ACCORDING TO THE NISPOM, REFRESHER TRAINING SHALL REINFORCE THE INFORMATION PROVIDED DURING THE INITIAL SECURITY BRIEFING AND SHALL KEEP EMPLOYEES INFORMED OF APPROPRIATE CHANGES IN SECURITY REGULATIONS. THE FOLLOWING ADDITIONAL TOPICS ARE PROVIDED FOR INCLUSION AS APPROPRIATE*

REPORTING REQUIREMENTS

Because of your job, you have been granted access to classified information that is vital to national security. You are charged with safeguarding that information. It is both an honor and a privilege that allows you to make a very special contribution to your country. However, it carries certain obligations that you must meet in order to maintain your access.

One of your obligations is to report to your security office those behaviors, incidents, or events that might in some way impact national security and your ability (or that of your co-worker) to function positively and effectively in a national security environment.

Based on the guidelines set forth in the National Industrial Security Procedures Operating Manual (NISPOM) you should report the following to your security officer:

FOREIGN TRAVEL

Report all foreign trips in advance in which a pre-travel defensive security briefing is requested/required or if travel is to a HOT SPOT country. If you're unsure is the country is a HOT SPOT then please contact your Security Officer.

- Business or personal travel (vacation, family emergency, etc)
- Report your trip in advance as necessary
- Follow up with your security office upon your return

FOREIGN CONTACT

A foreign national with whom one has continuing contact may be a stranger, business/work associate, or someone quite close to you such as a boyfriend, girlfriend, relative's spouse, or family friend.

- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard as suspicious
- Close and continuing contact with a foreign national in any capacity: in person, by telephone, via internet, etc.
- Contact with anyone who works for, or is associated with, a foreign government (including a foreign embassy) or a foreign-owned organization or business
- Financial obligations to, investments in, or employment with foreign nationals and companies

PERSONAL LIFE CHANGES

- Change of name
- Change in marital status (including legal separation)
- Change in cohabitation (involving a non-US citizen)

PSYCHOLOGICAL COUNSELING

- Consultation with a mental health professional (marital, family, grief counseling, and counseling need not be reported)
- Prescribed drugs as a result of psychological counseling

FINANCIAL CONCERNS

- Excessive indebtedness
- Liens
- Collections
- Bankruptcies
- Garnishments
- Judgments
- Unexplained financial affluence of an accessed individual

COMPUTER/INFORMATION SYSTEM MISUSE
- Unauthorized entry into an automated information system, whether government or contractor, for any reason
- Modification, destruction or manipulation of hardware or software on any government or contractor equipment

PASSWORD MISUSE
- Obtaining/using someone else's password
- Sharing a password
- Using a password to browse through another's account without permission
- Copying/Deleting information on another's account without permission

IMPROPER SECURITY PRACTICES
- Inadvertent or deliberate removal of classified information/materials to an unauthorized area
- Inadvertent or deliberate unauthorized destruction of classified information/materials
- Knowledge of a security violation or infraction & not reporting it
- Inoperability of locks, doors, vaults, etc., that are in place to security classified information and/or materials
- Deliberate or inadvertent disclosure of classified information/materials to an unauthorized person
- Loss of classified information/materials
- Requests for classified or sensitive information/materials through unauthorized channels

ALCOHOL-RELATED ISSUES
- Arrests
- Treatment
- Counseling

DRUG USE
- Illegal/improper use of narcotics, non-medicinal drugs, non-prescription drugs, or controlled substances
- Previously unreported drug use
- Use of prescription drugs prescribed for someone else (friend, spouse, boyfriend, girlfriend, child, parent)

CRIMINAL CONDUCT
- All arrests (regardless of whether or not there is a conviction)
- Knowledge of a criminal act by another accessed individual
- Knowledge of a criminal act by a member of your immediate family or close relative

SUSPICIOUS INCIDENTS
- Personal Security
- Facility Security

You may make your report to your security office via electronic mail, facsimile, telephone, or in person. Telephonic or in-person reporting must be followed by a written report. All information about the incident(s) or event(s) should be reported as soon as possible.

Clearly, we are unable to list all possible eventualities for each general heading. If you are in doubt as to whether a behavior, incident, or event should be called to the attention of your security office, REPORT IT! Your security office is in the best position to make a determination of the risks and to help mitigate or resolve them.

WHEN IN DOUBT , REPORT!

DEFENSE HOTLINE

The Defense Hotline is an important avenue for reporting fraud, waste, abuse, and mismanagement. To date, the Defense Hotline received more than 228,000 calls and letters. Because of Defense Hotline investigations the government saved or recovered $425 million. More importantly, many of the cases resulted in safer products and equipment for our military personnel and Defense Department employees.

Anyone, whether a service member, civilian employee, defense contractor, or private citizen, who witnesses what he or she believes to be a violation of ethical standards and/or the law, including but not limited to fraud, waste, or abuse of authority, potential leaks of classified information, or potential acts of terrorism, should report such conduct through his or her chain of command, respective service Inspector General, or directly to his or her respective service Inspector General or directly to the Inspector General of the Department of Defense Hotline at 800-424-9098.

The below listed violations should be reported to the Defense Hotline.

- Threats to Homeland Security
- Unauthorized Disclosures (Leaks)
- Human Trafficking
- Contract and procurement irregularities:
    - o Cost/labor mischarging
    - o Defective pricing
    - o Defective parts
    - o Bid rigging
    - o Product substitution
    - o Spare parts overpricing
- Bribery and acceptance of gratuities
- Significant cases of mismanagement
- Conflicts of interest
- Travel (TDY/TAD) fraud
- Abuse of authority
- Theft and abuse of Government property
- Military Reprisal (Violations of the Whistleblower Protection Act involving service members)
- Violations of the Whistleblower Protection Act involving Defense contractor employees and non-appropriated fund employees
- Improper referrals of military personnel for mental health evaluations
- Gross waste of funds

COPY MACHINES

Copy machines, whether you're using them for classified or unclassified data they are still a security risk. Many copy machines contain a hard drive which captures an image of the document being copied whether you used the machine to make a copy, send a fax, or scan a document. The below web address is a true 'eye opener'. It'll give you something to think about regardless of whether your machine is owned or leased. You don't want a plethora of information stored on a copier hard drive that an un-cleared copy machine repairman (or a savvy crook) can gain access to.

http://www.youtube.com/watch?v=iC38D5am7go

Keep an eye on repairman to ensure they're not downloading information from the hard drive. Check into software that can erase the data and do so on a regular basis, but definitely ensure it is erased before turning the machine in for repair or trade.

UNAUTHORIZED PUBLIC RELEASE INFORMATION

You are reminded that publication of classified information in the media does not render it unclassified. News articles reported that the web site Wikileaks published thousands of stolen documents, many of them classified. You should not go to this site, or similar sites, via your company or personal computer. Viewing classified information via the web will introduce classified information to the web cache on your computer and will constitute an unauthorized disclosure of classified information (AKA: Spillage) resulting in expensive cleanup procedures. As a cleared individual you can be held liable if classified material is found in your possession without the proper authorization or safeguarding.

Please remember that classified information appearing in public media does not mean that it is automatically declassified. Per NISPOM directives, Contractors shall continue the classification until formally advised to the contrary.

You have a responsibility to safeguard classified material. Improperly viewing classified documents is a violation of this safeguarding practice. Additional questions regarding the propriety of any classified documents should be brought to the immediate attention of the company security officer.

NEED TO KNOW – A FREQUENT DILEMNA

In the conduct of your daily duties, you may run into situations that make you question whether an individual has a need-to-know certain information you have in your possession. For example, you may be involved in a very sensitive special project or operation.

An individual from the office next door inquires about the project. You know that all personnel in the building have a SECRET clearance. Do you grant him access immediately; quickly decide that he does not have a need-to-know, and tell him so; or tell him that you will get back to him when you have more information?

You should ask him the reasons for his request for access. If he is unable to convince you of his need for the information, you should deny the individual access until you determine his need-to-know or seek guidance from your supervisor or Security Officer. Determination of need-to-know is the personal responsibility of everyone, but if there is any doubt in your mind as to an individual's need-to-know, always as your supervisor or Security officer before granting access to any classified or sensitive information.

COMPUTERS

The need-to-know principle also applies to computers and disks used on the job.

- Any passwords that you use to access work automated systems are yours exclusively and should never be shared with co-workers.
- Always secure your computer when leaving an area for an extended period of time by logging off and securing media such as disks, tapes, and cartridges.
- Ensure media is assigned classification at the highest level of information ever processed on the system on which it is used.
- These media must be protected at that level.
- Always take time to affix classification and data description labels and secure the media when finished.
- When you exchange media with another person, be sure that the media contains only that information which he or she has a need-to-know.

SPEAKING WITH CARE

Another area where you may overlook the need-to-know principle is the RUMINT (rumor intelligence), pillow talk, or gossip. You like to talk about your work, especially within the government contracting realm where you know everyone is cleared. However, there are areas where persons from various offices congregate and innocent "chit-chat" can reveal sensitive information. Even though you know that a person is cleared, either because he has a badge or from personal recognition, he or she may not need-to-know everything you might feel like discussing. In short, in every meeting place, look around, be sure that everyone has the required need-to-know, and then speak.

The same applies to sensitive but unclassified information. Remember that even unclassified information may require prior approval for release. Ensure you follow company or government guidelines if you are unsure whether or not to release information.

TELEPHONES

You will probably use standard telephones, STU IIIs, and secure or unsecure fax machines. Standard security procedures dictate the types of information that you can discuss or transmit on each instrument. However, when someone calls to discuss classified or sensitive information or ask for a fax, you must also ensure that the individual has a need-to-know for that information before providing it.

Follow the same routine as if you were speaking face-to-face with this person. Do not try talking around classified or sensitive information.

YOUR RESPONSIBILITY

You share the requirement to protect classified information along with every other cleared individual. Your personal responsibilities include using all the security tools available to you, such as secure phones, faxes, safes, badges and the like and learning the security skills you need to succeed in a high security environment.

One of these skills is the ability to ask a person for sufficient information to enable you to make an informed decision regarding their need to know. Use both the tools and the skills. Remember, not every cleared person who casually ask you about your job is a spy but continued questioning concerning classified or sensitive information where obvious need-to-know does not exist may be indicative of a security concern.

If you notice this type of behavior, discuss it with your supervisor or Security officer. Remember, the need-to-know principle was developed as a personal security measure to prevent unauthorized disclosure of classified and sensitive information.

Questions? As always your FSO is available to assist you with any questions or concerns that you may have. Additional guidance from the Defense Security Service (DSS) can also be found on-line at www.dss.mil.