



INITIAL SECURITY BRIEFING

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 Briefing provides a good foundation.

TOPICS



Physical Security



Personnel Security



Information Security



Antiterrorism



Cybersecurity



Public Release of



Information



Operations Security

Policies

PURPOSE

Understand National and DoD security policies to counter threats

Identify threats to classified and unclassified government assets including, but not limited to:

- Insider
- Criminal and Terrorist Activities
- Foreign Intelligence Entities
- Foreign Governments



KEY PERSONNEL

Command Security Manger:

Ms. Denise Lee

(202) 433-9687

Assistant Command Security Manager:

Mr. Andrew Duley

(202) 433-9688

Security Assistant :

Mr. Donnel Andrews

(202) 433-4285





PHYSICAL SECURITY



PHYSICAL SECURITY

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

- Perimeter Fences
- Antiterrorism
- Employee and visitor access controls
- Badging
- Intrusion Detection Systems
- Guards/patrols
- Prohibited items
- Entry/exit inspections
- Escorting
- CCTV
- Local procedures





PERSONNEL SECURITY



PERSONNEL SECURITY | Individual Responsibility

You are responsible for

- Becoming familiar with local security regulations pertaining to your assigned duties
- Notifying your Command Security Manager of changes in your status which could affect your security clearance, defined later in this security brief.





PERSONNEL SECURITY | SECURITY CLEARANCE

Position sensitivity and/or duties determine level of clearance and access

Position Sensitivity

- Critical Sensitive, Non-Critical Sensitive, Non-Sensitive

Clearance levels

- Top Secret, Secret, or Confidential





PERSONNEL SECURITY | BACKGROUND INVESTIGATION

- **Includes investigations for:**
 - DoD Civilians
 - Military
 - Contractors
- **Conducted to determine suitability for granting a security clearance**
 - Single Scope Background Investigation (SSBI)/Tier 5
 - Access National Agency Check and Inquires (ANACI)/Tier 3
 - National Agency Check with Law and Credit (NACLC)/Tier 3
- **Subject to continuous evaluation**
 - SSBI-Periodic Reinvestigation (SSBI-PR)/Tier 5 R
 - Phased Periodic Reinvestigation (PPR)/Tier 5 R
 - NACLC/Tier 3 R





PERSONNEL SECURITY | ACCESS REQUIREMENTS

CLEARANCE ELIGIBILITY



SF 312



NEED TO KNOW



ACCESS





PERSONNEL SECURITY | DEBRIEFING REQUIREMENTS

- **Coordinate access debriefing during out-processing**
 - Collateral
 - NATO
 - COMSEC
 - SAP
 - SCI





PERSONNEL SECURITY | REPORTING REQUIREMENTS

- **Changes to:**
 - Name
 - Marital Status
 - Citizenship
- **Adverse information**
 - Based on facts **NOT** rumors
 - Self or co-worker
 - Includes but not limited to:
 - Criminal activities
 - Alcohol or drug related incidents
 - Financial difficulties





PERSONNEL SECURITY | REPORTING REQUIREMENTS

- **Loss, compromise, or suspected compromise of classified information**
 - Secure information immediately
 - Report immediately to security or supervisor
- **Foreign contacts**
 - Continuous contact with foreign nationals
 - Includes, but is not limited to:
 - Cohabitation
 - Marriage
 - Suspicious contacts with or by foreign nationals
 - Member of immediate family or spouse's immediate family is a citizen of a foreign country





PERSONNEL SECURITY | REPORTING REQUIREMENTS

- **Foreign Travel**
 - Complete and submit CNIC Foreign Travel Form to Command Security Office
- **Other employment or service**
 - Foreign government, national, organization or entity, or a representative of any foreign interest (paid or unpaid)
- **Lost or stolen badges**





PERSONNEL SECURITY | REPORTING REQUIREMENTS

Potential Espionage Indicators Exhibited by Others

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





INFORMATION SECURITY



INFORMATION SECURITY

- **Pertains to the protection of classified and controlled unclassified information (CUI) from unauthorized disclosure, including, but not limited to:**
 - Marking
 - Handling
 - Transmission
 - Storage
 - Destruction





INFORMATION SECURITY | CLASSIFICATION LEVELS

TOP SECRET Exceptionally Grave Damage to the National Security

SECRET Serious Damage to the National Security

CONFIDENTIAL Damage to the National Security





INFORMATION SECURITY | TYPES OF MATERIAL

Includes, but is not limited to:

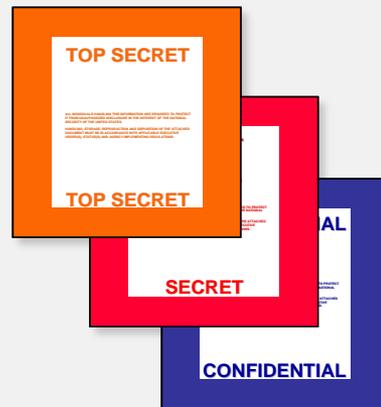
- Machinery
- Documents
- Emails
- Models
- Faxes
- Photographs
- Reproductions
- Storage media
- Working papers
- Sketches
- Maps





INFORMATION SECURITY | MARKING

Appropriately marked to alert recipients of the information's classification



TOP SECRET (TS)

SECRET (S)

CONFIDENTIAL (C)





INFORMATION SECURITY

How Is Information Classified?

- **Original Classification**
 - Only specific positions within the U.S. Government can originally classify information
- **Derivative Classification**
 - All cleared DoD and contractor personnel can be derivative classifiers

Provide definitions of original classification and derivative classification according to EO 13526 and DoD Manual 5200.01 Volume 1





INFORMATION SECURITY

What Information Can Be Classified?

Only information that falls under one or more categories of section 1.4 of Executive Order 13526 may be eligible to be classified:

- a) military plans, weapons systems, or operations
- b) foreign government information
- c) intelligence activities (including covert action), intelligence sources, methods, or cryptology
- d) foreign relations or foreign activities of the United States, including confidential sources
- e) scientific, technological, or economic matters relating to the national security
- f) United States Government programs for safeguarding nuclear materials or facilities
- g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- h) the development, production, or use of weapons of mass destruction





INFORMATION SECURITY

Information cannot be classified to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security
- Classify basic scientific research information not clearly related to national security





INFORMATION SECURITY

Classification Challenges

- **You have a responsibility to report information that you believe is improperly or unnecessarily classified.**
- **Contact your security official for additional guidance for submitting a classification challenge.**





INFORMATION SECURITY

Safeguarding Classified Information

- Must be under the positive control by an authorized person or stored in a locked security container, vault, secure room, or secure area
- Must respect and understand the markings and the downgrade/declassification instructions on classified material
- Must receive appropriate training prior to performing derivative classification duties and refresher training every two years thereafter
- Discuss or send via secure communications
- Process on approved equipment
- Destroy by approved methods
- Discuss in an area authorized for classified discussion





INFORMATION SECURITY

Sanctions

- **You may be subject to criminal, civil or administrative sanctions if you knowingly, willfully, or negligently:**
 - Disclose classified information to unauthorized persons
 - Classify or continue the classification of information in violation of DoD regulations
 - Create or continue a Special Access Program (SAP) contrary to the requirements of DoD regulations
 - Disclose controlled unclassified information (CUI) to unauthorized persons
 - Violate any other provision of applicable DoD regulations
- **Contact the Security Office for additional guidance**





INFORMATION SECURITY

Sanctions

- **Sanctions may include, but are not limited to:**
 - Warning
 - Reprimand
 - Loss or denial of classified access
 - Suspension without pay
 - Removal from employment
 - Discharge from military service
 - Criminal prosecution





INFORMATION SECURITY

Controlled Unclassified Information (CUI)

- **CUI is unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, and Government-wide policy.**
- **Departments and agencies within the U.S. Government assign different CUI designations.**
- **CUI designations include, but are not limited to:**
 - For Official Use Only (FOUO)
 - Law Enforcement Sensitive (LES)
 - Sensitive But Unclassified (SBU)





ANTITERRORISM



ANTITERRORISM

- **Antiterrorism includes 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.**
- **Additionally, antiterrorism includes actions taken to prevent or mitigate hostile actions against personnel (including family members), information, equipment, facilities, activities, and operations.**
- **Personnel must participate in annual ATO Level I training; see N3AT for local guidance.**





CYBERSECURITY



CYBERSECURITY

- **Cybersecurity prevents damage to, protects, and restores information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.**
- **Information systems include, but are not limited to:**
 - Computers
 - Electronic communications systems/services
 - Personal Digital Assistant (PDA) (i.e. BlackBerry)





CYBERSECURITY

Responsibilities

- **Participate in annual cybersecurity training**
- **Comply with password policy directives and protect passwords from unauthorized disclosure**
- **Contact N6 for additional guidance**





PUBLIC RELEASE OF INFORMATION



PUBLIC RELEASE OF INFORMATION

- **Release of government information must be approved by the Public Affairs Office (PAO)**
- **Do not discuss classified or sensitive information with the media; refer inquiries to your local PAO**
- **Public Affairs Director:**

CAPT Wendy L. Snyder

Phone: 202 685 0867

Email: wendy.snyder@navy.mil





OPERATIONS SECURITY



OPERATIONS SECURITY

- **Operations Security (OPSEC) is a systematic process that is used to mitigate vulnerabilities and protect sensitive, critical, or classified information**
- **Initial orientation at a minimum shall include an explanation of OPSEC, its purpose, threat awareness, the organization's critical information, and the individual's role in protecting it.**
- **Contact local OPSEC Officer for additional guidance**





POLICIES



POLICIES

Reference Security Policies and Regulations (not all inclusive):

- Executive Order 13526 - Classified National Security Information
- Executive Order 12968 - Access to Classified Information
- DoDD 5205.02E, DoD OPSEC Program
- DoDI 2000.12, DoD Antiterrorism (AT) Program
- DoDI 8500.01, Cybersecurity
- DoDM 5200.01, Vol. 1-4, DoD Information Security Program
- DoD 5200.2-R, DoD Personnel Security Program
- DoD 5200.08-R, DoD Physical Security Program
- Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors



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.

QUESTIONS

- Contact List
- Security Manager (SM): Denise Lee
 - Assistant SM: Andrew Duley
 - Security Assistant: Donnel Andrews
 - Antiterrorism Officer: Contact N3AT
 - OPSEC Officer: Mr. Andrew Duley