

What information are you revealing?



Practice
OPSEC



If the information does not belong to you,
then keep a tight lid on it.

That False Sense of "I'm Rich" Feeling

Do you have that I'm rich feeling because you own a smart phone? Keep in mind that feeling is temporary, especially if your Smartphone is revealing more than you are aware of.

Be Smart: Know When and Where to Use your Smart phone. Be aware of where you can use your cell phone while at work. If unsure, it does not hurt to ask your supervisor or your local security office if cell phones are permitted in the area you are in.

**QUESTIONS? CONCERNS? SUGGESTIONS?
POINT OF CONTACT: OPERATION SECURITY /
CRIME PREVENTION
760.939.5025**



Crime Prevention

When you utilize OPSEC every day, you are also preventing crime:

- Report suspicious activities
- Conduct End-of-the-Day Security Checks
- Do not forget to take your CAC
- What you see here (at work) stays here (at work)
- Secure your rooms and buildings just like you would your house or vehicle

COMPUTER CRIMES Why attack a computer?

- Financial fraud or gain
- theft of resources
- gaining a competitive edge
- vandalism
- illicit eavesdropping
- maliciousness

These are some of the reasons computers are attacked. Information is power! Do your part by safeguarding your desktop or laptop computer information. Crime prevention is everyone's responsibility. After all, it is one of your security responsibilities.

WHY WE NEED CLEARANCES AND FAVORABLE DETERMINATIONS

The basic personnel security policy states no individual will be given access to classified information or assignment to sensitive duties unless a FAVORABLE personnel security determination has been made regarding their loyalty, reliability, and trustworthiness.

THE NATIONAL SECURITY STANDARD

The national security standard which must be met for personnel security clearance eligibility and eligibility for assignment to sensitive national security positions which is based on all available information to an individual's loyalty, reliability, and trustworthiness are such that entrusting them with access to classified information or assignment to sensitive position is clearly consistent with the interest of national security.

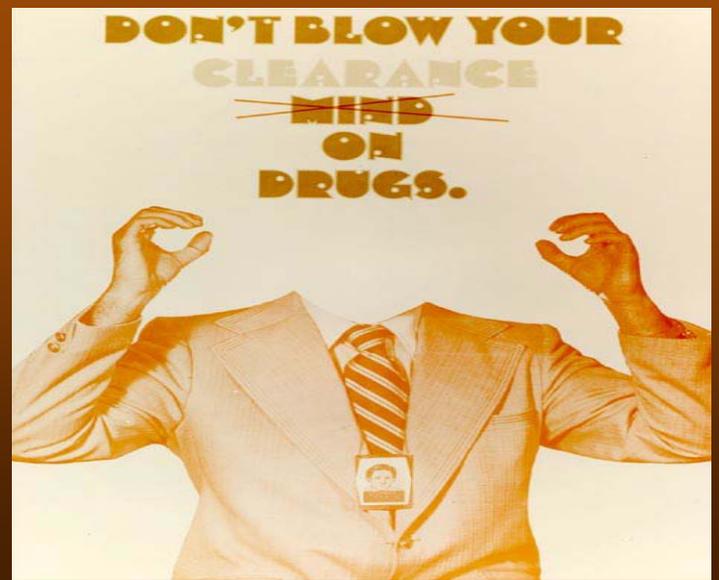
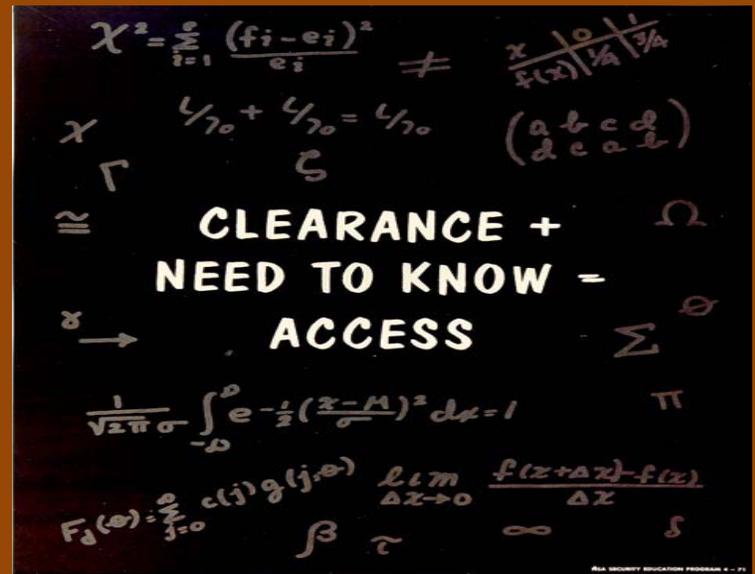
THE CONTINUOUS EVALUATION PROGRAM

The security clearance process is a tool which helps make sure that national security information is not given to people who cannot be trusted. Not all people are equally trustworthy and people change over time therefore, the continuous evaluation program (CEP) ensures any changes or unfavorable information are reported to the adjudication facility. So even though your personnel security investigation (PSI) is completed, your continuing need for access to classified information and assignment to a sensitive position is assessed.

QUESTIONS? POINT OF CONTACT:

760.939.1028

EMAIL: [GRILL US](#)



Security clearance & Sensitive Duty Assignment

A favorable sensitive duty assignment eligibility determination by DON CAF does not mandate the employing command to make such assignment. Rather it establishes that an employee has been determined to be eligible for such assignment based on national security standards, depending on the operational needs and the suitability requirements of the employing activity.

Eligibility determinations are made using the appendix G. personnel security eligibility standard to both sensitive national security position determination and security clearance eligibility determinations. These determinations cannot be made exclusive of each other. A determination that an individual is not eligible for assignment to a sensitive national security position will also result in the removal of eligibility for security clearance.

In wars past, you could tell the enemy by the UNIFORMS they wore...



It won't be that simple with the Information Warriors of tomorrow!

To some it may be too late but to the rest of us, it is never too late to start or to continue protecting and safeguarding our nation's secrets.

As we are entrusted with sensitive government information or national security information, we shall hold close the foundation of our freedom.

So you ask yourself, "What information?" and your security office says, "Very good answer. That's what I'm talking about. Keep up the good work." As you are walking away, you are still puzzled as in what information you cannot release or talk about.

Each employee is entrusted to safeguard the information, material, or area they work with daily. Remember that information, material, or area belongs to the government.

IN THE INTEREST OF OUR NATIONAL SECURITY

ACCESS TO CLASSIFIED INFORMATION

The basic policy for access to classified information states under the U.S. Navy regulations; the commanding officer's responsibility for his command is absolute. COs have ultimate responsibility and authority for all determinations regarding persons who may have access to classified information under their control. No one has the right to have access to classified information solely because of rank, position, or security clearance eligibility as per SECNAV M-5510.30 chapter 9.

QUESTIONS? POINT OF CONTACT:

760.939.1028

EMAIL: [GRILL US](#)

NEED-TO-KNOW POLICY

Access is only permitted to eligible individuals after determining that the individual has a NEED TO KNOW.

Access to classified information is not authorized by the favorable conclusions of the clearance eligibility determination.

Need to know is a preventive measure to identify and deter unauthorized access. Knowledge, possession of, or access to classified information is not provided to any individual solely by virtue of the individual's office, rank, or position.

Although access can only be authorized for individuals with established security clearance eligibility at or above the level of classified information required, having security clearance eligibility **does not** equate to need-to-know.



Information Assurance

February/March 2012 VOL # 16

COMMON ACCESS CARDS ARE GOVERNMENT PROPERTY. DO NOT MISUSE OR ABUSE THE CARD. IF LOST, STOLEN, OR MUTILATED, CONTACT FORCE PROTECTION OR CUSTOMER SERVICE DETACHMENT.

As DOD employee, you have the ultimate responsibility to safeguard your Common Access Card at all times while at work as well as off work. Keep in mind the amount of personally identifiable information the card has. If the card is misplaced or lost, contact your supervisor or security office as soon as you find out it is no longer in your possession. As you know, the Common Access Card is the key to entering areas and IT systems; so immediately contact security. A key lost is a treasure for someone who may misuse or abuse the card by obtaining unauthorized access to restricted areas. That unauthorized entry is logged as YOU having access and the trail of mishaps begin with your name. The card used by someone other than the holder is equal to identity theft. And by the way, after reapplying for a new card, you will never want to lose sight of the card again. The application procedures have changed tremendously. Contact your security office, Information Assurance office, or the customer service detachment (CSD) for more information on replacing your card, when lost, stolen, or mutilated and have some professional courtesy for those that are assisting you.



**NAVAL AIR WEAPONS STATION CHINA LAKE
INFORMATION ASSURANCE POINT OF CONTACT:
(760) 939-1233 E-MAIL: GRILL.US**



SECURE COMMUNICATIONS STARTS WITH YOU

- Secure communication is not just about communicating classified information by encryption. It is about communication of all kinds;
- The minute you open the internet browser or e-mail attachment, the secure communication starts.
- While off base, ensure work related programs or developments are not freely communicated. Be aware of who might be listening.
- The use of cell phones in restricted areas and communicating over the cell phone.

Computer security is everyone's responsibility. Computer information will only be protected when all employees do their part to protect information on their desktop, laptop computers, and information on the network.