Student Guide - DoD Annual Security Awareness Refresher Training

Introduction

Welcome to the Department of Defense (DoD) Annual Security Awareness Refresher Training!

The purpose of this training is to provide a review of basic security principles and responsibilities to protect DoD assets.

Prior to reviewing course material, we will test your knowledge using a pre-test. If you score a 75% or higher on the pre-test, you will be provided feedback on questions missed and receive a certificate of completion. If you score less than 75%, you will be required to view the content for the questions you missed. Once all required sections have been completed, you will be required to take a post-test until you score a 75% or higher in order to receive a certificate of completion.

Pre-Test

Pre-test questions are available in the course and will not be shown here.

Personnel Security

The Personnel Security Program provides security policies and procedures and establishes standards, criteria, and guidelines for personnel security determinations and overall program management responsibilities.

Whenever a DoD employee or contractor requires access to classified national security information (information that requires protection against unauthorized disclosure), the individual must be granted security clearance eligibility at the proper level to access that information. The security clearance process is a tool that helps make sure national security information is not given to people who cannot be trusted.

Within the DoD, each position is categorized with respect to security sensitivity. Categories include:

- **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.
- **Critical-sensitive:** Position requires eligibility for access to TS information and has the potential for exceptionally grave damage to National Security.
- **Non critical-sensitive:** Position requires eligibility for access to Secret or Confidential level information and has the potential for significant damage to National Security.
- **Non-sensitive:** Position requires no clearance or other sensitive National Security duties.

The Personnel Security Clearance Process ensures members of the Armed Forces, DoD civilian employees, DoD contractor personnel, and other affiliated persons are granted access to classified information and/or assignment to a national security sensitive position consistent with the interests of national security. The Personnel Security Clearance Process includes Investigation, Adjudication, Periodic Reinvestigation, and Self-Reporting throughout the process.

Investigations

The Revised Federal Investigative Standards (FIS), signed in 2012, establishes requirements for conducting Federal background investigations to determine eligibility and will be implemented using a phased approach. The revised FIS utilizes a new five-tiered investigative model. For the purposes of this course, we will only focus on Tier 3 and Tier 5 security background investigations, adjudications, periodic reinvestigations, and self-reporting.

The FIS Tier 3 and Tier 5 security background investigations are conducted for national security positions to determine your eligibility for:

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

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

Adjudications

After the investigation is completed, 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 (DoD CAF) is the primary authority for making security clearance 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.

Periodic Reinvestigation

Under the FIS, there are two types of periodic reinvestigations for national security clearances:

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

- **Tier 5 R:** Required for continued TS or SCI clearance eligibility. Tier 5 reinvestigations have been extended from five years to six years with DNI endorsement.

For more information see the DoD Memorandum "Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog" located in the course resource page.

Self-Reporting

As part of the Security Clearance 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 would be: Marriage/co-habitation, addition of a new family member, divorce, or the receipt of a large sum of cash (i.e., lottery).

Adverse Information

Adverse information must also be reported, but what is adverse information? "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 report include:

- Criminal activity, including domestic violence or issuance of a restraining order, driving under the influence/driving while intoxicated (known as a DUI or DWI) and traffic tickets in excess of $300
- Excessive indebtedness or recurring financial difficulties and 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 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 anyone requesting access to classified or controlled information.

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

Information Security

So what is classified information? Classified information is official government information that has been determined to require protection against unauthorized disclosure in the interest of National Security and that has been so identified by being marked. Only individuals with the appropriate clearance eligibility, need-to-know, and signed Standard Form (SF) 312 Classified Information Nondisclosure Agreement may access classified information. All classified documents require a cover sheet. 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.
- **Secret:** If compromised, could cause **serious damage** to national security - use SF 704 as a cover sheet.
- **Confidential:** If compromised, could cause **damage** to national security - use SF 705 as a cover sheet.

We just discussed classified documents. For classified media, such as CDs/DVDs, hard drives, and thumb drives, be sure to use the appropriate medium tags or stickers. Classified medium tags are as follows:

- SF 706, Top Secret label
- SF 707, Secret label
- SF 708, Confidential label

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 clearance, need-to-know, who access classified information as part of their official duties, and are properly trained may derivatively classify information.

Safeguarding and Protecting Information

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

Safeguard CUI by using:

- Locked cabinets
- Rooms with locked outer office doors
- Key or cipher locked rooms

Safeguard classified information by using:

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

In addition to storing classified information in an approved 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, 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 container. If your space has been approved for open storage, contact your security office for additional guidance. When opening or closing a container, record the date and time on the SF702, 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 compromised
- When the security container is taken out of service; you must reset to the factory settings of 50-25-50

The SF700 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 safe or facility are found open and unattended. For more information on the SF 700, review the SF 700 Short.

End of Day Security Procedures

At the close of each day, check the entire workspace and store all classified materials. Ensure containers have been secured and initial the SF702 Security Container Check Sheet within the "Checked By" column. Then, verify you have secured all areas and complete the SF701 Activity Security Checklist.

Preparing Classified Documents for Mailing

Let's turn our attention to preparing classified documents for transportation. If classified material is being mailed, it must be properly prepared. 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 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 return address, no personal names, as well as the mailing address, again no personal names must be marked on the outer envelope. There must be no classification markings on the outer envelope.

Transmitting/Transporting Classified Information

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

- Top Secret may be transmitted by:
    - Direct contact between cleared U.S. personnel
    - Protected facsimile, message, voice (Secure Telephone Equipment (STE))
    - Defense Courier Service (DCS)
    - Appropriately cleared courier

  TS/SCI documents **<u>may not</u>** be sent through the U.S. Postal Service or overnight express (i.e., FedEx) under any circumstances!

- Secret may be transmitted by:
    - U.S. Postal Service registered mail or priority mail express within and between the U.S. and Puerto Rico
        - You must check the "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 that 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 may be transmitted by:
    - 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 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
    - Facsimile, the sender is responsible for determining appropriate protection will be available at the receiving location prior to transmission

Transporting Classified 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 coffee shops. 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, 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 to prevent anyone from reconstructing the classified information. The preferred method of destruction is shredding (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
- Pulverizing

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

Non-record CUI documents may be destroyed by any of the methods above or as long as the information cannot be recognized or reconstructed.

Security Incidents

Previously, we discussed the importance of protecting classified information; however, there are times when this information is accidentally or willfully disclosed leading to a security incident. A security incident can be categorized as either an infraction or violation. Do you know how to differentiate 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(s) who does not have an appropriate security clearance, authorized access, or need-to-know.

A data spill, or Negligent Discharge of Classified Information (known as NDCI), is always a violation and occurs when data is placed on an information technology 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 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 a need-to-know
- Failing to mark classified information
- Discussing classified information in unauthorized areas

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 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.

Pre-Publication Review 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, 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, 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.

Physical Security

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, and information and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

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 (IDS):** 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 contract 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 valid employee identification. The common access card (CAC) is the standard form of identification for DoD employees. Your CAC must be safeguarded and secured at all times and protected from loss, theft, and misuse. If your CAC is lost or stolen, report it to the Security Office immediately.

Operations Security

Do you consider Operations Security (OPSEC) in your day-to-day activities? OPSEC is the process by which we protect critical information whether it is classified or unclassified that can be used against us. 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 the adversary 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

Foreign Travel

Official and Unofficial

All DoD government personnel must provide advanced notice of foreign travel, both official and unofficial to the Security Office. 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 your Security Office for specific travel procedures. 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 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.

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
- Provide a complete copy of your itinerary: flight, hotel, and planned sites to visit (include in foreign travel 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 incur certain risks associated with travel to, through, or within foreign countries. You are required to complete a travel briefing/report for personal travel. Be sure to follow component or agency guidance.

Post-Test

Post-test questions are available in the course and will not be shown here.