DoD

Initial Security Indoctrination

Security Message

The protection of Government assets, people and property, both classified and controlled unclassified, is the responsibility of each and every member of the Department of Defense, regardless of how it was obtained or what form it takes. Our vigilance is imperative in the protection of this information. Anyone with access to these resources has an obligation to protect it.

The very nature of our jobs dictates we lead the way in sound security practices. Anything less is simply not acceptable. This Initial Security Indoctrination provides a good foundation. Your Agency/Department will supplement this indoctrination with local security policies, procedures, and responsibilities.

Contents

- Physical Security
- Personnel Security
- Information Security
- Antiterrorism/Force Protection
- Information Assurance
- Public Release of Information Operations Security
- Reporting Requirements
- Regulations
- Closing

Objective

- This briefing will:
  - Identify your personal security responsibilities
  - Provide a basic understanding of DoD security policies
  - Explain the importance of protecting government assets

Why Security?

- DoD Security Regulations, Directives, and Programs are established to counter threats
- Threats to classified and unclassified government assets can include:
  - Insider (government employees, contractor employees, and authorized visitors)
  - Criminal and Terrorist Activities
  - Foreign Intelligence Services
  - Foreign Governments

Local Security Office

- Know your local security official:
  - Name
  - Location / contact information
- They will provide you with guidance on security matters within your organization

Add local security info here

Physical Security

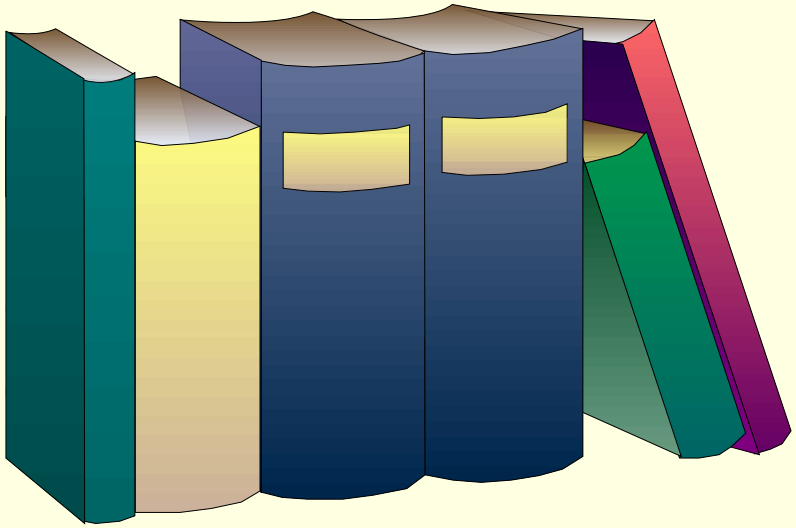
Physical security offers security-in-depth, and includes, but is not limited to:

- Perimeter fences
- Employee and visitor access controls
- Badges/Common Access Cards (CAC)
- Intrusion Detection Systems
- Random guard patrols
- Prohibited item controls
- Entry/exit inspections
- Escorting
- Closed circuit video monitoring

Additional information is available from your local Security Official

Individual Responsibility

- You are responsible for:
  - Becoming familiar with local security regulations pertaining to your assigned duties
  - Notifying your Security Official of changes in your status which could affect your security clearance, defined later in this indoctrination



Your Security Clearance

- Your position sensitivity and/or duties will determine your level of clearance or access
- There are three levels of security clearance:
  - Top Secret
  - Secret
  - Confidential
- Your local Security Official will provide additional guidance if you require a security clearance

Your Investigation and Clearance

- All DoD government and contractor personnel are subject to a background investigation
- Investigations are conducted to determine suitability for a position of trust and/or granting of a security clearance
- Your suitability is continually assessed

Refer to DoD 5200.2-R, DoD Personnel Security Program, Chapter 9 for full details

CLEARANCE

Administrative action, usually involving a form of background investigation and adjudication determination

+

SF 312

Classified Information Nondisclosure Agreement: All persons authorized access to classified information are required to sign a SF 312, a legal contractual agreement between you and the U.S. Government.

+

NEED TO KNOW

Determination made by an authorized holder of classified information that a prospective recipient requires access to perform a lawful and authorized government function.

=

ACCESS

The ability and opportunity to obtain knowledge of classified information. This can involve seeing, hearing, or touching classified information, material, or equipment.

You Must…

- Coordinate with your local security official regarding debriefings and/or out-processing requirements

Information Security

- Pertains to the protection of classified and sensitive information, to include but not limited to:
  - Marking
  - Handling
  - Transmission
  - Storage
  - Destruction

Classification Levels

There are ***THREE*** levels of Classification

TOP SECRET

Exceptionally Grave Damage to the National Security

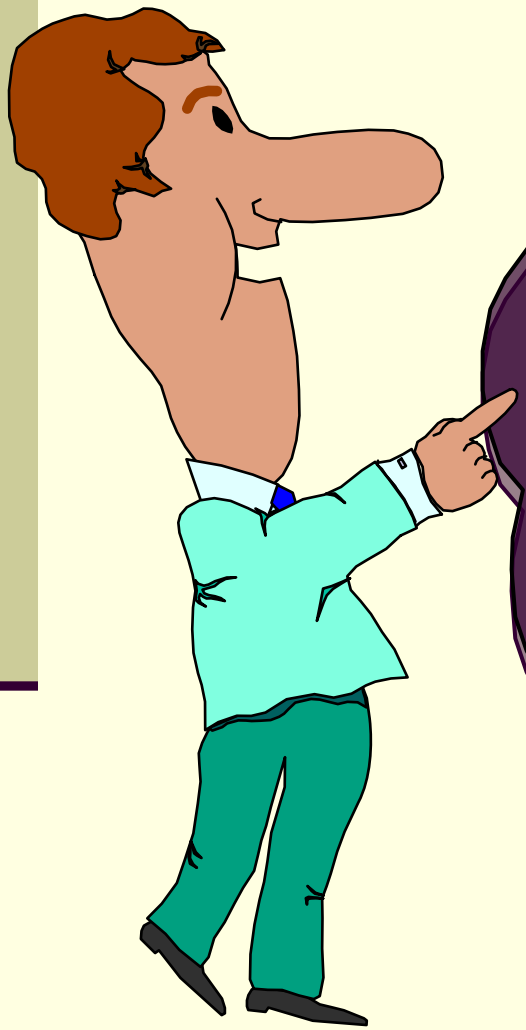
SECRET

Serious Damage to the National Security

CONFIDENTIAL

Damage to the National Security

Classified Material can include ANY of these and must be properly marked:



Machinery, Documents
Emails, Models, Faxes
Photographs, Reproductions
Storage Media, Thumb Drives
Working Papers, Meeting Notes
Sketches, Maps, Products,
Substances, or Materials

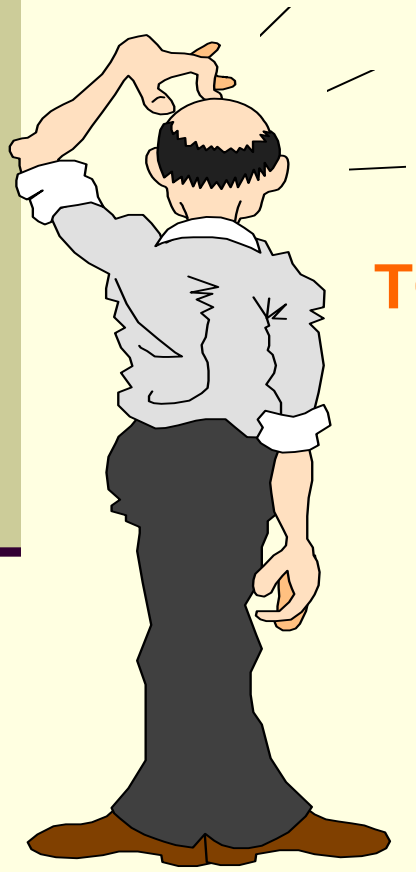
How Do I Identify Classified Documents?

?

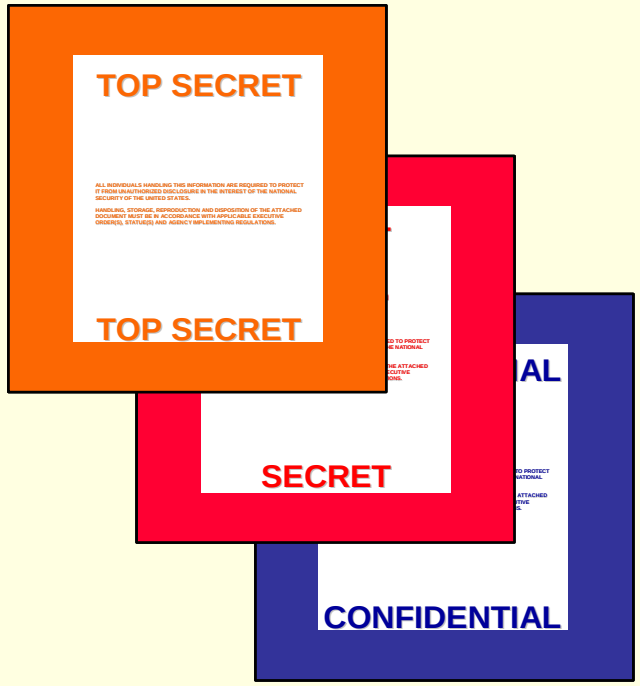
CONFIDENTIAL (C)

SECRET (S)

TOP SECRET (TS)

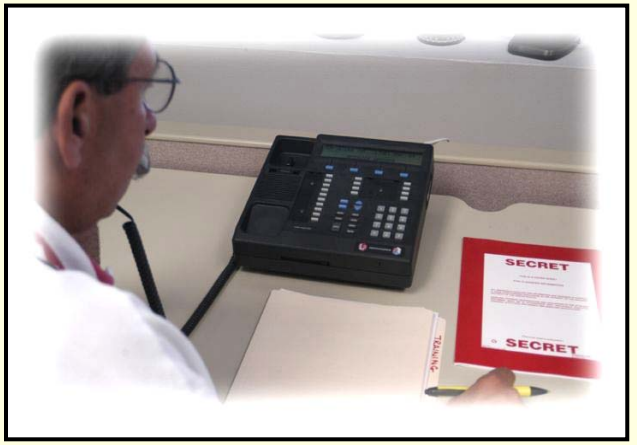


All classified information must be appropriately marked to alert potential recipients to the information's classification.



Classified Information:

- Must be under the control or guarded by an authorized person or stored in a locked security container, vault, secure room, or secure area



- Must be discussed on secure telephones or sent via secure communications
- Must be processed on approved equipment
- Must be destroyed by approved methods
- Must be discussed in an area authorized for classified discussion.

Antiterrorism/Force Protection

- Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces
- Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information

Additional information is available from your local Security Official

Information Assurance (IA)

- In the performance of your duties you may be required to have access to government computer systems
- Information assurance protects and defends information and information systems by ensuring their availability, integrity, authenticity, confidentiality

DoD IA Responsibilities

- Participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering

- Comply with password or pass-phrase policy directives and protect passwords from disclosure

You will receive additional computer security training

Public Release of Information

- Public release of government information must first be approved by the Public Affairs Office

Operations Security “OPSEC”

- Operations Security (OPSEC) is a systematic process used to mitigate vulnerabilities and protect sensitive, critical, or classified information

Additional information is available from your local Security Official

Reporting Requirements…

- You Must Report Change of:

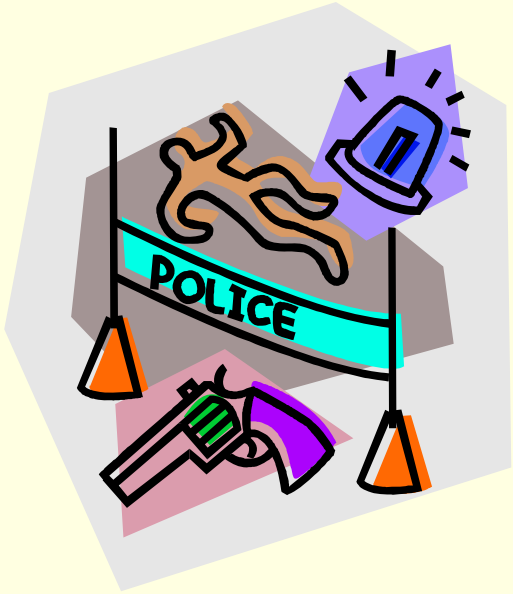
Name

Marital Status

Citizenship

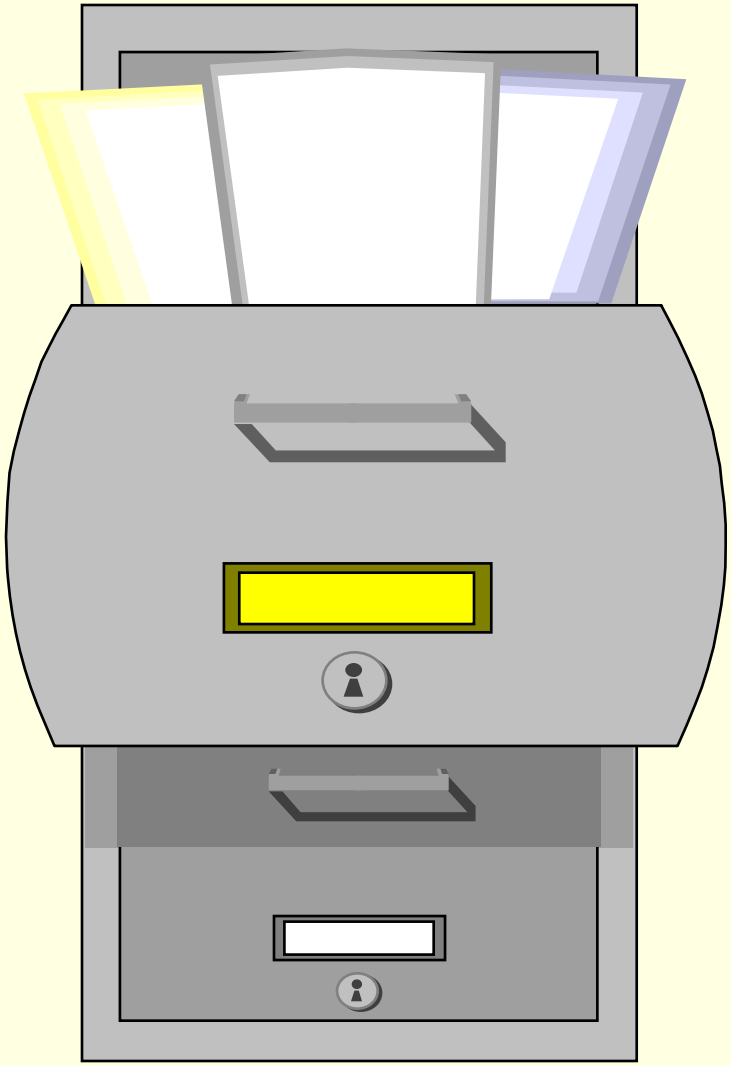
You Must Report…

- Adverse information concerning yourself or a co-worker
- Adverse information includes, but is not limited to recent arrests, alcohol or drug related problems, and/or financial difficulties, etc



You Must Report…

- Loss, compromise, (or suspected loss or compromise) of classified information, including evidence of tampering with a security container used for storage of classified information



You Must Report…

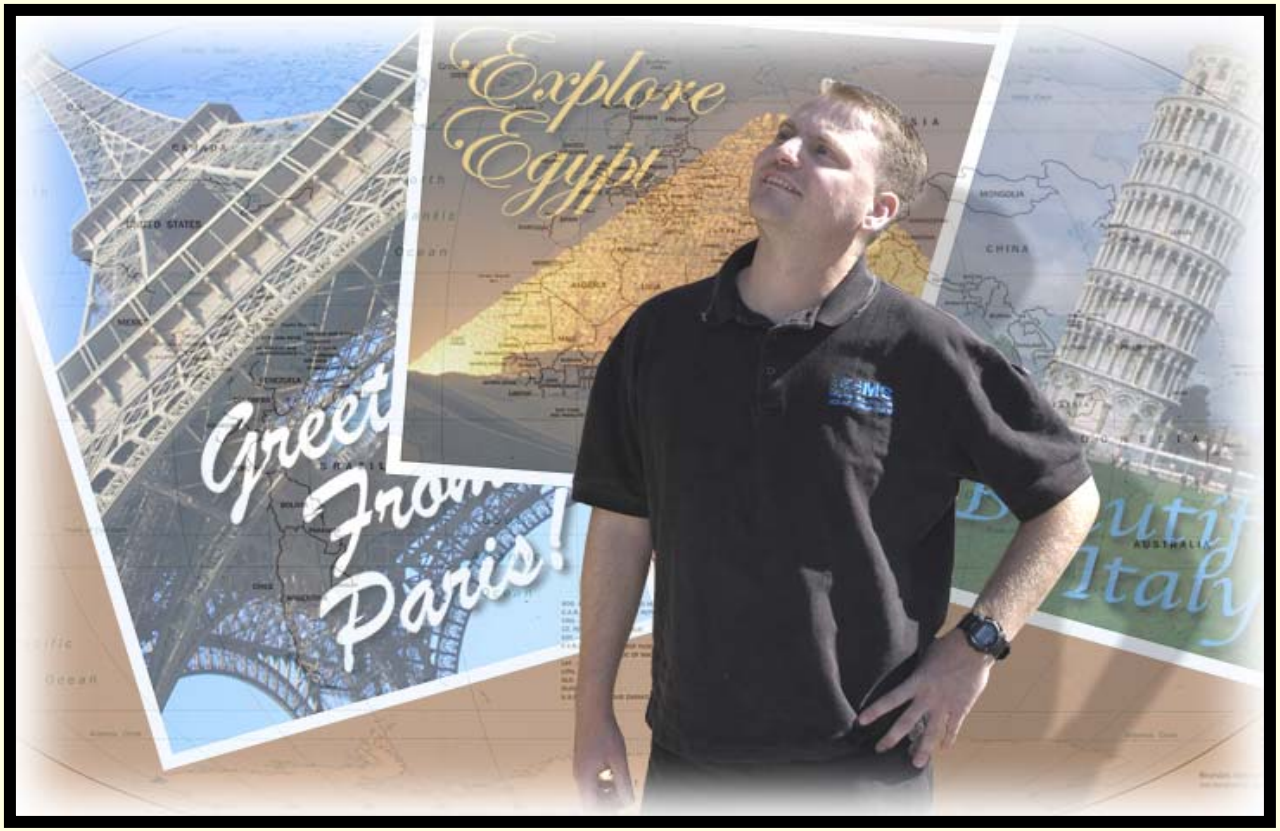
- All continuing contacts with foreign nationals, to include shared living quarters and marriage
- Suspicious contacts with/by foreign nationals

You Must Report…

- If a member of your immediate family (or your spouse's immediate family) is a citizen or resident of a foreign country

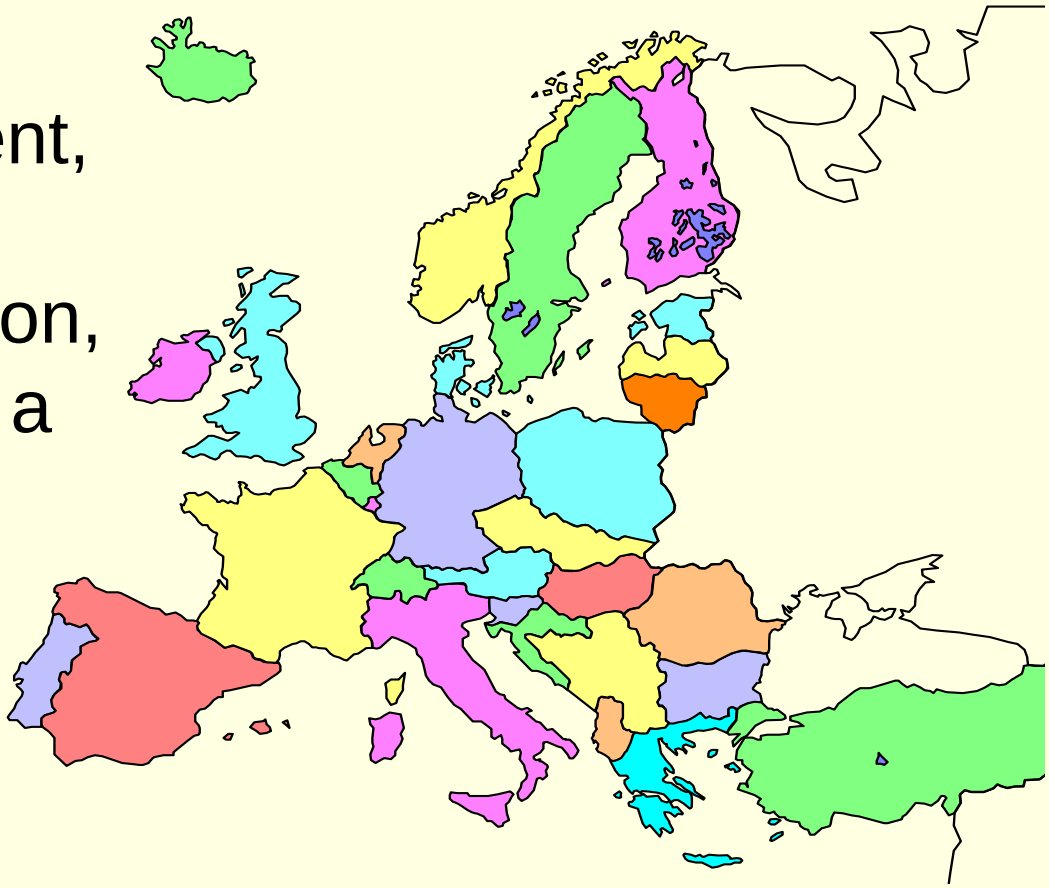
You Must Report...

Foreign travel in accordance with your agency's policies and procedures



You Must Report…

- Any potential employment or service, whether compensated or volunteer, with a foreign government, foreign national, foreign organization, or other entity, or a representative of any foreign interest



You Must Report…

- A lost or stolen badge or Common Access Card (CAC) immediately to your local Security Official

You Must Report …

- All holders of a security clearance must report information to their security office that might have a bearing on their continued eligibility for access to classified information

You Must Report …

- **Potential Espionage Indicators Exhibited by Others**
  - Unexplained affluence
  - Keeping unusual work hours
  - Divided loyalty or allegiance to the U.S.
  - Disregarding security procedures
  - Unreported foreign contact and travel
  - Pattern of lying
  - Attempts to enlist others in illegal or questionable activity
  - Verbal or physical threats
  - Inquiry about operations/projects where no legitimate need to know exists
  - Unauthorized removal of classified information
  - Fraud/Waste/Abuse of government credit cards and/or travel or training advances

YOU CAN MAKE A DIFFERENCE!

- Security is a team effort . . . Your diligence in promptly reporting concerns and adhering to your agency's security policies and procedures will ensure the integrity of national security. As a team, we can protect our warfighters, colleagues, and families from potential harm.

Security Regulations

- **Reference Security Regulations, not all inclusive:**
  - Executive Order 12958, as amended - Classified National Security Information
  - Executive Order 12968 – Access to Classified Information
  - Director of Central Intelligence Directive No 6/4
  - DoD 5200.1-R, DoD Information Security Program
  - DoD 5200.2-R, DoD Personnel Security Program
  - DoDD 5205.2, DoD Operations Security (OPSEC) Program
  - DoD 5200.8-R, DoD Physical Security Program
  - DoDD 8500.1, Information Assurance
  - DODI 8500.2, Information Assurance Implementation
  - DoDD 2000.12, DoD Antiterrorism (AT) Program
  - Homeland Security Presidential Directive (HSPD)-12

Contact…

Your Local Security Official With Any Questions