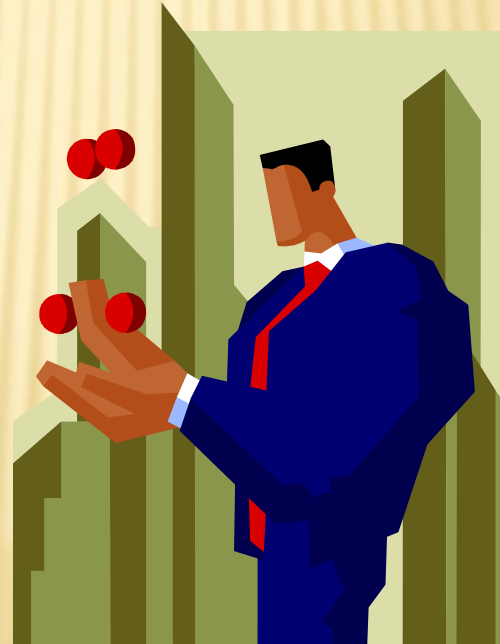




ANNUAL SECURITY REFRESHER BRIEFING

INTRODUCTION

The protection and safeguarding of classified information is all of our responsibilities.



HOW LONG WILL THIS TAKE...?

This Refresher Briefing is built to satisfy annual refresher requirements in a minimum amount of time - about 20 minutes

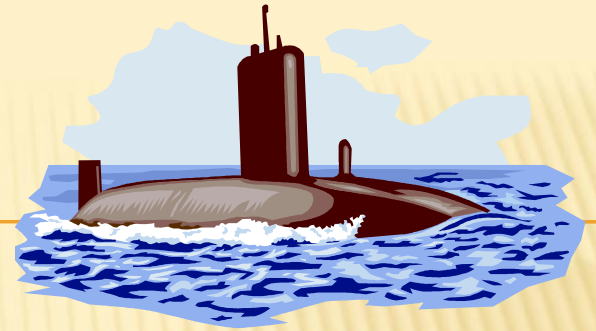
****There will be a test at the End****

REFRESHER TOPICS:

- ❑ Cleared Facility
- ❑ Personnel Security Clearance Eligibility Criteria
- ❑ Cleared Personnel
- ❑ What is Classified Information?
- ❑ Levels of Classified Information
- ❑ Safeguarding of Classified Information
- ❑ Security Violations
- ❑ Counterintelligence Awareness
- ❑ Individual Reporting Requirements
- ❑ Foreign Travel
- ❑ Reporting Hotline Numbers



CLEARED FACILITY



- ❑ A Facility Clearance (FCL) is a determination that a company is eligible for access to classified information or award of a classified contract. This process involves an evaluation of the corporate organization; key leadership; outside corporate relationships; foreign influence, etc.
- ❑ Companies are required to complete a DOD SECURITY AGREEMENT (DD Form 441) which outlines its security responsibilities.
- ❑ As a defense contractor, we are bound by Department of Defense (DoD) rules and regulations to properly protect and control all classified material in our possession. We are authorized to accept and safeguard classified information and materials.
- ❑ **You**, as an employee, are equally bound under the law to provide the same protection and control.

PERSONNEL SECURITY CLEARANCE ELIGIBILITY CRITERIA

Security judgment is based on pattern of behavior, not a single action. It's the "whole person" concept. The 13 Adjudication Guidelines and examples of activities reviewed are:

- ❑ ***Allegiance to US*** – Sabotage, espionage, treason, terrorism. Statements or actions that show allegiance to other than US
- ❑ ***Foreign Influence*** - Unreported personal contacts with foreign intel service, government or persons seeking classified information.
- ❑ ***Foreign Preference*** – Foreign national family members or close contacts. Exercise of any right, privilege or obligation of foreign citizenship
- ❑ ***Sexual Behavior*** – Criminal sexual behavior. Compulsive, self destructive and high risk behavior that you are unable to stop
- ❑ ***Personal Conduct*** – Recurring pattern of poor judgment, irresponsible or unstable behavior. Deliberate omission or falsification of information on a security questionnaire.
- ❑ ***Financial Considerations*** - Not paying bills. Living beyond your means. Not filing tax returns (tax evasion). Bankruptcy.



PERSONNEL SECURITY CLEARANCE ELIGIBILITY CRITERIA



- ❑ ***Alcohol Consumption*** - DUI/DWI. Irresponsible behavior while intoxicated. Concealment of drugs or alcohol while at work.
- ❑ ***Drug Involvement*** - Use of illegal/illicit drugs. Positive drug test for illegal/illicit drugs. Misuse of prescription drugs.
 - ***NOTE:*** Possessing and using marijuana is legal in some states but it is still a federal crime and will impact your clearance.
- ❑ ***Psychological Conditions*** – Problematic behavior not addressed through counseling or other professional avenues.
- ❑ ***Criminal Conduct*** – Arrest. Spousal or child abuse/neglect. Pattern of disregard for rules and regulations.
- ❑ ***Handling Protected Information*** - Unauthorized disclosure. Taking/sending classified information home. Downloading info to an unapproved system.
- ❑ ***Outside Activities*** - Service/employment, paid or unpaid, with a foreign government or representative/person of a foreign interest.
- ❑ ***Use of Information Technology Systems*** - Unauthorized entry into any compartmented system. Attempting to circumvent or defeat security or auditing systems. Introduction, removal, or duplication of hardware/software or media to or from system without authorization.

CLEARED PERSONNEL

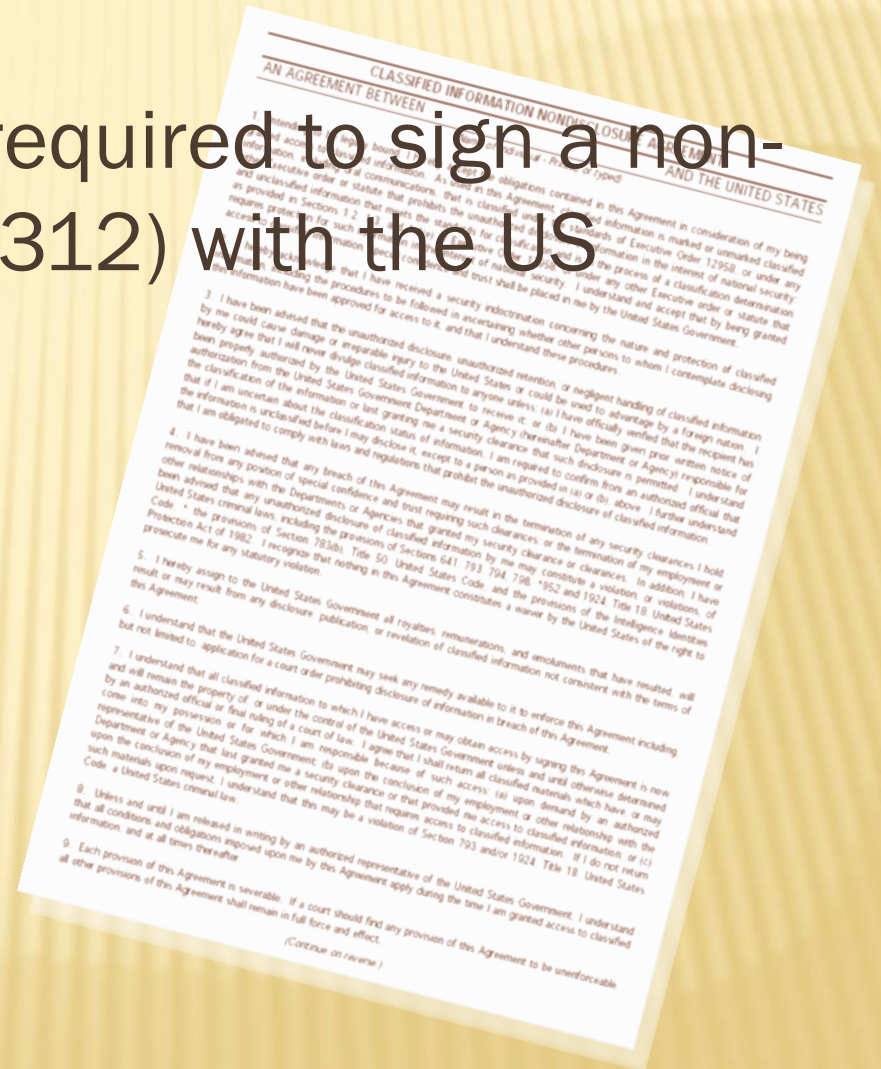
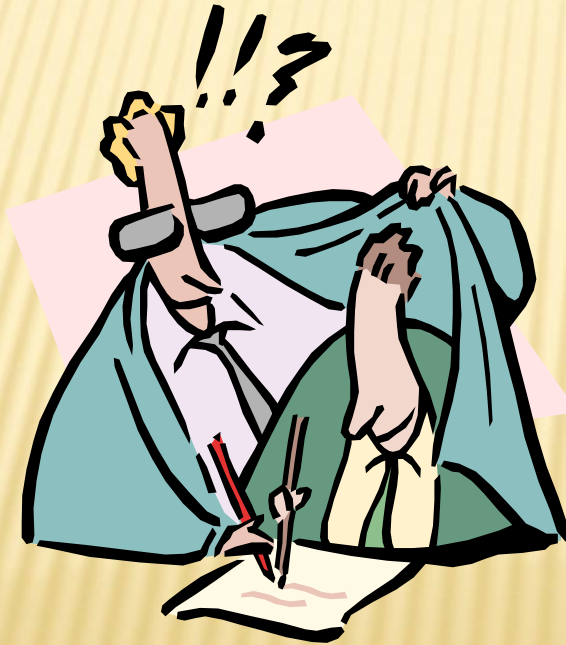
- Department of Defense Central Adjudication Facility (DoD CAF) grants a security clearance based upon the personal information provided on your application (eQIP) and appropriate back ground investigation.
- Access to information is restricted based upon the person's status: Citizen of the United States; Lawful Permanent Resident Alien; or a foreign national authorized to work in the U.S.

Position	Legal Status	Access Levels Allowed
Requires access to classified information	US Citizen	Secret, Top Secret, SCI
Requires access to Controlled Unclassified Information (CUI)	US Citizen Lawful Permanent Resident Aliens	CUI – no government IT systems or technical data access
Requires access to CUI/Government IT Systems/ITAR Technical Data	US Citizen	CUI/Government IT Systems/ITAR Technical Data
General Positions – no access to classified information	Anyone authorized to work in the US	Low sensitivity information



CLEARED PERSONNEL

- Once cleared, you are required to sign a non-disclosure contract (SF312) with the US Government.



CLEARED PERSONNEL



- ❑ The SF312 is a contractual agreement between the U.S Government and you. The primary purpose of the SF 312 is to inform you that:
 - A special trust has been placed in you;
 - This agreement is binding upon you for life (even if you no longer require a security clearance);
 - You are responsible to protect classified information from unauthorized disclosure; and
 - There are serious consequences for not complying with the terms of this agreement.

CLEARED PERSONNEL

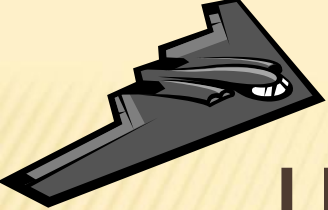


- ❑ All cleared employees will receive some form of security briefing – whether Indoctrination; Orientation; Refresher or other prior to accessing classified information.
- ❑ Dependent upon your specific job and location, security procedures will be based upon instructions provided by the client through DD 254; Classification Guide or other instruction/requirement stated in contracts.
- ❑ All employees must comply with the client security requirements to include security briefings; access to client provided IT systems and classified information.
- ❑ A violation of client security policies and procedures may be grounds for removal from the contract.

WHAT IS CLASSIFIED INFORMATION?

- ❑ Classified Information is that information, the unauthorized disclosure of which could adversely affect the national security of the United States.

The information is usually owned by, produced by, or for or under the control of the U.S. government, and meets the criteria of Executive Order 12356.



LEVELS OF CLASSIFIED INFORMATION

- ❑ **Top Secret**-The unauthorized disclosure of information will cause exceptionally grave damage to US national security.
- ❑ **Secret**-The unauthorized disclosure of information will cause serious damage to US national security.
- ❑ **Confidential**-The unauthorized disclosure will cause damage to US national security.
- ❑ There are other categories of information which, while not classified, also deserve mention:
 - **For Official Use Only (FOUO)** is unclassified government information which is exempt from general public disclosure and must not be given general circulation.
 - **Company private or proprietary information** is business information not to be divulged to individuals outside the company.
 - Recently DoD has placed great emphasis on protecting **Controlled Unclassified Technical Information**. The treatment of this type of information will be addressed in follow on slides



LEVELS OF CLASSIFIED INFORMATION

Controlled unclassified technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. There are no exceptions for commercial items.

- *Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.*



Contractors are required to safeguard unclassified controlled technical information and to report the compromise of such information to the DoD within 72 hours of discovery.

Contractors subject to the clause are required to implement data security controls identified in **National Institute of Standards and Security (NIST)** publication SP 800-53

Contractors are **responsible for assuring that their subcontractors** that are provided with controlled technical information also comply with the data security standards. The new contract clause is a mandatory “flow-down” clause to subcontractors. This includes so-called “cloud” data storage providers.

SAFEGUARDING OF CLASSIFIED INFORMATION

- ❑ Must be under constant personal custody
- ❑ Must never be discussed in public places.
- ❑ Must be discussed on secure phones
- ❑ Must never be left unattended
- ❑ Must be stored in GSA approved storage containers.
- ❑ Must never be processed on your computer unless approved by the Designated Approval Authority.



SAFEGUARDING OF CLASSIFIED INFORMATION



You must never reveal or discuss classified information with anyone other than those that are properly cleared and have a need to know.

If you are in doubt ask your FSO.

SECURITY VIOLATIONS

- ❑ Minor Violations MAY include:
 - Verbal Counseling
 - Written Counseling

- ❑ Major Violations MAY include:
 - Same as minor violations
 - Loss of employment
 - Loss of your security clearance
 - Arrest
 - Imprisonment or fines



Watch out for this guy!!



- ❑ There are representatives from other nations whose goal is to obtain classified information and to utilize that information to their own advantage, and to damage US national security. A clear line must be drawn to protect classified information; anything that is subject to export controls; proprietary information; and controlled unclassified technology.
- ❑ Two most common approaches are:
 - Coercion/Blackmail
 - Cultivation of Relationship

COUNTERINTELLIGENCE AWARENESS

Other approaches include:

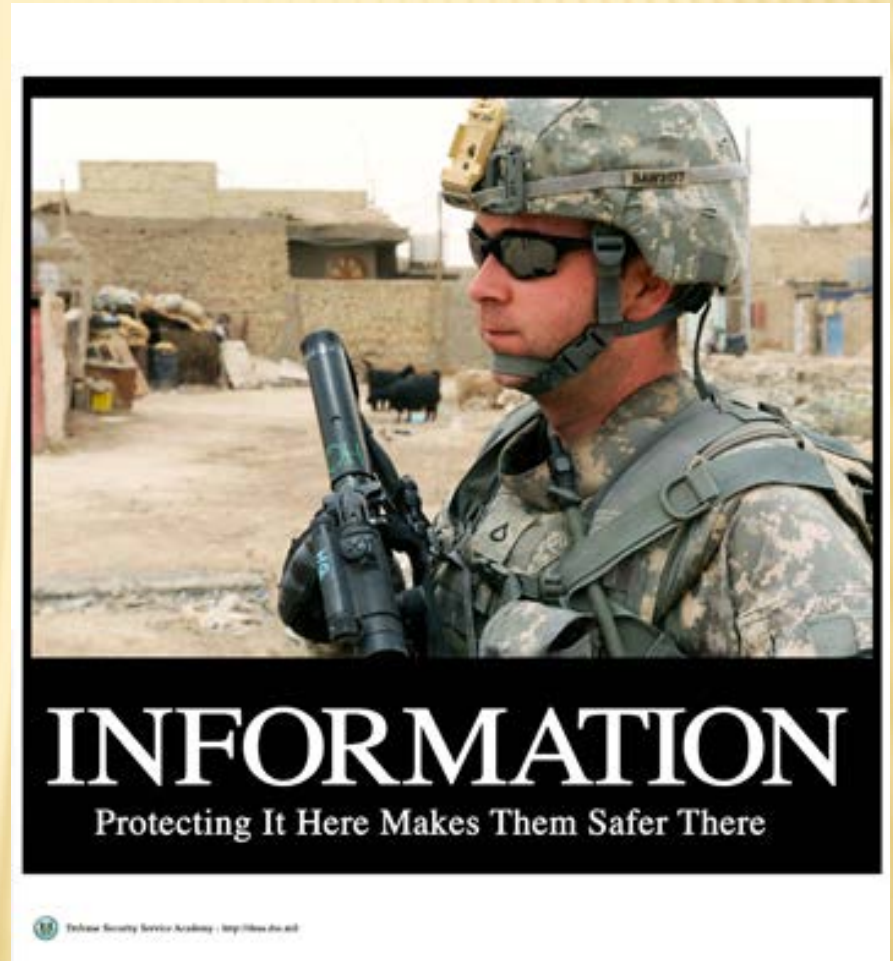
- ❑ Suspicious Network Activity
 - Cyber Intrusion; Viruses/Malware; Backdoor Attacks; Acquiring User Names/Passwords
- ❑ Attempted Acquisition of Technology
 - Front Companies for 3rd Parties; Protected Info; Controlled Technologies; Equipment; Diagrams; Plans
- ❑ Request for Information
 - Attempt to get info through price quotes or market surveys
- ❑ Solicitation or Marketing Services
 - Foreign entities through sales, rep or agency offers; RFI/RFP technical or business services
- ❑ Seeking Employment
 - Resume submissions, applications and references

If you encounter any of these situations that seem suspicious, contact your security officer



WHAT ARE WE DEFENDING?

Information concerning military capabilities, locations, equipment; and technology is protected for a reason. Unauthorized release of this information, whether classified or sensitive can have a detrimental effect on the Warfighters' survivability.



INDIVIDUAL REPORTING REQUIREMENTS

- ❑ Change of personal status: marital status, name change, cohabitation of an intimate nature.
- ❑ Adverse information - arrests, criminal activities, use of drugs, out of character behavior, or treatment for emotional or mental disorders, recurring financial difficulties or excessive indebtedness.

INDIVIDUAL REPORTING REQUIREMENTS

- ❑ Known or suspected espionage or sabotage – suspicious contacts.
- ❑ Becoming a representative of a foreign interest.
- ❑ Known or suspected compromise of classified information.
- ❑ Close and continuing relationships with foreign nationals.



FOREIGN TRAVEL

- ❑ You must report all Foreign Travel and a foreign travel briefing is required. Personnel holding TS/SCI may have additional reporting requirements. Check with your government client or FSO. It is your responsibility to make those arrangements BEFORE you leave.
- ❑ You will need to complete the briefing, complete and return the last page to the FSO prior to leaving. You may even get a telephone call from your FSO to discuss your trip prior to and upon your return as well.
- ❑ Develop a personal travel plan and give it to your office and family
- ❑ Learn the cultures, customs and laws of the country you visit.
- ❑ Visit <http://www.state.gov//> to find country specific information such as:
 - What countries are on the national threat list
 - What countries have high crime/type
 - Shots required
 - Visa/Passport requirements, etc..



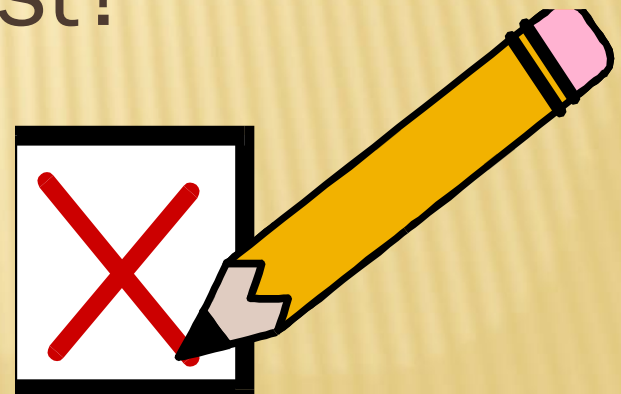
REPORT IT! (HOTLINE NUMBERS)

- ❑ Defense Department 1-800-424-9098, (703) 693-5080
- ❑ Defense Intelligence Agency (703) 907-1307
- ❑ National Security Agency (301) 688-6911
- ❑ Department of Army 1-800-CALLSPY (1-800-225-5779)
- ❑ Naval Criminal Investigative Service 1-800-543-NAVY (1-800-543-6289)
- ❑ Air Force Office of Special Investigations (202)767-5199
- ❑ Central Intelligence Agency Office of the Inspector General (703) 874-2600
- ❑ Department of Energy (202) 586-1247
- ❑ US Nuclear Regulatory Commission Office of the Inspector General 1-800-233-3497
- ❑ US Customs Service 1-800-BE-ALERT (1-800-232-5378)
- ❑ Department of Commerce/Office of Export Enforcement (202) 482-1208 or 1-800-424-2980 (to report suspicious targeting of US export-controlled commodities)
- ❑ Department of State Bureau of Diplomatic Security (202) 663-0739
- ❑ When traveling overseas, suspect incidents should be reported to the Regional Security Officer (RSO) or Post Security Officer (PSO) at the nearest U.S. diplomatic facility

... one more thing

We are glad you paid attention.

Ready for the test?



THANK YOU!

There is no test. So now what....?

Please go to the **SUBMIT** tab located at the right of the menu choices of the Industrial Security Education, Training, and Awareness main page to complete the confirmation portion of this briefing. The security section will get an email confirmation attesting your completion of the briefing.

You are Done!!!