SECURITY AND OPSEC BRIEFING

The purpose of this briefing is to familiarize you with the level of access, handling, and stowage of classified and sensitive material and information and to provide guidance and direction concerning Operational Security (OPSEC). Your assignment to the Naval Safety Center carries with it grave responsibilities for safeguarding classified and sensitive information to which you may be granted access during your assignment. You are also responsible for helping maintain the security of this command by complying with various security regulations, all of which have been issued for the purpose of providing necessary protection against classified information falling into the hands of unauthorized personnel and of preventing sabotage. The importance of the security of this command cannot be overemphasized.

The following information is given to you in order that you may better understand your duties in the area of security. The determination that information requires protection is called CLASSIFICATION. There are three levels of classification in order of the highest security level to the lowest are: Top Secret, Secret, and Confidential. Each classification requires specific protective measures, and the loss of any classified material will result in damage to national security.

Classified information may only be given to persons who have been authorized access to it. Just as classified material is assigned levels of classification, there are different levels of personnel security clearances. Individuals are cleared for access to the level of information required in their jobs. For example, a person whose job requires access to some Secret material will be given a Secret clearance and may have access to Secret and Confidential information, but not Top Secret. However, just because you hold a Secret clearance does not mean you may have access to all Secret information. You must also have a NEED TO KNOW; that is, in addition to having the proper clearance, your official duties must require that you have the information.

Safeguarding requirements permit classified information to be used or stored only where and when it can be properly protected. YOU MAY NOT:

1. Leave classified information unprotected - it must either be properly stored or in the custody of a cleared person.
2. Read or discuss classified information in an unsecured area - classified information may only be used where uncleared persons or persons without a need to know will neither see nor hear it. This includes ship movement/operations and capabilities.
3. Remove classified information from the command - except in approved situations and with specific permission of the Commanding Officer or Command Security Manager.
4. Reproduce classified information - except as approved by the command Security Manager.
5. Give classified information to a visitor without first verifying the visitor's identification, clearance, and need to know.
6. Discuss classified or sensitive information over the telephone or by email.
7. Send classified information out of the command by other than approved methods.
8. Dispose of classified information by other than approved methods or without required records.
9. Bring Portable Electric Devices (PED) that contain wireless communications capability, audio, video, photographic recording and/or transmission capabilities in areas where classified information is processed or stored except when authorized/ approved by Senior Cognizant Security Authority (DAA), based on a risk assessment and appropriate security countermeasures. This includes pagers, mobile/cellular telephones, personal digital assistants/job, performance aids, `laptop/ notebook' computers, digital imagery (still/video) devices and devices of similar capability, functionality or design.
10. **AT NO TIME SHOULD CLASSIFIED MATERIAL BE ELECTRONICALLY TRANSFERRED FROM A SIPRNET LOCATION TO A NIPRNET SITE.**

This list is only intended to alert you to some problem areas and not to give you specific information on how to handle each case. That guidance is contained in the DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM REGULATION (SECNAVINST 5510.36A) and COMNAVSAFECENINST 5510.2L. They should be consulted in any case of doubt on how to safeguard classified information properly.

Sometimes, when rules are not followed or somebody makes a mistake, a situation will occur in which classified information may be compromised. Any person discovering unprotected classified information or an unauthorized disclosure of classified information has TWO immediate responsibilities; FIRST, to attempt to protect the classified information from further compromise or risk of compromise and, SECOND, to report the circumstances to a responsible official. If you cannot protect both the classified information and report the occurrence, have someone else make the report while you continue to protect the information. If you are ever the cause of the compromise, or are approached by someone and asked to make an unauthorized disclosure of classified information, don't try to handle the situation yourself. Report it immediately to your Security Manager or Supervisor.

Operations Security (OPSEC). OPSEC is primarily (but not exclusively) focused on unclassified information or activity which may compromise critical information. The goal of OPSEC is to identify and protect. Operations Security is not a one time thing - it's a continuing process. It's an attitude of vigilance and caution ("street smarts"), based on understanding the value of certain unclassified information to some who is not part of your organization. As discussed above, discussion of classified or sensitive information over non-secure communications is strictly prohibited. You must also be vigilant of any sensitive information such as (not all inclusive): staff budget, travel itinerary (especially the Admiral's), schedules of visiting dignitaries, phone lists, and orders. On a daily basis, we discuss ship/squadron schedules - it's the nature of our business. Always exercise caution - don't set yourself or the command up - you never know who's out there watching and listening.

Official government telecommunications systems and facilities, including official DOD computers, telephones, computer systems, and telephone systems, are subject to comsec monitoring at all times. Systems include, but are not limited to all tactical radios, cellular telephones, INMARSAT, commercial satellite, and any fixed system conveying voice, video, fax, or data.

The enemy only used unclassified information on 9-11 - never forget it - stay focused on security.

_____
FULL NAME (TYPE OR PRINT LEGIBLY)

_____
DATE/SIGNATURE