.
- If your sources specify a combination of a date(s) and an event(s), mark your document for declassification on the latest date or event.
- If all of the information comes from documents marked “OADR,” use the latest of the document dates and mark your document with the declassification instructions as follows: “Declassify on: Source marked OADR; Date of Source: XX XXX XXXX” (where the Xs represent the latest document date).

- If the information comes from sources that have a variety of declassification instructions, apply the most restrictive declassification instruction. Generally, they will be in this order (from most restrictive to least restrictive): (1) “25X1,” (2) any of the “X1” through “X8” markings, (3) “Source marked OADR,” and (4) the latest date specified for any of your sources.

How do I communicate my derivative classification determinations?

Marking classified documents is our principal (and often our only) means of communicating derivative classification determinations.

How to Mark Your Documents

We mark classified materials in order to:

- alert the reader of the material that something in it is classified.
- indicate the highest level of classified information in the material.
- show the reason for classification (required for originally classified documents).
- show what portions of the material contain the classified information.
- show the source of classification.
- give information regarding the downgrading and declassification of the information.
- give any special warning or handling notification.

Portion marking

Each "section, part, paragraph or similar portion" must be marked to show the highest level of classification of the information in that particular portion. These markings are placed in parentheses and normally are located at the beginning of the portion itself.

One exception is that subject and title lines are marked after the portion.

Another exception is that illustrations, charts, and graphs are marked within or next to the illustration, chart, or graph.

Overall marking

There are two overall marking requirements: overall page marking and overall document marking.

Overall page marking:

This indicates the highest level of classification for the information contained in or revealed by the page. The level of classification is spelled out and is marked conspicuously at the top and bottom of each *interior page* of a document.

Overall document marking:

This indicates the highest level of classification for the information contained in or revealed within the document itself and is placed on the top and bottom of the front cover (if any), the title page (if any), the first page, and on the outside of the back cover (if any).

Applicable associated markings

Markings other than those that indicate the classification of the information are considered applicable associated markings. These markings are placed on the face of the document and include:

- the “classified by” line (for originally classified documents).
- the “derived from” line (for derivatively classified documents).
- the “classified why” line (shows the reason for classification of originally classified documents).
- the “declassify on” line.
- downgrading instructions, if any.
- warning notices and control markings, if any (portion and page markings are also required).
- the originating office and date.

How to Transmit Classified Materials

Secret

Secret materials can be transmitted by:

- an authorized component courier service.
- an authorized electronic system, e.g., a STU-III or STE.
- handcarrying (with proper authorization).
- Defense Courier Service (not routinely but under certain circumstances).
- Registered mail (within US and Puerto Rico – It can be sent to an APO/FPO address only if you can ensure that the mail will not pass out of US control during its trip).
- Protective Security Service for large bulky items (check with your security office).
- United States Postal Service Express Mail (check with your security office for limitations).
- Holder of GSA contract for overnight delivery (currently FedEx) (check with your security office for limitations).

Confidential

Confidential materials can be transmitted by:

- an authorized component courier service.
- an authorized electronic system, e.g., a STU-III or STE.
- handcarrying (with proper authorization).
- Defense Courier Service (not routinely but under certain circumstances).
- registered mail (for NATO outside US; for APO/FPO outside US; when uncertain if destination within US; to DoD contractor or other Executive Branch agency, when appropriate).
- First Class mail (between DoD activities within US and territories – do not use for mail to DoD contractors or other Executive Branch agency).
- certified mail (to DoD contractor or other Executive Branch agency).
- constant surveillance service for large bulky items (check with your security office).

Contact your local security office for guidance on transmission of top secret and for further information concerning transmission of classified materials**.**

Handcarrying

Handcarrying is the last choice for transmitting classified information. It should be used only after all other means have been found to be inadequate.

Prior to leaving:	While traveling:	Also, if traveling by a commercial aircraft:
● Obtain written authorization (1) Travel orders, (2) DD Form 2501, or (3) Letter of authorization (required for travel on commercial aircraft). ● Get briefing. ● Make arrangements for overnight storage (if applicable). ● Double wrap materials. ● Inventory the classified materials. One copy will be maintained by the courier's security office and one copy with the courier.	● Keep materials in your personal possession or under your constant surveillance. ● Do not read, study, display, or use the materials in public. ● Never leave materials unattended.	● Ensure that all airlines involved are U.S. carriers, or that no U.S. carrier is available before using a foreign carrier. ● Coordinate with the airlines. ● Have in your possession: (1) Military/government ID (2) Letter of authorization. ● Allow airline/airport officials to inspect outside of package. ● Don't bind material with metal straps or otherwise cause airline/airport officials to be suspicious or want to inspect inside the package.

Contact your local security office for information on the requirements for handcarrying.

How to package

Inner wrapping:

- opaque material
- classified text should have no direct contact with wrapping
- highest classification and warning notices
- wrapped to make detection of tampering easy
- address
- return address

Outer wrapping:

- opaque material
- wrapped to make detection of tampering easy
- no classification markings
- "Do Not Forward" on First Class mail for Confidential
- addressed to activity, not person (do not put a person's name in address)
- return address

How to Destroy Classified Materials

Normally, the people authorized to destroy classified materials are the user (or custodian) of the material and designated destruction officials for activities, if used. Check with your local security officials.

The material is considered to be destroyed when information cannot be reconstructed. Until that condition is reached, the material must be protected and the access rules of clearance and need-to-know remain in effect.

Burn bags, when utilized, must be protected until the contents are destroyed.

Authorized methods of destruction.

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

Contact your local security office for the location of destruction equipment which meets the standards for destruction and for information on other methods for destroying classified materials.

Procedures to Follow When Reproducing Classified

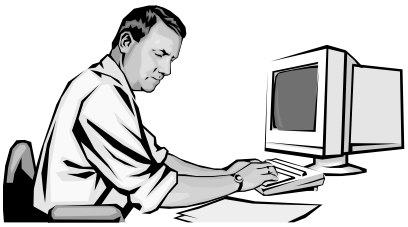
- Use only those machines for which classified reproduction has been authorized and so designated.
- Ensure that latent images will not cause compromise.
- Apply accountability rules and limitations which pertain to the originals to any reproduced copies.
- Always check the copier to make sure you haven't left the original or any copies in it.

Contact your local security office for more specifics.

Rules to Follow When Typing Classified

When using a typewriter:

- Place the appropriate classification marking on the ribbon cassette.
- Store the ribbon cassette in a proper security container after you are finished typing.
- Properly destroy the ribbon when it is no longer needed or usable.



When using a word processor/computer:

- Check with your local security office to ensure that you are authorized to use that particular equipment for processing classified.
- Follow your local security procedures.

Using the Phone/FAX for Classified

For verbal discussions:

- use a STU-III, STE, or some other authorized secure communication equipment.
- follow the encryption procedures for that equipment.
- while using the equipment, ensure that other people are not within hearing range of your voice.

For FAXs:

- use a secure FAX unit.
- follow the encryption procedures for that equipment.
- prior to 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.

Contact your local security office for further requirements.

Rules for Taking Classified Home to Work On

Before you take classified material home to work on it, you must meet the following criteria:

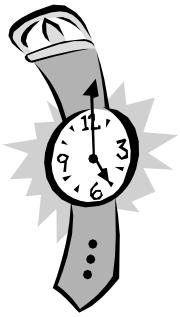
You must:

1. have an approved classified materials security container at your residence.
2. obtain (or get briefed on) the procedures for protecting the materials.
3. maintain a record of the materials taken home.
4. for Top Secret materials:

   obtain the approval of the SECDEF, SECAF, SECARMY, or SECNAV; or Commander of the Combatant Commands; or the Senior Agency Official of your Component.

   for Secret materials:

   obtain the approval of the Head of your Component or the designee (may be designated to Major Command level).



End Of The Day Security Check

1. Check the entire work area for classified materials. [Include trash cans, reproduction equipment, in/out boxes, desk tops, etc.]
2. Check container to ensure it is not open.
3. Record the check on SF 701 (Activity Security Checklist).

4. Perform the above steps if you work during the off-hours.