**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 Program 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

- 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. Report the following to your FSO:

- 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)

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 CONTACTS

* efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
* contacts by cleared employees with known or suspected intelligence officers from any country,
* or any contact which suggests a cleared employee may be the target of an
attempted exploitation by the intelligence services of another country.

You may make your report to your security office via electronic mail, 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!**

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](http://www.dss.mil).

