Student Guide - DOD Initial Orientation and Awareness Training

Introduction

Welcome to the Department of Defense, or DOD Initial Orientation and Awareness Training!

The purpose of this training is to provide you with the basic security knowledge necessary to recognize threats to our National Security information and be able to counter those threats in the performance of your responsibilities. Security Managers, if you need to customize this training to meet your organization's needs, a customizable template is available in the resources tab.

Objectives

By the end of this course, you will be able to:

- Describe the National Security eligibility Process
- Understand the Information Security Program and your role in it
- Describe the pre-publication process
- Explain the importance of the Physical Security Program in protecting classified national security information
- Recognize the role of Operations Security (OPSEC)
- Understand the requirements for reporting foreign travel

Introduction to Personnel Security

The Personnel Security Program (PSP) aims to protect national security by ensuring only loyal, trustworthy, and reliable individuals may access classified information and/or be assigned to national security sensitive positions. It also establishes the standards, criteria, and guidelines upon which personnel security determinations are based. Finally, it uses a comprehensive background investigative process to make this determination.

Two key aspects of the PSP are providing access to classified information and ensuring the protection of national security.

Position Designations

Whenever a DOD employee or contractor requires access to classified national security information in the performance of their duties, the individual must be granted national security eligibility at the proper level to access that information. National security eligibility is a favorable determination that affords an individual eligibility for access to classified information or assignment to a national security sensitive position. The National Security Eligibility Process is a four-phased approach that ensures the DOD does not grant access to national security information to people who cannot be trusted.

Civilian personnel designation requirements vary based on how the position is categorized. Within the DOD, each position is categorized with respect to security sensitivity. The Office of Personnel Management (OPM) defines the four civilian position sensitivity levels as Special Sensitive, Critical Sensitive, Non-Critical Sensitive, and Non-Sensitive.

- **Special Sensitive:** Position requires eligibility for access to Sensitive Compartmented Information (SCI)/Top Secret (TS) or Special Access Program (SAP) level information and has the potential for inestimable damage to National Security. (Tier 5)
- **Critical Sensitive:** Position requires eligibility for access to Top Secret (TS) information and has the potential for exceptionally grave damage to National Security. (Tier 5)
- **Non Critical Sensitive:** Position requires eligibility for access to Secret or Confidential level information and has the potential for significant or serious damage to National Security. (Tier 3)
- **Non-Sensitive:** Position requires no eligibility and does not pose damage to National Security. (Tier 1)

National Security Eligibility Process

Military, civilian, contractor, consultant, and other affiliated personnel assigned to national security positions or who are required to perform national security duties will be subject to investigation to determine whether they are and will remain reliable, trustworthy, of good conduct and character, and loyal to the United States and whether granting or continuing national security eligibility is clearly consistent with the national interest.

The four phases of the National Security Eligibility Process are Access, Investigation, Adjudication, and Continuous Evaluation/Periodic Reinvestigation.

Access

The employing activity determines access level based on eligibility, need-to-know, and the requirements of the position held. Before granting access to classified information, all individuals will execute the appropriate non-disclosure forms in accordance with Section 552 of Title 5, United States Code (U.S.C.). If individuals decline to execute the nondisclosure forms, the DOD Component will withhold classified access and report the refusal to the adjudication facility. DOD Components will maintain records of all initial briefings.

Federal Investigative Standards (FIS)

The Federal Investigative Standards, also known as FIS, define a five-tiered investigative model developed in accordance with Executive Order

(EO) 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information". The FIS set standard requirements used to conduct background investigations that determine eligibility to access classified information or hold a national security sensitive position.

For the purposes of this course, we will only focus on Tier 3 and Tier 5 Access, Investigation, Adjudication, and Continuous Evaluation/Periodic Reinvestigation.

National Security Background Investigations

The Tier 3 and Tier 5 national security background investigations determine eligibility for:

- Access to classified information
- Acceptance or retention in the Armed Forces, and
- Assignment to a designated national security sensitive position

Your refusal to complete security documentation may result in the denial or revocation of your eligibility.

Adjudications

After the investigation is complete the case is sent to Adjudications to assess the probability of future behavior that could have an adverse effect on national security.

The DOD Consolidated Adjudications Facility (CAF) is the primary authority for making security eligibility determinations for DOD personnel.

Each case is weighed on its own merits utilizing the whole person concept, which looks at all available and reliable information about an individual's past and present prior to reaching an adjudicative determination.

You can find more information on Adjudicative Guidelines in the resource tab.

Periodic Reinvestigation/Continuous Evaluation

In accordance with DODI 5200.02, "DOD Personnel Security Program (PSP)", all personnel in national security positions shall be subject to continuous evaluation. EO 13467 defines continuous evaluation as

reviewing the background of an individual who has been determined to be eligible for access to classified information. This includes additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.

Every six years, or as needed, you will be subject to a periodic reinvestigation for continued security eligibility. According to the FIS, there are two types of periodic reinvestigations for national security eligibility:

- **Tier 3 R:** Required for continued Secret and Confidential eligibility. Tier 3 R periodic reinvestigations will continue to be conducted every ten years.

- **Tier 5 R:** Required for continued TS or SCI eligibility. Tier 5 reinvestigations have been extended from five years to six years with Director of National Intelligence (DNI) endorsement.

For more information see the Jan 17, 2017, DOD Memorandum "Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog" available in the resources.

Self-Reporting

As part of the National Security Eligibility Process, you must self-report any changes in status, adverse information, and foreign contacts as they occur to the Security Office.

Remember, if you don't self-report, someone else might! Reporting does not automatically result in revocation of eligibility so don't be afraid to report!

Change in Status

Some examples of change in status are:

- Marriage/co-habitation
- Addition of a new family member
- Divorce
- Receipt of a large sum of cash, for example, lottery winnings.

Adverse Information

Adverse information may also be reported, but what is adverse information? Adverse information is "any information that

adversely reflects on the integrity or character of a cleared employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access to classified information clearly may not be in the interest of national security." Some examples of adverse information that you must self-report include:

- Criminal activity, including domestic violence or issuance of a restraining order
- Driving under the influence or driving while intoxicated (known as a DUI or DWI)
- Traffic tickets in excess of $300
- Excessive indebtedness or recurring financial difficulties or bankruptcy
- Use of illegal drugs or misuse of controlled substances
- Any pattern of security violations or disregard for security regulations

Foreign Contacts

DOD personnel are also required to report any close and continuing association with a foreign national to the Security Office. This also includes relationships involving financial or personal ties and requests from anybody seeking access to classified or controlled information.

Note: Failure to report foreign contacts when required may result in reevaluation of eligibility for access to classified information.

Knowledge Check 1

Which Periodic Reinvestigation is required for continued Secret Clearance eligibility?

Tier 2 R
Tier 3 R
Tier 4 R
Tier 5 R

Correct answer: Tier 3 R

Knowledge Check 2

A favorably adjudicated background investigation is required for access to classified information.

True

False

Correct answer: True

Knowledge Check 3

Which of the following must be reported?

Driving while intoxicated
Divorce
A new car purchase
Issuance of a restraining order
Vacation to Disney World

Correct answers: Driving while intoxicated, divorce, issuance of a restraining order

Information Security

Now let's take a look at the Information Security Program and the role that you play in it. Information Security is defined as the system of policies, procedures, and requirements established to protect classified and controlled unclassified information (CUI) that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

Levels of Classified Information

So what is classified information? Classified national security information is official government information that has been determined to require protection against unauthorized disclosure in the interest of national security and is marked to indicate its classified status when in documentary form.

Only individuals with the appropriate eligibility, need-to-know, and signed Standard Form (SF) 312 Classified Information Non-disclosure Agreement may access classified information.

All classified documents require a cover sheet. Classified media such as CDs, DVDs, hard drives, and thumb drives require medium tags or stickers.

The levels of Classified Information are:

- **Top Secret:** If compromised, could cause **exceptionally grave damage** to national security - use SF 703 as a cover sheet. For media, use the SF 706 Top Secret label.
- **Secret:** If compromised, could cause **serious damage** to national security - use SF 704 as a cover sheet. For media, use SF 707, Secret label.

- **Confidential:** If compromised, could cause **damage** to national security - use SF 705 as a cover sheet. For media, use the SF 708, Confidential label.

  Unclassified: This does not require a cover sheet, but you must use the SF 710, Unclassified label for media.

Knowledge Check 1

Which of the following levels of classified information could cause serious damage to National Security if compromised?

Controlled Unclassified Information
Confidential
Secret
Top Secret

Correct answer: Secret

Original Classification

Original classification is the initial government decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing.

Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the DOD.

Authority shall be delegated to, and retained by, only those officials who have a demonstrable and continuing need to exercise it.

Top Secret, Secret, and Confidential may only be used to mark Executive Branch information that has been properly designated as classified national security information under Executive Order (EO) 13526. Information shall not be classified for any reason unrelated to the protection of national security. Individuals who have substantial reason to believe that information in their possession is improperly or unnecessarily classified, must bring their concerns to the attention of their Security Manager or the OCA (with cognizance over the information) to bring about any necessary corrections. Your agency may or may not have an OCA. Please note that additional training is required for OCAs. Refer to DODM 5200.01 Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification”, for more information.

Derivative Classification

Derivative classification is defined as incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

Only individuals with the appropriate security eligibility, need-to-know, who access classified information as part of their official duties, and are properly trained, may derivatively classify information.

Banner lines are at the top and bottom of the document and provide the overall classification marking.

Portion markings denote the classification for each paragraph, sub-paragraph, or section in the document. The Classification Authority Block (CAB) must include the name and position title or personal identifier of the DERIVATIVE classifier and, if not otherwise evident, the Component and office of origin, the source document or classification guide that the document was derived from, downgrade instructions if applicable, and the declassification date.

The only requirement for the placement of the CAB is that it be on the face of the document. While placement on the bottom left of the page is most typical, whether it is placed on the right or left side or appears as one line is determined by available space.

Knowledge Check 2

The Classification Authority Block must be placed:

On the face of the document
On every page of the document
On the last page of the document

Correct answer: on the face of the document

Classification by Compilation

Classification by compilation occurs when unclassified elements of information are combined to reveal classified information, or when classified elements combine to reveal information at a higher classification level than the individual elements.

Marking Slides/Working Papers

Slide presentations and working papers must also be marked. For slide

presentations, the first slide must have the overall classification of the presentation. Each successive slide must be marked either with the overall classification or with the classification of the individual slide. The classification authority block shall be placed on the first or, less preferred, last slide. This placement is required only once. All content of briefing slides, including bullets, captions, titles, and embedded graphs, charts, and figures, shall be portion marked. When marking charts, graphs, or figures, the marking shall indicate the classification of the portion (e.g., bullet, caption, or title), not of the chart itself.

Working papers must be marked with the highest classification of any information contained in the document. They must be dated when created and annotated as "Working Papers." Working papers must be destroyed when no longer needed or re-marked within 180 days as a finished document or when released by the originator outside the originating activity.

For more information on marking, access the Marking Job Aid available in the Resources.

Knowledge Check 3

Working papers must be remarked within _____days as a finished document.

60 days
90 days
180 days
365 days

Correct answer: 180 days

Reproduction

Classified information shall be reproduced only to the extent required by operational necessity or for complying with applicable statutes or directives. In addition, users must adhere to the following guidelines:

- Use only equipment approved to reproduce classified information at the appropriate level
- Ensure that all copies are subject to the same controls as the original copy
- Limit reproduction to what is mission-essential and ensure that the appropriate countermeasures are taken to negate or minimize risk
- Personnel reproducing are knowledgeable of the procedures for classified reproduction and aware of the risk involved with the specific reproduction equipment being used
- Comply with reproduction limitations placed on classified information by originators and special controls applicable to special types of classified information

- Facilitate oversight and control of reproduction

Processing Classified Information on Information Systems

Let's look at the rules for processing classified information on information systems:

- Only systems assessed or authorized to process information at the appropriate level may be used
- Do not install any software on your computer without proper approval
- Do not use another individual's username and password
- Do not allow another individual to use your computer
- Do not attempt to circumvent or defeat security or auditing systems without prior approval
- Do not permit any unauthorized individual access to any sensitive computer network
- Do not modify or alter the operating system or configuration of any system without approval
- Do not write your password down anywhere, it must be memorized

NOTE: Classified documents must be retrieved from the printer in a timely fashion.

Controlled Unclassified Information (CUI)
The Information Security Program also protects controlled unclassified information, or CUI in which unauthorized disclosure could cause foreseeable harm. Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding is considered CUI.

As part of the phased DOD CUI Program implementation process endorsed by the CUI Executive Agent (EA) pursuant to the Information Security Oversight Office (ISOO) Memorandum dated August 21, 2019, the designation, handling, and decontrolling of CUI (including CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management) will be conducted in accordance with DODI 5200.48, "Controlled Unclassified Information", and Sections 252.204-4008 and 252.204-7012 of the Defense Federal Acquisition Regulation Supplement (DFARS) when applied by a contract to non-DOD systems.

All DOD CUI must be controlled until authorized for public release in accordance with DOD Instructions 5230.09, 5230.29, and 5400.04, or DOD Manual 5400.07.

Types of Controlled Unclassified Information

Some examples of CUI include:

- Investigation documents
- Inspection reports
- Agency budgetary information
- Procurement (bids/proposals)
- Personally Identifiable Information (PII)
- Information protected under the Privacy Act of 1974

Does not include classified information.

Information will not be designated CUI in order to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Prevent open competition
- Control information not requiring protection under a law, regulation, or government-wide policy, unless approved by the CUI EA at the National Archives and Records Administration (NARA), through the Under Secretary of Defense for Intelligence and Security (USD(I&S))

Safeguarding

We discussed marking, reproducing, and processing information, but how do you safeguard it? There are differences in safeguarding CUI and classified information.

For CUI:
During working hours, steps will be taken to minimize the risk of access by unauthorized personnel by not reading, discussing, or leaving CUI unattended where unauthorized personnel are present.

After working hours, if the government or government-contract building provides security for continuous monitoring of access, then CUI will be stored in unlocked containers, desks, or cabinets.

If building security is not provided, CUI will be stored in:

- Locked desks, file cabinets, or bookcases
- Locked rooms, or
- Similarly security areas

Safeguard classified information by using:

- General Services Administration (GSA) approved security containers (if not cleared for open storage)
- Vaults and secure rooms

In addition to storing classified information in an approved security container, there are other requirements for protecting classified information. You must:

- Use a secure telephone
- Maintain control of the material at all times
- Never leave classified information unattended
- Never "talk around" classified information by using codes or hints

Remember, that you must never divulge any classified information to unauthorized personnel regardless of the passage of time, the public source of disclosure of data, or their prior clearance, access, or employment status. There is no statute of limitations regarding the unauthorized disclosure of classified information. Contact your Security Office for any questions.

Storage Containers

All classified material must be stored in a GSA-approved security container. If your space has been approved for open storage, contact your security office for additional guidance.

When opening or closing a security container, annotate the date and time on the SF 702, Security Container Check Sheet.

Combinations to security containers and doors to facilities where classified information is processed must be changed under the following conditions:

- When first put into use
- When someone who knows the combination no longer requires access (unless other access controls are in place)
- When the combination is suspected to have been compromised
- When the security container is taken out of service; you must reset to the factory settings of 50-25-50 and combination padlocks must be reset to the standard combination of 10-20-30

The SF 700 Security Container Information must be completed to record the combinations to security containers, secure rooms, and controlled area doors and to identify personnel to be contacted if a security container or facility are found open and unattended. For more information on the SF 700 review CDSE's SF 700 Short.

End of Day Security Procedures

At the close of each day, check the entire workspace and store all classified materials. Ensure security containers have been secured and initial the SF 702, Security Container Check Sheet within the "Checked By" column. Then, verify you have secured all areas and complete the SF 701, Activity Security Checklist.

This may be an additional duty, so check with your Security Manager to find out who has this responsibility.

Knowledge Check 4

Which form is used to record combinations of security containers?

SF 312 – Classified Information Non-Disclosure Agreement
SF 700 – Security Container Information
SF 701 – Activity Security Checklist
SF 702 – Security Container Check Sheet

Correct answer: SF 700 – Security Container Information

Preparing Classified Documents for Mailing

Let's turn our attention to preparing classified documents for transportation. Requirements are as follows:

- The document must have a cover sheet and be placed in an opaque envelope.
- The highest classification level and the dissemination controls must be placed at the top and bottom of both sides of the inner envelope.
- The envelope must be wrapped and reinforced tape must be used to detect signs of tampering.
- The name and address of the recipient and return address (office where it should be returned to if undeliverable or if the outer envelope is damaged or found open) must be noted.
- The inner envelope must also contain a document receipt and destruction certificate.
- Place the inner envelope inside another opaque envelope that is durable enough to properly protect the material from accidental exposure.
- The outer envelope must have reinforced tape to facilitate detection of tampering.
- The outer envelope must be addressed to an official U.S. Government activity or to a DOD contractor with a facility clearance and the appropriate storage capability.
- The outer envelope must contain the return address, with no personal names, as well as the mailing address, again no personal names.
- There must be no classification markings on the outer envelope.

Transmitting and Transporting Classified Information

There are different procedures for transmitting and transporting Top Secret/SCI, Secret, Confidential, and CUI information:

- Top Secret/SCI material may be transmitted by:

    - Direct contact between cleared U.S. personnel
    - Protected facsimile, message, voice
    - Defense Courier Service (DCS)
    - Appropriately cleared courier

    Top Secret/SCI documents **may not** be sent through the U.S. Postal Service or overnight express (i.e. FedEx) delivery services under any circumstances!

- Secret material may be transmitted by:
    - Any of the means approved for the transmission of TS information
    - Appropriately cleared contractor employees, if applicable
    - U.S. Postal Service registered or express mail within and between the U.S. and Puerto Rico
        - You must check "Signature is Required" box
        - Use of external (street side) express mail collection boxes is prohibited
    - U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the U.S. and territories provided the information does not pass out of U.S. citizen control and does not pass through a foreign postal system or foreign inspection
    - Commercial delivery for urgent, overnight delivery only

    Incoming commercial delivery packages must be treated as classified upon receipt and a verification of shipment must be conducted. Open immediately and secure (if applicable).

- Confidential material may be transmitted by:

    - Any of the means approved for the transmission of Secret information
    - U.S. Postal Service certified mail to DOD contracting companies or non-DOD agencies
    - Government agencies (but not contracting companies) may send Confidential material by U.S. Postal Service First Class mail between DOD Components in the U.S. and its territories only. It cannot be sent to contractors via First Class mail
        - Outer envelope shall be marked **"Return Service Requested"**

    Use of external or street side mail collection boxes is prohibited for sending classified material.

- CUI and material may be transmitted by:
    - U.S. Postal Service First Class mail, parcel post, or for bulk shipments via fourth class mail
    - Approved secure communications systems (avoid wireless telephone transmission when other options are available)
    - Facsimile, the sender is responsible for determining that appropriate protection will be available at the receiving location prior to transmission

Knowledge Check 5

SECRET material may be sent via certified mail.

True
False

Correct answer: False

Transporting Classified Materials Within Your Facility

While transporting classified material within your facility, you must provide reasonable protection for the information. The material must be transmitted by cleared personnel and they must travel to the destination without stopping; this includes restrooms and stops for coffee. The transporting must be done person-to-person, and the material may not be left unattended.

Transporting Outside the Facility

For transporting or hand-carrying outside the facility, classified information must be double wrapped or packaged as though it were being sent by mail. For other than commercial air, a briefcase or zippered pouch may serve as the outer wrapper if it is locked and approved for carrying classified material.

The material must be kept under your constant control and delivered only to an authorized person. Prepare an inventory of the material and leave one copy in your office and another copy with a security officer or other responsible person.

You will be required to receive a courier briefing and carry a courier card. Hand-carrying is authorized when the classified information:

- Is not available at the destination
- Is urgently needed for a specific purpose
- Cannot be transmitted in a timely manner

When transporting via commercial aircraft, Courier Letters are required. The courier letters are prepared by the Security Office, and the original and sufficient

copies to provide to airline officials must be carried. The courier letter is only valid for the time it takes to safely transport the classified material to the destination. Be sure to coordinate in advance with airline and terminal officials (including intermediate terminals).

Carrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for overnight storage in a U.S. Government office or a cleared contractor facility.

Destruction of Classified Information

Classified documents and material shall be destroyed completely in order to prevent anyone from reconstructing the classified information. The preferred method of destruction is shredding by using a National Security Agency (NSA) approved shredder.

There are other methods used to destroy classified information such as:

- Burning
- Wet pulping
- Mutilation
- Chemical decomposition, and
- Pulverizing

For non-palpable material or for more information about destruction procedures, contact your security office for additional guidance.

Methods used for clearing, sanitizing or destroying classified information technology (IT) equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

Record and non-record CUI documents may be destroyed by any of the methods for destroying classified information, or as long as the information cannot be recognized or reconstructed. If a law, regulation, or government-wide policy specified a method of destruction, agencies must use the method prescribed.

Knowledge Check 6

Which of the following methods are appropriate for destroying classified information?

Shredding
Burning
Recycling
Throw in trash

Correct answers: Shredding, burning

Security Incidents

We have discussed the importance of protecting classified information; however, there are times when this information may be accidentally or willfully disclosed leading to a security incident.

A security incident can be categorized as either an infraction or violation. Do you know the difference between a security infraction and a security violation? An infraction does not involve loss, compromise, or suspected compromise. A violation could result in a loss or compromise. A loss occurs when classified information or material cannot be accounted for or physically located. Compromise occurs when classified information is disclosed to a person or persons who do not have an appropriate security eligibility, authorized access, or a need-to-know.

A data spill, also known as Negligent Discharge of Classified Information, or NDCI, is a violation and occurs when data is placed on an IT system with insufficient controls to protect the data at the required classification. Most violations and infractions are preventable, so STOP, THINK, and ASK for guidance.

Report violations and infractions immediately to your supervisor and the Security Office. Remember, an infraction that remains uncorrected or unreported may lead to a violation in the future.

Types of Security Incidents

Here are some examples of security incidents:

- Classified material not properly stored
- Classified container not properly secured
- Permitting personnel access to classified information without verifying need-to-know
- Failing to mark classified information
- Discussing classified information in unauthorized areas

NOTE: For more information on security incidents refer to DODM 5200.01 Vol. 3 available in the resources.

Sanctions

You may be subject to criminal, civil, or administrative sanctions if you knowingly, willfully, or negligently disclose classified information or CUI to unauthorized persons. Other punishable offenses include classifying information or continuing the classification of information in violation of DOD regulations.

Sanctions may include but are not limited to: warning, reprimand, loss, or denial of classified access, suspension without pay, termination of employment, discharge from military service, and criminal prosecution.

Knowledge Check 7

A data spill is a _____.

Security infraction
Security violation
None of the above

Correct answer: Security violation

Classified Information in Public Media

In the case of classified information appearing in the public media, remember, never confirm or deny its existence.

Do not respond to questions about programs or projects including those released through:

- Radio or TV
- Newspapers
- Magazines
- Trade journals
- Social media sites, such as Facebook, Twitter, Pinterest, or LinkedIn

Reminder: Any classified information found in the public media may not be viewed or downloaded from unclassified IT systems. Make a note of the URL and other details for where the information was present.

Questions received concerning material appearing in the media shall be referred to your Public Affairs and Security Offices.

Knowledge Check 8

Personnel who receive questions regarding classified information appearing in the media shall be referred to:

Your Security Office
Your Public Affairs and Security Office
The DOD Director
The local U.S. Congressional delegation and your Public Affairs Office

Correct answer: Your Public Affairs and Security Office

Pre-publication Process

Everyone granted access to official information is personally responsible for protecting the information and for complying with the pre-publication security review processes. Materials subject to pre-publication review include:

- Books, manuscripts, or articles to be sent to a publisher, editor, movie producer, or game purveyor, or their respective support staffs
- Any speech, briefing, article, or content that will be publically disseminated
- Any information released to the public, even through Congress or the courts
- Official government and defense industry products as well as materials submitted by cleared, or formerly cleared personnel

The Defense Office of Prepublication and Security Review (DOPSR) is responsible for reviewing written materials both for public and controlled release to ensure information that is publically released does not contain classified, controlled unclassified information or other information that in aggregate may lead to a compromise of national security. See DODI 5230.29, "Security and Policy Review of DOD Information for Public Release" for more information.

Industrial Security

There may be times where you will be working with contractor personnel assigned to your organization. These contractors may or may not be cleared. It is your responsibility to ensure that contractors you work with are appropriately cleared and have a need-to-know for access to classified information. Check with your security office on verifying contractor employee eligibility and need-to-know.

Contractor personnel are cleared under the National Industrial Security Program (NISP), and generally follow the requirements of the National Industrial Security Program Operating Manual (NISPOM). Need-to-know is determined by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program. Contractors participating in the NISP are required to establish procedures to determine need-to-know. Contractors assigned to your organization are required to comply with your facility's security program.

Knowledge Check

Contractor personnel are cleared under which program?

Physical Security Program (PSP)
Information Security Program (ISP)

National Industrial Security Program (NISP)
Operations Security Program (OSP)

Correct answer: National Industrial Security Program (NISP)

Physical Security

Now let's turn our attention to the Physical Security Program. Physical security is that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

Physical Security Countermeasures

At your facility you may notice some of the physical security countermeasures such as:

- **Barriers and fencing:** establish boundaries and deter individuals
- **Intrusion Detection Systems (IDSs):** deter, detect, document, deny, or delay intrusion by detecting a change in the environment. These systems can be exterior or interior and include sensors, control units, transmission lines, and monitor units.
- **Security forces:** made up of DOD, military and contractor personnel, and trained dogs. Most installations and facilities maintain a specially identified group of personnel who serve as the enforcement medium for the physical security program.

Employee Identification

Another part of Physical Security is access control. In order to access a DOD facility you must have a valid employee identification that meets the requirements of Homeland Security Presidential Directive 12 or HSPD-12. The common access card (CAC) is the standard form of identification for DOD employees. In addition to your CAC your organization may issue additional forms of identification (i.e., additional ID cards, or a badge and credential) in order to perform your duties or access restricted areas. Your CAC and other required identification must be kept secure at all times, and protected from loss, theft, and misuse. If your CAC, or other forms of identification are lost or stolen, report it to the Security Office immediately.

All forms of identification must be turned into the Security Office on termination of employment, reassignment to a non-credentialed position, suspension from duty or confirmed misconduct of a serious nature.

Note: If you are issued badges and credentials, they are not to be used as personal identification and must be displayed only when performing official duties.

Escort Requirements

It is imperative that all cleared personnel must ensure access to controlled areas by non-cleared personnel remains at an absolute minimum unless it is mission essential. Only cleared personnel who are familiar with the security procedures of the facility are authorized to escort non-cleared personnel. Ensure all visitors complete and sign the Visitor Log upon entry.

Knowledge Check 1

The standard DOD-wide form of identification is the _____.

State driver's license
Common access credential
Common access card
Central access card

Correct answer: Common access card

Knowledge Check 2

Intrusion detection systems are only used on the exterior of a facility or installation.

True
False

Correct answer: False

Operations Security

Do you consider Operations Security (OPSEC) in your day-to-day activities? OPSEC is the process of identifying critical information and analyzing friendly actions attendant to military operations and other activities. It focuses on preventing our adversaries' access to information and actions that may compromise an operation. OPSEC challenges us to look at ourselves through the eyes of an adversary and deny them the ability to act. An adversary can be an individual, group, country, or organization that can cause harm to people, resources, or missions.

Here are some good individual OPSEC practices:

- Remove your ID badge when you leave your facility
- Do not post or send sensitive information over the Web
- Guard against calls to obtain sensitive information
- Do not discuss sensitive information in public, or over the telephone
- Watch for and report suspicious activity

Knowledge Check

OPSEC is a methodology that denies critical information to the adversary.

True
False

Correct answer: True

Who Could Be a Threat?

So who could be a threat? Any person who lacks the proper national security eligibility and need-to-know but still seeks to gain access to classified information. Some examples are cleared employees, visitors, overly curious family, friends, or neighbors, or foreign nationals.

Most of these threats will exhibit some type of potential espionage indicator (PEI). Listed below are just a few examples:

- Unexplained affluence
- Concealing foreign travel
- Unusual interest in information outside the scope of assigned duties
- Attempting to gain access, without need-to-know
- Foreign travel of short duration
- Illegal downloads

These indicators are not limited to those with access to classified information. Be sure to report all suspicious contacts to your Security Office.

Foreign Travel - Official

All DOD government personnel must provide advance notice of foreign travel plans to the Security Office and receive approval prior to foreign travel. If required, the Security Office will forward the country clearance request to the appropriate U.S. Embassy for approval. Requirements may be different for each agency, so check with you Security Office for specific travel procedures. Standard procedures include the following:

- You must obtain a defensive foreign travel security briefing prior to travel or at least once a year from the Security Office to be briefed on the risks associated with capture, interrogation, harassment, entrapment, or exploitation by hostile nations or groups. Depending on the country you are traveling to, you may also require a country specific briefing from the Counterintelligence office.

- Antiterrorism/Force Protection Level 1 training must be current. If detained or subjected to significant harassment or provocation while traveling, contact the

nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer.

The Security Office will provide information on current threat warnings associated with traveling to and from foreign countries.

Foreign Travel - SCI

It is mandatory for all SCI-Indoctrinated personnel planning foreign travel, personal or official, follow the steps discussed previously. In addition you must:

- Complete a foreign travel questionnaire prior to travel
- Provide a complete copy of your itinerary: flight, hotel, and planned sites to visit (include in the foreign travel questionnaire)
- Upon return from travel, complete a secondary questionnaire
- Be aware of the nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer

Persons granted access to Top Secret and SCI or Department of Energy (DoE) "Q" level classified information incur certain risks associated with travel to, through, or within foreign countries highlighting the need for a defensive security briefing. This briefing provides information on the risks involved in traveling to foreign countries and ways to help minimize those risks.

Failure to report foreign travel may result in reevaluation of eligibility for continued SCI access.

Knowledge Check

How often must you receive a defensive foreign travel briefing?

At least once a year
Prior to travel
At least twice a year
Every two years

Correct answers: At least once a year, prior to travel

Summary

Now that you have completed this course, you should be able to:

- Describe the National Security Eligibility Process
- Understand the Information Security Program and your role in it
- Describe the pre-publication process
- Explain the importance of the Physical Security Program in protecting classified

national security information
- Recognize the role of Operations Security (OPSEC)
- Understand the requirements for reporting foreign travel