

# **SECURITY ORIENTATION BRIEF**

1. A decision has been made to grant you access to classified information. Access to classified information is granted on the “need to know” basis. It has been determined that you will need to handle classified information in order to complete your assigned duties. Within this brief we will discuss some of the important procedures you must follow whenever you come into contact with classified information.
2. First of all, the rules and procedures for handling, storing and disseminating classified information are established by the Department of the Navy. These rules are found in the Information Security Program. The Information Security Program for Department of the Navy personnel (including the Marine Corps and civilians) are contained in SECNAV 5510.30C. This directive contains all the rules for maintaining proper security and handling of classified information.
3. Before granting you access to classified information, it must be determined that you are trustworthy and reliable. This determination is made after all available information about you is gathered. A personnel security investigation is conducted by the Officer of Personnel Management. The type of investigation conducted (T3, T5, ANACI, NACLC, PRS, SSBI, SBPR, etc.) depends upon what level of access you will be expected to receive. Basically, the higher the level of access, the more thorough the investigation becomes. In addition, locally available command records (PMO, CID, SRB, etc.) are screened. With this information, a determination can be made to grant you a security clearance.
4. Now that you have access to classified information, what are your responsibilities?
  - a. You are responsible for maintaining proper security for all classified information with which you come into contact with. This includes closely following established security measures when you have classified information in your possession. You will also be expected to exercise personal censorship. Personal censorship means that you must always be on your guard to protect the information which you have knowledge of against unauthorized disclosure.
  - b. You are responsible for ensuring that any classified information with which you are charged is only given to personnel who have been authorized access. In addition, you must be satisfied that the individual has a valid “need to know” that contents of the requested classified information.
  - c. You are expected to ensure that all classified information is returned to the proper storage area when you secure for the day. In addition, a double check of your work space will be conducted by at least two people to ensure that all classified material has been returned to its proper storage container.
5. Some of the general rules concerning the handling of classified information are as follows:
  - a. Never leave classified information adrift.
  - b. Never discuss classified information in an unsecured area.
  - c. Never remove classified information from this Command without proper approval.
  - d. Never reproduce classified information without approval.
  - e. Never allow a person access to classified information until you confirm the individual’s clearance, access, and “need to know.”

- f. Never discuss classified information over the telephone.
  - g. Never carry the combination to security containers or storage rooms in your wallet, or keep them in unsecured places.
  - h. Never fail to report a suspected security violation.
6. Occasionally, when someone makes a mistake, a situation may arise in which classified information is subject to compromise. Your first action should be to protect or recover the classified information from further compromise. Secondly, report the incident and all circumstances surrounding the compromise or possible compromise to appropriate security personnel.
7. If you are approached by someone and asked to disclose sensitive or classified information, be certain to report the incident immediately. Do not try to handle the situation yourself, but do try to remember the description of the individual(s) involved.
8. The security clearance and access you have been granted is a privilege, not a right. You can lose your clearance and access through for example: violation(s) of the UCMJ to include Drug or Alcohol abuse or adverse involvement with law enforcement agencies. To gain an overall understanding of what can cause an individual to lose clearance you can review SECNAV 5510.30C, Encl (12).
9. In accordance with SECNAV 5510.30C, Encl (12), I understand that I am responsible to self-report any violations of the standards of conduct required of persons with access to classified information and/or assignment to sensitive duties.
10. This orientation brief is intended to mention some of the procedures concerning the handling and protecting of classified information. Remember, safeguarding classified information is every Marine and civilian's responsibility, and the best weapon to use in safeguarding our classified information is to become familiar with the Information Security Program.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Printed Name)

---