



## Reporting Unsecured and Securing Classified Material 4.G.03

**Learning Objective(s):** **LOCATE** your unit’s physical security plan and familiarize yourself with your unit’s protocol for responding to the discovery of unsecured classified material.

### **Why You Need to Know This**

Security is an “All Hands” responsibility and one that requires constant vigilance. As a member of the United States Coast Guard you are personally and individually responsible for providing proper protection of classified information under your custody and control. In addition, you are equally responsible to report and secure any unsecured classified material which you may come in contact with in the performance of your duties. No matter how minor, any security infraction must be reported immediately to your Command Security Officer (CSO) so that the incident may be evaluated and any appropriate action taken.

This lesson will provide you with the information you will need to know in regards to reporting unsecured and securing classified material.

---

### **Topics Covered**

This section will cover the following topics:

- Security Classification Levels
- Classified Material Identification
- Storing Classified Material
- Identifying Individuals Access to Classified Material
- Responding to the Discovery of Classified Material

At the end of this lesson there will be a Learning Activity. Members are encouraged to first look at this learning activity and the sign off requirements located in “**For You and Your Supervisor**” section in order to take proper notes.

---

**Security  
Classifications  
Levels**

Information which requires protection against unauthorized disclosure in the interest of national security shall be classified Top Secret, Secret or Confidential. No other terms shall be used to identify classified information. Classification levels are assigned to determine the level of protection and the damage unauthorized disclosure could cause. The three classification levels are:

- **Top Secret:** Information requiring the highest degree of protection. The unauthorized disclosure of top secret information could reasonably be expected to cause exceptionally grave damage to the national security.
  - **Secret:** Information requiring a substantial degree of protection. The unauthorized disclosure of secret information could reasonably be expected to cause serious damage to the national security.
  - **Confidential:** Information requiring protection. The unauthorized disclosure of confidential information could reasonably be expected to cause damage to national security.
- 

**Identifying  
Classified Material**

Items containing classified material will be marked with the highest classification level of any portion of the document. (i.e. part of the document is Secret, but the rest is Confidential, the entire document will be marked Secret.) Items are marked differently based on the type of item it is.

The following is a list of item types, and if they are classified, how they are marked:

- **Documents** – If the document is only one page than the classification will be marked on the bottom and top of the page. For documents containing more than one page, the classification marking will appear on the top and bottom of the outside cover, the title page, and the outside back cover. All other internal pages will be marked with the overall classification or with the marking indicating the highest classification level of the information contained on that page.
-

**Identifying  
Classified Material  
(Continued)**

- **Electronically Transmitted Material** – Electronically transmitted material shall be marked the same as other classified documents, with the following special provisions:
    - The classification line must indicate the highest level of classification.
    - For information printed by an automated system, overall and page markings may be applied by the system, provided they stand out conspicuously from the text. This may be achieved by surrounding the markings with asterisks or other symbols.
    - Properly completed “Classified by” and “Derived from” line must be included in the last line.
  - **Charts, Maps and Drawings** – This type of information shall bear the appropriate classification marking under the legend, title block or scale, in such a manner as to differentiate between the classification assigned to the document as a whole and any classification assigned to the legend title itself.
  - **Photographs** – Negatives and positives shall be marked with appropriate classification markings and kept in a case, folder, etc. bearing conspicuous classification markings. Rolls of negatives shall be marked at the beginning and end of each strip and single negatives marked with the appropriate classification. Applicable classification markings shall be shown clearly on the image of each transparency or slide and its border.
  - **Videotapes and Motion Picture Films** – This type of material shall be marked at the beginning and end of each reel or tape by titles bearing the appropriate classification markings. Such markings shall be projected on the screen. The outer case or cover for reels and tapes shall bear the same classification markings.
  - **Recordings** – Recordings (sound or electronic) shall contain a beginning and end statement of assigned classification. Recordings shall be kept in containers or on reels that bear conspicuous classification markings.
  - **Microfilm** – Classification markings shall be conspicuously marked on microfilm.
-

**Storing Classified Material**

The physical storage requirements for classified material are listed below:

- **Spaces** which contain classified material shall be designated as a **“Restricted Area”**.
  - **Security containers** used for the storage of classified material shall be inspected for tampering when any of the following occur:
    - A security container has been found open and unattended.
    - The combination is suspected of having been compromised.
    - A newly obtained security container has been received.
  - **Top Secret** information shall be stored in a GSA-approved security container with one of the following supplemental controls:
    - The location that houses the security container shall be subject to continuous protection by guard or duty personnel.
    - Guard or duty personnel shall inspect the security container once every two hours.
    - An Intrusion Detection System with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.
    - Security-In-Depth when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740.
  - **Secret** information shall be stored by one of the following methods:
    - In the same manner as prescribed for Top Secret information.
    - In a GSA-approved security container or vault without supplemental controls.
  - **Confidential** information shall be stored in the same manner as prescribed for Top Secret information except that supplemental controls are not required.
-

**Identifying  
Individuals with  
Access to  
Classified Material**

The unit-level positions responsible for the day-to-day management of security-related matters are listed below:

**Command Security Officer (CSO):** The CSO works under the direction of the Commanding Officer, who is ultimately responsible for all national security information at his/her unit. The CSO shall be a commissioned officer, chief warrant officer, senior petty officer (E-7 through E-9) or civilian employee (GS-9 or above). The CSO is the key person at a unit when it comes to security related matters. Among their many duties, the CSO is responsible for developing and maintaining the unit's physical security plan which includes keeping a list of individuals at the unit designated by the command as having the need-to-know and access to classified information or classified spaces.

**Classified Material Control Officers (CMCO):** The CMCO works under the direction of the CSO. Chief among the duties of the CFO is responsibility for maintaining accountability records for the security control point (SCP) and ensuring the proper operation of the classified material control system (CMC).

**Document Control Station Officer (DCSO):** The DCSO works under the direction of the CMCO and is responsible for receiving and transmitting through the security control point all classified material flowing in and out of the element which is being serviced.

---

**Responding to the  
Discovery of  
Classified Material**

If classified material is discovered unguarded, misplaced or not properly secured the following actions should be taken:

- **DO NOT** attempt to read or interpret the information.
- If near a phone, call the **Command Security Officer (CSO)** or **Officer of the Day (OOD)** and report the discovery **IMMEDIATELY**.
- If you are not near a phone, request assistance by asking someone to help you to call or contact the **CSO** or **OOD**.
- **DO NOT** leave the material unguarded while waiting for the proper authorities to arrive.
- If handy, **cover the material** with a folder or sheet of paper to shield it from view.

After the information is safely secured, the Command Security Officer will begin an investigation as to how and why the information was left unprotected. It will be important for the person who discovers the material to remember as much as they can about who was there, what was going on, and who may have been in the space or area, prior to the discovery of the material.

---

## Learning Activity



To successfully complete this requirement you will need to complete the following:

- Identify your unit's Command Security Officer (CSO) by name.
- Locate and read your unit's physical security plan.  
**Note:** Each unit should have a signed instruction guiding personnel on their responsibilities pertaining to the storage of classified information, and what to do in the event that classified or sensitive material is found unprotected.
- Complete the on-line Security Education Training Awareness (SETA) Mandated Training (MT) found on the Coast Guard Portal at the following link:  
<https://cgportal.uscg.mil/delivery/Satellite/trained>  
The course takes approximately 20 minutes to complete. When you are done, print out a record of your course completion and show it to your supervisor.

---

## For You and Your Supervisor

In order to meet the sign-off requirement for this lesson **YOU** must perform the following:

1. Prior to meeting with your supervisor review the contents of this lesson and organize your thoughts.
2. Identify your unit's CSO by name and locate your unit's physical security plan.
3. Discuss the plan and your unit's protocol for responding to the discovery of unsecure classified material.
4. Take the on-line SETA course. Upon completion of the course present a copy of your course completion record to your supervisor.

Before signing off on this requirement your **SUPERVISOR** must:

1. Make sure the member has reviewed the unit's security plan and understands the local protocol for responding to the discovery of unsecure classified material.
  2. Verify completion of the SETA MT course; noted by the course completion record.
  3. Provide the member with corrective feedback and answer any questions they may have related to this topic.
  4. Sign-off the check-off sheet on the Record of Enlisted Professional Military Education (E-PME) Performance Requirements.
-

**References**

The references used to develop this lesson can be found at CG Directives (CG-612), [www.uscg.mil/directives](http://www.uscg.mil/directives):

- Classified Information Management Program, COMDTINST M5510.23(series)
  - Physical Security and Force Protection Program, COMDTINST M5530.1(series)
  - Personnel Security and Suitability Program, COMDTINST M5520.12C(series)
  - <http://cgweb2.comdt.uscg.mil/CGDIRECTIVES/>
-