UNITED STATES MARINE CORPS
THE BASIC SCHOOL
MARINE CORPS TRAINING COMMAND
CAMP BARRETT, VIRGINIA 22134-5019

SECURITY OF CLASSIFIED MATERIALS
W130119XQ
STUDENT HANDOUT

Security of Classified Materials

Introduction

Maintaining the security of classified materials is vital to the mission of the Marine Corps. All Marines are responsible for protecting these documents.

Importance

As an officer, you are required to report any incident that you believe is a security violation, to educate your subordinates in the importance and procedures of handling classified materials, and to maintain your personal standards of conduct.

In This Lesson

This lesson gives you an understanding of how to safeguard classified materials and an awareness of those key billets within a battalion/squadron that are in charge of protecting such materials.

This lesson covers the following topics:

Learning Objectives

Terminal Learning Objectives

TBS-LDR-1014 Given an evaluation, define Operational Security (OPSEC), without omitting key components.

TBS-LDR01012 Given an evaluation, identify immediate actions for safeguarding suspected classified material, without omitting key components.

Enabling Learning Objectives

TBS-LDR-1012a Given an evaluation, identify the levels of classified materials security classification, in sequence, without omission.

Security of Classified Materials (Continued)

Learning Objectives (Continued)

Enabling Learning Objectives (Continued)

TBS-LDR-1012b Given a scenario, identify procedures for classified material spillage or compromise, without omission

TBS-LDR-1012c Given a scenario, identify the procedures for reporting persons suspected of espionage, without omission.

TBS-LDR-1012d Given an evaluation, identify the methods used by foreign agents to collect information, without omission.

TBS-LDR-1012e Given an evaluation, identify procedures for handling of "For Official Use Only" materials, without omission.

TBS-LDR-1014b Given Marines and personal information, identify ways to safeguard personally identifiable information (PII) in accordance with SECNAVINST 5211.5E.

TBS-LDR-1014c Given Marines and personal information, define personally identifiable information (PII), without error.

Basic Definitions

Operational Security (OPSEC)	The process to deny the enemy critical information about us.
Communications Security (COMSEC)	Measures and controls taken to deny unauthorized persons information derived from telecommunications systems and ensure authenticity of such communications.
Classified Information	Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so identified by the assignment of a security classification.
Classified Material	A document or any media upon which classified information is recorded or embodied.
Security	The establishment of a protected environment for classified information and materials.
Access	The ability and opportunity to obtain knowledge of classified information or possession of classified materials.
Need to Know	The necessity for access to knowledge or possession of classified information in order to carry out official military or government duties.
Clearance	An administrative determination by a designated authority that an individual is eligible for access to classified information of a specific classification designation or less.

Classification Designators

Top Secret	TOP SECRET is the designator applied to material whose unauthorized disclosure can be expected to cause exceptionally grave damage to national security.
Secret	SECRET is the designator applied to material whose unauthorized disclosure could be expected to cause serious damage to national security.
Confidential	CONFIDENTIAL is the designator applied to material whose unauthorized disclosure could be expected to cause identifiable damage to national security.
Unclassified	Material which does not fall into one of the three categories above are designated UNCLASSIFIED.

Classification Designators (continued)

For Official Use Only (FOUO)

FOUO, although NOT a classification designator, may be used instead of UNCLASSIFIED to designate unclassified portions containing information exempt from mandatory public release.

Classification Authority

Original Classification Authority

The Secretary of the Navy severely restricts the power to classify new material or information which is not derived from previously existing material or information.

Derivative Classification Authority

This power is inherent to all personnel who work with classified materials and information. Specifically, if you produce or extract classified material or information from other classified material, you are responsible for classifying the newly created material to the appropriate level. This authority must be exercised daily to ensure security.

Personal Security Clearances

Final Clearance

Final clearance is granted on completion of all investigative requirements:

- Top secret: Based on a single scope background investigation.
- Secret: Based on a favorable national agency check.
- Confidential: Based on a favorable national agency check.

The Department of the Navy Central Adjudication Facility is the issuing authority. Commanding officer's assent is required.

Interim Clearance

Interim clearance is granted for six months until the requested investigations are complete. The individual's commanding officer bears the responsibility.

In addition to the proper clearance, an individual must have a need to know in order to be granted access to classified material or information.

Billet and Individual Responsibilities

Commanding Officer (CO)

The CO:

- Is directly responsible and, therefore, accountable for all matters pertaining to the security of classified materials and information held or used by the command.
- Must ensure that physical security is adequate and maintained.
- Must ensure that all subordinates who routinely handle classified materials receive formal, specialized instruction and that the entire command receives an annual security brief.
- Must establish and review the inspection procedures for the unit's Classified Material Control Custodian (CMCC).
- Must continually evaluate personnel with regard to their eligibility for access, to include clearances and a need to know.

Security Manager

The CO assigns the unit security manager, usually the battalion executive officer (XO). The security manager:

- Investigates all security violations and suspected compromises of classified information and material.
- Develops the unit standard operating procedures (SOP) and emergency plans.
- Supervises accounting and control procedures.
- Supervises the S-2 to ensure that personnel have appropriate clearances for the level of material with which they work.
- Is responsible for outside visitors to the command.

Custodians

The two different custodians in the infantry battalion are the classified material control custodian (CMCC) and the electronic keying material systems manager. Custodians:

- Store classified material in containers appropriate for the classification level of material being stored.
- Receive, distribute, and account for classified material.
- Destroy unneeded, unused, and superseded material

Billet and Individual Responsibilities (Continued)

Classified Material Control Custodian (CMCC)	Normally, the CMCC is the S-1/Adjutant and handles classified materials such as operation orders, message traffic, publications, manuals, etc. Generally the CMCC controls/handles classified material that is *not* communication-oriented.
Electronic Keying Material Systems Manager	The battalion CO assigns the electronic keying material systems manager, usually a Staff Non Commissioned Officer of any MOS. Generally, the electronic keying material systems manager handles classified material associated with communications such as key tapes, operation codes, AKAC-874s, automated communication electronics operating instructions (ACEOIs), etc.
Unit Intelligence Officer (S-2)	The S-2 is usually assigned as the assistant security manager and: • Initiates and monitors the progress of security investigations. • Informs the CO of all changes to individual security clearances. The S-2 is the staff section where individuals report to obtain or upgrade a security clearance.
Individual Marines	All Marines: • Report all security violations or suspected compromises, including espionage attempts, to the security manager *immediately.* • Use classified material in a controlled environment that limits the number of people who have access to it. • Cover or close material if uncleared personnel approach. • Never leave classified material unsecured. • Never take classified material home. • Memorize safe combinations; written records of combinations are only maintained in the CMCC and may not be held by any individual. • Store nothing valuable with classified material. • Do not discuss classified material with anyone other than cleared personnel with need to know. • Destroy material exactly when told using the prescribed method.

Billet and Individual Responsibilities (Continued)

Individual Marines (continued)	• Treat derivative classified material with the same respect as original material. • Are familiar with the emergency destruction plan. • Report all contacts with foreign nationals from hostile countries.

Personal Conduct Standards

Security clearances are issued to trustworthy and competent personnel who are required to work with classified information and material. Clearances may be denied or revoked and access suspended if an individual violates the established standards. Standards are established for the following areas:

- Loyalty.
- Foreign preference.
- Security responsibility safeguards.
- Criminal conduct.
- Mental or emotional disorders.
- Foreign connections.
- Financial affairs.
- Alcohol abuse.
- Drug abuse.
- Integrity.

Personally Identifiable Information

Personal Information (PI) Defined	Information about an individual that identifies, relates, or is unique to, or describes him or her (e.g., SSN, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.).
Personally Identifiable Information (PII) Defined	Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records. PII falls under the sub-classification For Official Use Only (FOUO).

Personally Identifiable Information (Continued)

Department of Navy Policy Regarding PI/PII

DON activities/employees/contractors are responsible for safeguarding the rights of others by:

- Ensuring that PI/PII contained in a system of records, to which they have access or are using to conduct official business, is protected so that the security and confidentiality of the information is preserved.
- Not disclosing any information contained in a system of records by any means of communication to any person or agency, except as authorized by this instruction or the specific PA systems of records notice.
- Not maintaining unpublished official files.
- Safeguarding the privacy of individuals and confidentiality of PI/PII contained in a system of records.
- Properly marking all documents containing PI/PII data (e.g., letters, emails, message traffic, etc) as “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE – Any misuse or unauthorized disclosure can result in both civil and criminal penalties.”
- Not maintaining privacy sensitive information in public folders.
- Reporting any unauthorized disclosure of PI/PII from a system of records to the applicable Privacy POC for his/her activity.
- DON activities shall not maintain records describing how an individual exercises his/her rights guaranteed by the First Amendment (freedom of religion; freedom of political beliefs; freedom of speech; freedom of the press; the right to peaceful assemblage; and petition for redress of grievances), unless they are: expressly authorized by statute; authorized by the individual; within the scope of an authorized law enforcement activity; or are used for the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains.

Espionage

Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. It is based off the Espionage Act, also known as the Sedition Act, which was passed in 1917 during WWI. This law made it illegal for any person to convey information in an effort to promote the success of the nation's enemies. It deemed a criminal anyone who, "when the United States is at war, shall willfully make or convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, shall willfully cause or attempt to cause insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States, or shall willfully obstruct the recruiting or enlistment service of the United States, to the injury of the service or of the United States."

Some common methods used by spies to try to acquire information are:

- Exploiting or stealing classified equipment and technology
- Illegally transferring U.S. technology from third countries
- Covert espionage.
- Recruitment of Americans to a foreign cause or the exploitation of human intelligence.
- Cyber attacks.

If you suspect someone of espionage, report the incident or person immediately to your chain of command, security manager, S-2 Intelligence Officer, or Naval Criminal Investigative Services (NCIS).

Summary

This lesson has covered the basic terms and definitions associated with the security of classified materials and the responsibilities of individual Marines with regard to safeguarding classified materials. Further guidance can be found in the references listed herein.

References

Reference Number or Author	Reference Title
CMS 4	Communication Security Material (CMS) Manual
CSP 1	Cryptographic Security Policy and Procedures
MCWP 2-6	Counterintelligence
OPNAVINST 5510.1	Department of the Navy Information and Personnel Security Program Regulation
SECNAVINST 5239.3B	Department of the Navy (DON) Information Assurance Program

Glossary of Terms and Acronyms

Term or Acronym	Definition or Identification
Access	The ability and opportunity to obtain knowledge of classified information or possession of classified material
ACEOI	Automated communication electronics operating instruction
Classified Information	Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so identified by the assignment of a security classification
Classified Material	A document or any media upon which classified information is recorded or embodied
Clearance	An administrative determination by a designated authority that an individual is eligible for access to classified information of a specific classification designation or less
CMCC	Classified material control custodian
CMS	Communication security material
CO	Commanding officer
COMSEC	Communication security
FOUO	For official use only
Need to Know	The necessity for access to knowledge or possession of classified information in order to carry out official military or government duties
Security	The establishment of a protected environment for classified information and material
SOP	Standard operating procedure
XO	Executive officer

Notes