ANNUAL REFRESHER BRIEFING AT-A-GLANCE

CLASSIFICATION LEVELS

Three classification levels determined by the level of damage possible to our national security through unauthorized disclosure:

Confidential – identifiable damage

Secret – serious damage

Top Secret – exceptionally grave damage

ACCESS REQUIREMENTS & NEED TO KNOW

Authorized access to classified information may be granted only when two conditions are met – the recipient has a valid security clearance at a level at least as high as the information to be released, and has a need-to-know. It is the responsibility of the holder of the classified information to ensure the proper clearance and need-to-know of the recipient.

PROTECTING CLASSIFIED INFORMATION

Personnel accessing classified material have the responsibility to know the procedures and the person with whom they share the information.

Classification Markings: Markings are word symbols such as Confidential or Secret, designed for clarity and uniformity and placed according to definite criteria. Any employee who generates classified information must be fully aware of the requirements for the proper marking of the document.

Viewing: When viewing classified material within your workspace, you must ensure that it is not viewable by anyone but you. You must also post a sign indicating, "Classified work is in process."

Transmission: Classified information may be transmitted only to an organization authorized by the DOD to receive and properly store it. Any material transmitted outside the facility must be coordinated through your sponsor.

Generation: Only certain computer systems are approved for classified processing. Prior to access, you will require a special briefing and be provided with a unique User ID and password. Under no circumstances should you ever use another employee User ID when working on a classified computer system.

Reproduction: Only certain devices within the facility are approved for classified reproduction. Therefore, all reproduction of classified material must first be coordinated through your sponsor.

Destruction: Classified material that becomes outdated or no longer has value shall be destroyed. Destruction of classified material must be coordinated through your sponsor.

Storage: Classified material must be stored in GSA-approved containers, vaults, or closed areas with supplemental controls. Confidential material shall be stored in the same manner as Top Secret and Secret; however, no supplemental protection is required. In addition, an open a classified container must be under constant surveillance while it is in the open position.

Unauthorized Transmission: If you receive classified information over your unclassified email system, immediately report it to your sponsor, NMCI and the RED-INC FSO. Do NOT delete the email or file. NMCI/IT personnel will ensure the classified information is purged from your system and your FSO will make any necessary reports.

WHAT TO REPORT

Adverse Information

Any information that raises doubt about the integrity or character of a cleared employee or that causes the DOD to question an individual's judgment, reliability, or suitability to have access to classified information; may include the following:

- Financial
- Personal Conduct
- Allegiance to the USA
- Reliance on drugs or alcohol
- Criminal convictions

Do not report information based on rumor or innuendo.

Suspicious Contacts

- Efforts by any individual, regardless of nationality, to gain illegal or unauthorized access to classified information or to compromise a cleared employee
- All contacts between cleared employees and foreign intelligence officers
- All contacts that suggest that a cleared employee may be the target of an attempted exploitation by the intelligence officers of another country.

Other Reporting Requirements

A name change or citizenship change of a cleared employee. In addition, security violations, sabotage, acts of terrorism, espionage and subversive or suspicious activity must also be reported.

Termination of Employment

You must surrender to the issuer all classified material or equipment in your possession upon termination of employment. You also must sign a debriefing form and return your CAC to the RED-INC FSO prior to your departure.

DOD HOTLINE

Report fraud, waste, and abuse

800-424-9098

Classified Visit Process

Submit the Visit Request Form at least 7 days prior to visit.

Foreign Travel

If you travel to a foreign country for business or pleasure you must complete an International Travel Form prior to departure and be debriefed and sign the Post-Travel Certification upon return.

For security issues or any required reporting contact Valerie James, RED-INC FSO, at 301- 737-4361 ext 23