Student Guide - DSS Annual Security Awareness Training

Introduction

Hello, I'm Tim Harrison, Chief of Security for the Defense Security Service (or DSS). Welcome to the DSS Annual Security Awareness Training.

Here at DSS we have a dynamic mission that strengthens national security at home and abroad through our security oversight and education operations. Therefore, it is important that our employees stay informed of security related policies, regulations, and threats to our agency. As the chief of security, one of my responsibilities is to ensure that DSS personnel receive security education and training that:

- Provides the necessary knowledge and information to enable quality performance of security functions.
- Promotes an understanding of DSS Security Program policies and requirements and their importance to national security and interests.
- Instills and maintains continuing awareness of security requirements.

The training that you are about to take is just one step in accomplishing this mission. So please take advantage of this opportunity. And remember that security is everyone's responsibility.

Thank you!

Course Objectives

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

- Describe the Personnel Security Clearance Process
- Understand the Information Security Program and your role in it
- Explain the importance of the Physical Security Program in protecting classified information
- Recognize the role of Operations Security (or OPSEC)
- Recognize the importance of protecting your Badge and Credentials
- Identify and respond to threats

Personnel Security

The Personnel Security program is a set of administrative procedures that serves to ensure acceptance and retention of personnel in the Armed Forces and civilian employees in the Department of Defense (or DoD).

The Personnel Security Clearance Process ensures that members of the Armed Forces, DoD civilian employees, DoD contractor personnel, and other affiliated persons are granted access to classified information and/or assigned 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, established 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, and
- 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 DSS Personnel. Each case is weighed on its own merits utilizing the whole person concept, which looks at all available, reliable information about an individual's past and present prior to reaching an adjudicative determination.

Periodic Reinvestigation
Every five years, or as needed, you will be subject to a periodic reinvestigation for continued security clearance eligibility. There are two types of periodic reinvestigations for national security clearances.

- **Tier 3 R:** required every five years or as needed for continued Secret and Confidential clearance eligibility
- **Tier 5 R:** required every 5 years or as needed for continued Top Secret (TS) or Sensitive Compartmented Information (SCI) clearance eligibility

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!

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, and
- Any pattern of security violations or disregard for security regulations

Foreign Contacts
DSS 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 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

Now let's take a look at the Information Security Program and the role that you play in the program. 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.

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 Non-disclosure 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. All information, no matter what form or format it is in, must be marked. 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

Original Classification
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 believe that information in their possession is inappropriately classified or inappropriately unclassified must bring their concerns to the attention of the Office of Security. Remember only individuals specifically authorized in writing may originally classify documents. DSS does not have Original Classification Authority (OCA).

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. DSS derivatively classifies information.

Banner lines are at the top and bottom of the document and provide the overall classification markings as well as the dissemination control markings. Portion markings denote the classification for each paragraph, sub-paragraph, or section in the document. In the bottom left is the Classification Authority Block that includes the name and title of the classifier, the source document that the document was derived from, and the declassification date.

Classification as a Result of 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 title slide must have the overall marking and classification authority block. Each successive slide must have the overall classification marking at the top and bottom as well as portion markings for each individual bullet. If a slide has graphics, the portion marking is spelled out to provide a distinction between the classified status of the graphic and the overall classification of the slide. 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 outside the originating activity.

Reproduction
Classified information shall be reproduced only to the extent required by operational necessity. In addition, users must adhere to the following guidelines:

- Use only equipment approved to reproduce classified 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
- 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 accredited to process classified 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.

For Official Use Only (FOUO)
The Information Security Program also protects Controlled Unclassified Information (CUI). Within the DoD there is a type of CUI For Official Use Only (FOUO) that if disclosed could reasonably be expected to cause foreseeable harm. Examples of FOUO include:

- Investigation documents
- Inspection reports
- DSS budgetary information
- Procurement (bids/proposals)
- Personally Identifiable Information (PII)
- Information protected under the Privacy Act of 1974, and
- Does not include classified information

NOTE: A new CUI policy will be released in the near future.

Safeguarding and Protecting Information
We discussed marking, reproducing, and processing classified information, but how do you safeguard the information? Safeguard classified information, FOUO, and other CUI by using:

- Government Services Administration (GSA) approved containers (if not cleared for open storage)
- Locked cabinets
- Key or cipher locked rooms
- Rooms with locked outer office doors
- Guarded buildings or alarms

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 the DSS Security Office for any questions.

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 the AF310 document receipt and the 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 as well as the mailing address, no personal names for either, 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 FOUO 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
- 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 "Signature is Required"
    - 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
- 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"**
- FOUO may be transmitted by:
  - U.S. Postal Service First Class mail, parcel post, or for bulk shipments via fourth class mail

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, and
- 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
For destruction of Classified information, FOUO, or other CUI, shredding (using a National Security Agency (NSA) approved shredder) is the preferred method. For any shredder-related problems, contact the Security Office, the Support Services Office, and Logistics Management Division. Burning is another method of destroying classified information. Be sure to contact the Security Office to see if your location has a burning procedure plan. All non-palpable materials (i.e. classified equipment) shall be returned to the Property Management Office.

Security Incidents
In the previous slides, 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 DSS 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 need-to-know
- Failing to mark classified information
- Discussing classified information in unauthorized areas

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
- Facebook
- LinkedIn
- Social media sites, such as Facebook, Twitter, Pinterest, or LinkedIn

Questions received concerning material appearing in the media shall be referred to the DSS Public & Legislative Affairs Office and the DSS Security Office.

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

Employee Identification
A Common Access Card (CAC) is the DoD Federal credential under Homeland Security Presidential Directive 12 (HSPD-12). It is a standardized DoD-wide form of identification used by civilians, contract personnel, and military personnel. It contains protected personal identifying data and a Public Key Infrastructure (PKI) certificate set and is used for email encryption, digital signing, and network and application access. If your CAC is lost or stolen, report it immediately to the Security Office.

Escort Requirements
It is imperative that all cleared personnel ensure access to controlled areas by non-cleared personnel remains at an absolute minimum unless it is mission essential. Only DSS civilians, contract personnel, and military personnel (if applicable) are authorized to escort non-cleared personnel. In a controlled area like a Sensitive Compartmented Information Facility (SCIF), there can be three non-cleared persons per authorized escort. In a Secure Area (Collateral Space) five non-cleared persons per authorized escort are allowed. Ensure all visitors complete and sign the Visitor Log upon entry.

Safeguarding Classified Information
All classified material must be stored in a GSA approved container when not in use. Even if your space has been approved for open storage, the DSS Director has instituted a clean desk policy, which means that all classified material will be secured at the end of each day. Blinds and window coverings must remain closed at all times. 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 SF700, review the SF700 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.

Operations Security

Do you consider Operations Security (OPSEC) in your day-to-day activities? OPSEC is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures, identify, control, and protect unclassified information that is associated with sensitive activities and operations.

The OPSEC process is a five step analytical process. In Step 1, you must identify critical information. In Step 2, analyze the threats. For Step 3, analyze the vulnerabilities. In Step 4, assess risks. In Step 5, apply the appropriate countermeasures.

Badge and Credentials

If you have a DSS Badge and Credentials (B&C), they must be safeguarded and secured at all times. They must be protected from loss, theft, and misuse and displayed only when performing DSS duties. It is not to be used as personal identification. The DSS Badge and Credential must be turned in on:

- Termination of employment
- Reassignment to a non-credentialed position
- Issuance of an updated badge and credential
- Suspension from duty, or
- Confirmed misconduct of a serious nature

If your badge and credentials are either lost or stolen, please report it to the DSS Security Office immediately.

Threats

So who is a threat? Any person who lacks the proper clearance and need-to-know but still seeks to gain access to classified information. They can be:

- Cleared employees/Insider threat
- Visitors
- Other defense contractors
- Overly curious family, friends, or neighbors
- Foreign nationals/persons
- Students

Some Potential Espionage Indicators (or PEIs) are:

- Unexplained affluence
- Concealing foreign travel
- Unusual interest in information outside the scope of assigned duties
- Unusual work hours
- Taking classified material home
- Disgruntledness
- Copying files
- Unreported contact with foreign nationals
- Attempting to gain access, without need-to-know
- Unexplained absences
- Foreign travel of short duration

- Avoiding polygraph
- Terminating employment, and
- Illegal downloads

These indicators are not limited to those with access to classified information.

Report all suspicious contacts to the DSS Security Office.

Spies Still Exist
The role of the spy, "the Secret Agent," has become so sensationalized and magnified that it is very easy to think that spies exist only in the minds of fiction writers and that spying belongs in the same category as science fiction. Current threats include targeting of:

- Critical technologies
- Proprietary economic data
- U.S. officials
- National defense information
- Employees as industrial spies

Cases
Bryan Minkyu Martin, a Petty Officer and Navy intelligence specialist at the Joint Special Operations Command, pled guilty to attempted espionage and was sentenced to 34 years in prison in May, 2011. Martin was arrested in a sting operation in which he passed classified documents to an undercover agent of the FBI claiming to be an intelligence officer from a foreign country. Martin was suffering severe financial problems when he sold the classified material to a man he believed to be a Chinese spy.

Elliot Doxer, former employee of Akamai Technologies, Inc., pled guilty to espionage charges after offering to hand over confidential information about the Web acceleration company to an Israeli consular official in Boston. Doxer sent an email to the Israeli Consulate stating that he was willing to provide information from his employer that might help Israel. An undercover FBI agent posing as an Israeli intelligence officer spoke to Doxer and established a "dead drop" where the two could exchange information. For the next 18 months, Doxer visited the dead drop at least 62 times. Doxer provided customer and employee lists, contract information, and other trade secrets. He pled guilty to one count of foreign economic espionage and was sentenced in December 2011 to six months in prison, six months home confinement, and fined $25,000.

Foreign Travel - Official
All DSS government personnel who will be conducting official travel to or through foreign countries should obtain a DSS official passport. This is not required but is advisable. You must provide 30 - 45 days advance notice of travel

plans to the DSS Security Office. The DSS Security Office will forward the country clearance request to the appropriate U. S. Embassy for approval.
You must obtain a defensive foreign travel security briefing prior to travel or at least once a year from the DSS 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. The DSS 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
- 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 and below incur certain risks associated with travel to, though, or within foreign countries. You are not required to complete a travel briefing/report for personal travel; however, it is highly recommended that all personnel are briefed of the risks associated with capture, interrogation, harassment, entrapment, or exploitation by hostile nations or groups.

Reporting Requirements
According to DoDD 5240.06, personnel who fail to report contacts, activities, indicators, and behaviors associated with Foreign Intelligence Entities may be subject to judicial and/or administrative action.

If you believe that a foreign entity has attempted to contact or recruit you or you suspect a co-worker of suspicious activities; contact your Counterintelligence Office and DSS Security Office immediately.

Summary

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

- Describe the Personnel Security Clearance Process
- Understand the Information Security Program and your role in it
- Explain the importance of the Physical Security Program in protecting classified information
- Recognize the role of Operations Security (or OPSEC)
- Recognize the importance of protecting your Badge and Credentials
- Identify and respond to threats