Student Guide – DOD Annual Security Awareness Refresher Training

Introduction

Welcome to the DOD Annual Security Awareness Refresher Training!

Annual refresher training is designed to reinforce the policies, principles, and procedures covered in your initial and/or specialized training. 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 the 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

Select the Start Pre-test button to begin.

Personnel Security

The Personnel Security Program, or PSP, is designed to protect national security by ensuring only loyal, trustworthy, and reliable individuals are granted continued access to classified information or assigned to national security sensitive positions.

It establishes the vetting standards, criteria, and guidelines for personnel security eligibility or trust determinations.

The PSP also outlines the comprehensive background investigative process used to make all eligibility or trust determinations.

Trusted Workforce 2.0 Overview

In an effort to modernize the PSP, the interagency Security, Suitability, and Credentialing Performance Accountability Council or PAC is in the process of transitioning to Trusted Workforce 2.0, or TW 2.0.

Once fully implemented, the TW 2.0. initiative will reform the personnel vetting process through the use of new Federal Personnel Vetting Investigative Standards, among other concepts.

We will discuss these new standards and concepts in more detail throughout this module. For a quick overview, please review the Personnel Vetting Investigative Standards Crosswalk Job Aid in the Resources.

The goal of the government's personnel vetting reform is to improve onboarding and vetting processes, improve reciprocity and mobility within the federal workforce, and to advance real-time insight into the trusted workforce's behaviors through continuous vetting, or CV.

Another goal of the TW 2.0. initiative is to create a culture of trust in the personnel vetting process by promoting transparent communication between the individual and the government during each vetting phase.

Personnel Vetting Framework Overview

The TW 2.0 presents a revamped personnel vetting framework that establishes five personnel vetting scenarios that focus on establishing trust, maintaining trust, and re-establishing trust.

These scenarios follow an individual from their entry into the trusted workforce through their exit:

- Initial Vetting
- Continuous Vetting
- Upgrading Vetting
- Re-establishing Trust
- Transfer of Trust.

An individual can have many career changes or life changes that impact their position in the life cycle of the personnel vetting model. For this reason, a one-size-fits-all approach to personnel vetting is not efficient or practical.

This shift to a more streamlined personnel vetting framework allows for more efficient vetting and investigations. It also aims to enhance workforce mobility for trusted individuals.

Initial Vetting

The first scenario in the vetting life cycle, Initial Vetting, occurs when an individual enters into the trusted workforce. It is the first step for an outsider to become a trusted insider and is designed to establish the trust relationship between the government and the individual.

This initial vetting process takes a deep dive into the individual's background to investigate and collect relevant information that provides context for specific behaviors needed to make a trust determination.

One important goal of the personnel vetting reform is to enhance workforce mobility. The TW 2.0 will transition from five federal investigative standards to three. The three tiers in

this framework are Low, Moderate, and High.

Each tier appropriately aligns investigations to vetting for suitability, fitness, credentialing, and national security clearance eligibility decisions. The type of initial background investigation performed for an individual will still depend on the position designation or the level of access an individual requires.

Position designations align with a position's risk determination or its potential impact on national security. For example, a High Tier investigation occurs for an individual whose position requires access to Top Secret information. This investigation would be more comprehensive than a Moderate-Tier investigation that occurs for the individual whose position requires access to Secret or Confidential information.

Another shift in the initial vetting process with TW 2.0 is the rollout of DCSA's new IT platform known as the National Background Investigation Services, or NBIS. The National Background Investigation Services streamlines not only Initial Vetting but the entire vetting process from end to end.

Each step in the process is on one platform. This includes the application and initiation, the investigation, adjudication, the determination repository, and then finally continuous vetting or CV enrollment. The transition to NBIS includes the launch of the new eApp program to replace the functions provided by e-QIP. e-QIP was formerly used to process the standard forms questionnaire that federal applicants used to provide information for their initial background investigations.

The use of eApp has accelerated the background investigation process through improved application features that help applicants complete the detailed background investigation form more accurately. A few of its notable features are timeline validation, real-time address checks through the U.S. Postal Service, real-time form section reviews, branching questions, and auto-saving information.

Let's follow an applicant through the initial vetting process.

- The individual submits the security questionnaire associated with their position designation through eApp.
- The background investigation is initiated and conducted using the Federal Personnel Vetting Investigative Standards.
- Once the investigation concludes, a DOD Consolidated Adjudicative Services adjudicator reviews and makes a trust determination as to whether the individual is an acceptable risk.
- This determination is sent and stored in the clearance repository, and the initial vetting stage is complete.
- If the individual receives a favorable trust determination, he or she is enrolled in the CV program.

Continuous Vetting

During the second scenario in the personnel vetting framework, an individual has already established a trust relationship with the government, they are considered a trusted insider, and are now responsible for maintaining that trust.

So, what exactly is Continuous Vetting? Continuous Vetting, or CV, involves regularly viewing a cleared individual's background information to ensure they continue to meet requirements and should continue to hold positions of trust.

This process is designed to occur regularly throughout an individual's period of eligibility. CV relies on automated record checks that pull data from criminal, terrorists, and financial databases, as well as public records.

If an alert is received, DCSA assesses whether the alert is valid and worthy of further investigation. DCSA investigators and adjudicators then gather facts and use any relevant data found to make determinations.

CV helps DCSA mitigate potential security concerns before they become larger problems, either by working with the individual to mitigate issues, or in some cases suspending or revoking trust determinations. The primary goal of CV is to promote early detection, reduce risks, and address concerning behaviors and perceived vulnerabilities as they emerge.

With the emergence of the continuous vetting model in the TW 2.0, the need for periodic reinvestigations, or PRs, has been eliminated. Individuals will no longer undergo a PR at predetermined intervals as was required in the past. Instead, individuals will simply re-validate their security questionnaires at a determined timeframe.

For more information about Continuous Vetting, visit DCSA's Personnel Vetting website.

Upgrading Vetting

The third vetting scenario, Upgrading Vetting, occurs when an already vetted individual needs a higher level of security eligibility than they currently possess. To facilitate the upgrade in trust, there must be an upgrade in vetting, but the individual will not have to start from scratch with initial vetting.

Instead, the Investigative Service Provider, or ISP, will perform any additional investigation requirements that were not performed during the initial vetting stage. This method of building upon prior investigations allows federal agencies to have more timely access to the talent they need to support mission requirements.

Re-establishing Trust

The fourth Personnel Vetting scenario, Re-establishing Trust, occurs when a previously

vetted individual has had a break in employment or service for a period of time. Upon returning, that individual needs to re-establish trust between themselves and the government.

The government agency bringing on the individual has some flexibility in determining the level of vetting that will be conducted as long as the break in service was less than 36 months.

Transfer of Trust

Transfer of Trust is the fifth personnel vetting scenario in the TW 2.0 that occurs when an individual transfers across federal agencies or to a new government role.

Transparency in ISP reporting is critical in ensuring investigative and adjudicative actions are not duplicated.

Since Personnel Vetting requirements among all DOD entities will be aligned, reciprocity of trust determinations will be much easier to achieve.

CV and Self-Reporting

Remember, Continuous Vetting, or CV, is designed to ensure that you continue to meet security eligibility requirements through a process of automated records checks.

This responsibility does not fall solely on the government. You are also expected to take ownership of maintaining your eligibility through self-reporting and staying current on DOD rules and policies that could affect your eligibility status.

Let's take a look at the type of information you are required to self-report.

Self-Reporting Requirements

As part of the security eligibility process, you must immediately self-report any changes in status, adverse information, foreign contacts, and foreign travel to the Security Office. Remember, if you do not self-report, someone else might! Reporting does not automatically result in suspension or revocation of eligibility, so do not be afraid to report.

Everyone granted eligibility to access classified information is subject to the reporting requirements in Security Executive Agent Directive 3, or SEAD 3. Please note that your specific agency may have additional reporting requirements not discussed in this lesson. Select each topic on screen to review the types of changes in your status that you must report immediately.

Foreign Contact

You must report any unofficial contact with known or suspected foreign intelligence entities. This includes any continuing associations with foreign nationals that involve bonds of affection, personal obligation, intimate contact, or any contact that involves the exchange of personal information. The method of contact does not matter. It can occur in person or via electronic methods like phone calls, texting, emails or even through the postal system.

Adverse Information

Adverse information must be reported because it is an indicator that your continued access to classified information may not be in the best interest of national security. Adverse information is any information that might adversely reflect on your integrity or character as a cleared employee.

This list is not all-inclusive, but we will describe some examples of adverse information. Self-report any criminal activity. This includes domestic violence, receiving a restraining order, and driving under the influence or driving while intoxicated, also known as DUI or DWI. Self-report any traffic tickets in excess of $300 and any financial issues or changes such as excessive indebtedness, recurring financial difficulties, or filing for bankruptcy. Self-report using illegal drugs or misusing controlled substances. You should also report any security violations or disregard for security regulations.

Financial issues are the number one reason for security eligibility revocations and denials; however, it is important to understand that most financial issues can be mitigated if the financial delinquencies are largely out of your control, or you can show you have acted responsibly given the circumstances.

Concealing or failing to report adverse information often times has a greater negative influence than the actual information itself. To learn more about adverse information reporting requirements, visit CDSE's website and select The Adverse Information Reporting Short under Personnel Security.

Change in Status

A change in your personal status is also a reportable action.

- This includes any financial gains such as gambling winnings, selling a home or vehicle, or perhaps an inheritance. If the infusion of assets is greater than $10,000, it must be reported. Other reportable changes in status can include the birth of a child, a recent divorce, or a new marriage.

Foreign Travel

You are also required to report any foreign travel. To do so, submit an itinerary for unofficial foreign travel to your agency for approval. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary are discouraged.

Report any deviations from your approved itinerary within five business days of returning. Exceptions to this policy do exist and can be viewed in their entirety in SEAD 3.

To learn more, review the SEAD 3 Guidelines in the student resources.

Federal Law Consideration

The DOD has issued several memorandums pertaining to the use of marijuana, cannabinol or CBD, as well as investments in marijuana dispensaries, growing operations, and other marijuana industry-related businesses and stocks.

To review the relevant DOD guidance on CBD and marijuana, please select the student resources tab.

Marijuana remains a federally controlled substance despite state laws that legalize or decriminalize it. Prior recreational use remains relevant to the whole-person concept but does not, on its own, necessitate an unfavorable trust determination.

You should be aware as a federal workforce employee that the purchase, use, distribution, and cultivation of marijuana is forbidden, despite any state laws stating the contrary.

Recent DOD guidance also states that the willful and direct investment in businesses involved in processing, manufacturing, cultivating, purchasing, selling, or distribution of marijuana-related products should be considered by adjudicators in their evaluation as to whether an individual is trustworthy to occupy a national security position.

Un-willful and non-direct investments through mutual funds can be considered mitigating in such circumstances.

The DOD further advises the workforce to refrain from the use of CBD products. CBD products are not regulated by the FDA, which means Tetrahydrocannabinol, or THC, within CBD products is not FDA certified.

Therefore, there is a great risk that using CBD products can cause sufficiently high enough levels of THC to result in a positive marijuana drug test under agency-administered employment or random drug testing programs.

TW 2.0 Implementation

The DOD is implementing many changes to the Personnel Security Program and the processes used to vet its workforce. New policy and procedures are being released iteratively to ensure agencies are adhering to the requirements of TW 2.0.

It is imperative for you to stay aware of the latest PSP policy changes and implementation of the TW 2.0 to ensure you remain compliant with the requirements necessary to maintain your national security eligibility.

Controlled Unclassified Information

What is Controlled Unclassified Information, or CUI? CUI is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.

Unlike classified national security information, or CNSI, the Department of Defense, or DOD, personnel at all levels handle CUI when it is mission-related or deemed there is a lawful government purpose to do so.

Additionally, DOD personnel at all levels have the responsibility to protect CUI in their possession throughout its life cycle. CUI life cycle phases include identifying CUI appropriately, safeguarding it while it is under your control, sharing it according to guidelines and policy, and decontrolling it as soon as it is no longer requires protection.

Although CUI does not meet the threshold to be CNSI, or atomic energy information, it does require some level of protection from unauthorized access and disclosure and public release.

The establishment of CUI was necessary to formally acknowledge that certain types of unclassified information are extremely sensitive and valuable to the United States and require protection.

The CUI program establishes a common marking system across all federal agencies, a registry to capture the various categories of unclassified information that require safeguarding based on laws, regulations or government policies, and safeguarding standards.

As with other protected information, CUI can come in all forms. This includes:

- Electronic equipment such as cell phones and computers
- Physical documents
- Media
- Software

All types of CUI must be appropriately marked. This includes physical equipment, email, media, documents, and CUI display markings on DOD unclassified systems and networks where appropriate.

Additionally, DOD information systems used to process, store, or transmit CUI must be categorized at the moderate confidentiality impact level. This is in accordance with Part 2002 of Title 32, Code of Federal Regulations and DODI 8510.01 Risk Management

Framework for DOD Systems. We will discuss minimum required CUI markings in detail later in this module.

CUI History

So what is the history of CUI? The concept of CUI is not new. In 2004 the 9/11 Commission highlighted the need for improving information sharing between agencies that protect national security. This heightened focus to create a protected information-sharing environment eventually led to the issuance of Executive Order, or EO, 13556, Controlled Unclassified Information in 2010. This order established guidelines and requirements for the CUI program and designated the National Archives Records Administration, or NARA, to oversee all agency actions to ensure compliance with the order.

In response, NARA established the CUI office and appointed the Information Security Oversight Office, or ISOO, to handle these oversight responsibilities as the CUI Executive Agent. In 2012, the DOD issued DODM 5200.01 Volume 4 to address EO 13556. In November of 2016, the implementing guidance, 32 Code of Federal Regulations, or CFR, Part 2002, Controlled Unclassified Information was published as a final rule.

In March 2020, the DOD issued DOD Instruction, or DODI, 5200.48, Controlled Unclassified Information to replace DODM 5200.01 Volume 4.

The DOD CUI program, managed by the OUSD (I&S) Information Security Office, provides policy guidance and resources for DOD in accordance with national-level issues and orders. We will review resources offered on the DOD CUI Program website throughout this lesson.

Visit DOD CUI Program website for a quick review. DOD contractors should reference the Defense Federal Acquisition Regulation Supplement, or DFARS, Section 252.204-7008 and 252.204-7012 for guidance on protecting DOD CUI.

Legacy Considerations

Legacy information is any sensitive unclassified information that was marked prior to the implementation of the DOD CUI Program, such as For Official Use Only or FOUO, and Sensitive but Unclassified or SBU. The CUI program does not require the remarking or redacting of Legacy marked documents as long as it remains under the control of, or shared within, the DOD.

If a Legacy document is going to be shared outside DOD or used as a source in a derivative document, it must be reviewed beforehand to determine if it still aligns with a category in the new DOD CUI Registry. It must then be marked as CUI if the information still qualifies. Legacy information does not automatically qualify as CUI. The owner of the information must review it to determine if it meets new CUI requirements per DODI

5200.48.

Identifying CUI

It is important to standardize your process when creating or identifying CUI. Consider incorporating the steps we will review to help determine if the information meets the requirements in policy to be designated as CUI. The first step in the process when identifying or creating CUI is to determine if the information meets the standards for classification in accordance with DODM 5200.01 Volume 1. If the answer is no, then move to step two.

In step two, you need to determine if the information falls within a law, regulation, or government-wide policy that requires protection. To do this, search the appropriate CUI registry to identify if the information aligns with one of the CUI categories. As mentioned earlier, this step applies to Legacy information as well. All Legacy information must be reviewed to determine if it still qualifies as CUI per the registry.

The Information Security Oversight Office as the Executive Agent for CUI created the ISOO CUI Registry. This is the government-wide CUI online registry. It includes CUI categories, abbreviations and guidance for marking, Limited Dissemination Control guidance, a CUI Registry Change Log, and CUI policy guidance.

Visit the ISOO CUI Registry online to learn more. The DOD CUI Registry mirrors the ISOO registry with the addition of aligning CUI categories to national policy and DOD issuances. Visit the DOD CUI Program's CUI Registry to become more familiar with the official list of categories used to identify the various types of CUI. You can also review the list of CUI Categories and Abbreviations in Student Resources. Other federal agencies have also created their own CUI registries with approval from ISOO.

The information owner, or IO, of the CUI should seek guidance from their agency to determine the appropriate CUI registry to reference. If the information does not align with a law, regulation, or government-wide policy that requires protection, you cannot mark it as CUI. If you have identified the information as CUI, you can move on to step three where you make note of the CUI category abbreviation. You will need this CUI abbreviation for the Designation Indicator, or DI, block.

In some instances, CUI could fall under more than one category. In this case, all CUI abbreviations will need to be noted in the DI block. We will discuss the CUI DI block and other minimum marking requirements next.

Minimum Marking Requirements

Once you identify and designate the information as CUI, the next step in protecting the information is to apply the minimum marking and dissemination controls.

During the initial implementation of the CUI program, there are two minimum required

markings. The first requirement is to include just the acronym CUI centered in the banner and the footer of documents. The second requirement is to include the DI block at the bottom right of the first page or on the cover sheet.

These minimum marking requirements also apply to emails. The CUI banner and footer marking as well as the DI block can be justified left in the body of the email.

Portion marking documents containing CUI is optional at this time; however, if any portion markings are included anywhere in the document, they must be included consistently throughout. One exception to this is that when CUI is comingled with classified information, these documents must be portion marked.

The DI Block is similar to the Classification Authority Block, or CAB, used on all classified national security information. At minimum, the DI Block must include the name of the DOD component identifying the information is CUI.

Let's walk through the information on each line in the DI Block.

- The first two lines contain the controlled by information.
    - The first line should list the DOD component or owner of the CUI.
        - If the document is on official letterhead, the first controlled by line can be omitted.
- The second controlled by line must list the office responsible for making the CUI determination.
- The third line must list the categories of CUI in the document. Categories must align with the DOD CUI Registry.
- The fourth line must contain the Limited Dissemination Controls, or LDCs, and Distribution Statement if applicable. For example, a Distribution Statement is required for CUI containing Critical Technical Information, or CTI. ***(****For more information on minimum marking requirements and LDCs, visit the DOD CUI Program webpage and select the Training Resources tab.)*
- The fifth line must include the office phone number or mailbox for the originating DOD component or authorized CUI holder.

There are two controls levels for CUI - CUI Basic and CUI Specified. There are no laws, regulations, or government-wide policies specifying handling or dissemination requirements for CUI Basic; however, CUI Specified will include those specific requirements.

Forthcoming CUI guidance will outline specific distinctions and requirements for these two control levels. However, during the initial implementation of the CUI program, all DOD information will be safeguarded in accordance with CUI Basic.

Safeguarding CUI

During working hours, take steps to safeguard CUI to minimize the risk of access by

unauthorized personnel. This includes not reading or discussing CUI around unauthorized personnel and ensuring CUI is never left unattended.

After working hours, IF the Government or Government-contract building provides security for continuous monitoring of access, safeguard CUI properly by storing it in unlocked containers, desks, or cabinets. IF there is NO continuous security monitoring of building access, store CUI in locked desks, file cabinets, bookcases, locked rooms, or a similarly secured area.

At minimum when teleworking, as a "Best Practice," implement the same safeguarding measures as you would for a building not continuously monitored by security. Remember to establish and maintain a secure "Controlled" working environment.

Disseminating CUI

Remember when sharing CUI that no individual should have access to CUI unless it is determined that they have a lawful, government purpose. A lawful, government purpose is any activity, mission, function, operation, or endeavor that the U.S. government authorizes or recognizes as within the legal scope for disseminating CUI. The holder or owner of the CUI is responsible for making this determination before disseminating.

- Although using CUI coversheets, SF 901, is optional, as a best practice, use the coversheet as added protection to alert those receiving the information of protection requirements.
- CUI may be transmitted via first class mail, parcel post, or bulk shipments.
- Avoid disseminating CUI through cell phones when other options are available.
- When practical, transmit CUI electronically only via an approved and authorized secure communications system.
- Do not use your personal email to share CUI. At minimum, ensure to encrypt emails on DOD systems containing CUI.

CUI can be shared via facsimile or fax; however, the sender is responsible for determining that appropriate protections are in place at the receiver's location before sending. For example, the sender should confirm that someone authorized to receive CUI attends that fax machine.

Unauthorized Disclosure and Misuse

The DOD Components' Senior Agency Official, or CSAO, or appointed Component Program Manager, or CPM, must ensure procedures are in place to manage the unauthorized disclosure or other misuse of CUI. This includes improper CUI designation, marking, handling, disseminating, or any other incident placing CUI at risk of UD in accordance with DODI 5200.48.

Senior leaders and supervisors at all levels are responsible for taking administrative, legal, or other corrective actions in response to CUI misuse or UD. Actions should align

with appropriate law, regulation, or government-wide policy.

Corrective or disciplinary action should focus on implementing measures to protect CUI and eliminate any conditions or circumstances that contributed to the incident. UD of certain types of CUI, such as export controlled technical data, could result in criminal or civil sanctions.

Reporting of misuse, mishandling, or UD of CUI to the Unauthorized Disclosure Program Management Office, or UDPMO, is required. Additionally, when appropriate, it is required to notify the appropriate Military Department Counterintelligence or CI Organization of CUI UD incidents.

Decontrolling CUI

There is no required timeline for decontrolling CUI, unless specifically required by law, regulation, or Government-wide policy.

Agencies should promptly decontrol CUI as soon as it no longer requires safeguarding controls unless doing so conflicts with a related law, regulation, or government-wide policy.

CUI documents must be formally reviewed or undergo the prepublication review process in accordance with DODI 5230.09, Clearance of DOD Information for Public Release, before being decontrolled or released to the public.

Contact the CUI information owner to discuss decontrolling CUI when the need arises. Situations that may warrant a decontrol request include any request to release CUI to the public, the end of a contract, or upon contract renewal.

Destruction of CUI

Before destroying any CUI, ensure processing through records management in accordance with policy as well as following procedures in accordance with DODI 5230.09, Clearance of DOD Information for Public Release.

When destroying CUI, including electronic forms of CUI, agencies must ensure destruction methods leave CUI unreadable, indecipherable, and irrecoverable. If a law, regulation, or government-wide policy requires a specific destruction method, agencies must use the method prescribed.

Any methods approved to destroy classified information can be used for the destruction of CUI. Two approved methods for destroying paper-based CUI are cross-cut shredding that produces 1 mm x 5 mm particles (or smaller) or pulverizing. For additional guidance on destroying CUI documents and materials, reference DODM 5200.01 Vol. 3 and CUI Notice 2019-03.

Levels of Classified Information
So what is classified information? Classified information is official government information which has been determined to require protection against unauthorized disclosure in the interest of national security and marked to indicate its classified status. Only individuals with the appropriate security eligibility, need-to-know, and a 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. For classified media, such as CDs and 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 and Original Classification

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.

Original Classification

Original classification is the initial government decision about what information needs to be classified and protected as such. These decisions are important, because they have implications for how that information must be handled and for who may access and use it.

Only government officials with authority to make original classification decisions can originally classify documentation. The officials who perform original classification are referred to as Original Classification Authorities or OCAs.

Safeguarding Classified Information

Safeguarding

"Safeguarding classified information" means being able to securely receive, use, store, transmit, reproduce, and appropriately dispose of classified information. There are differences in safeguarding classified information and CUI.
Safeguard Classified Information by using:
GSA approved security containers (if not cleared for open storage), vaults, and 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, 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 eligibility, access, or employment status.

There is no statute of limitations regarding unauthorized disclosure, or UD, of classified information. Contact your Security Office for any questions.

Safeguard CUI by using:

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

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 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 or 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 reset to the standard combination 10-20-30

The Standard Form 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 security container 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.

Transmission and Transportation of Classified Information

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 also 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.

Transporting and Transmitting Classified Information

There are different procedures for transmitting and transporting Top Secret/SCI, Secret, Confidential, and CUI. Select each type to learn more.

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

- Any of the means approved for the transmission of TOP SECRET information
- Appropriately cleared contractor employees, if applicable
- U.S. Postal Service registered or priority express mail within and between the U.S. and Puerto Rico
  - You must check the "Signature is Required" box
  - Use of external (street side) priority 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 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 CONFIDENTAL 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 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.

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 (DD 2501). 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 or 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.

Methods used for clearing, sanitization or destruction of classified 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 approved for destroying classified information or by any method that ensures the information cannot be recognized or reconstructed. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed.

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 a 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 or persons who do not have appropriate security eligibility, authorized access, or need-to-know.

A spillage, 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 or unreported may lead to a violation in the future.

Types of Security Incidents

Here are some examples of security incidents:

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

For more information on security incidents refer to DODM 5200.01 Volume 3 in the Resource Tab.

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.

Prepublication Review Process

Everyone granted access to official information is personally responsible for protecting the information and for complying with the prepublication security review processes.

Materials subject to prepublication 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 publicly 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, or DOPSR, is responsible for reviewing written materials both for public and controlled release to ensure information that is publicly released does not contain classified, Controlled Unclassified Information or CUI 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. The Physical Security Program is that part of security concerned with physical measures designed to safeguard personnel; preventing unauthorized access to equipment, installations, material, and documents; and safeguarding against espionage, sabotage, damage, and theft.

Physical Security Countermeasures

At your facility you may notice some of the physical security countermeasures such as barriers and fencing, Intrusion Detection Systems or IDS, and security forces. Select each measure to learn more.

- **Security forces:** are 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.
- **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.

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 or CAC and the Personal Identity Verification or PIV are the standard forms of identification for DOD employees. Your CAC and PIV must be safeguarded and secured at all times, and protected from loss, theft, and misuse. If your CAC or PIV is lost or stolen, report it to your Security Office immediately.

Operations Security (OPSEC)

What is Operations Security? Operations Security, or OPSEC, isn't just a set of rules that dictates what you should or shouldn't say or do.

- It's a cyclical approach of denying critical information to an adversary.
- OPSEC is a method to identify, control, and protect critical information. It is also a method to analyze friendly actions and indicators that would allow adversaries or potential adversaries to identify and exploit vulnerabilities.
- Lastly, it is periodic assessment of security effectiveness.

OPSEC Cycle Overview

Leaders at all levels of the Department of Defense, or DOD, have the responsibility to integrate the OPSEC cycle into planning, executing, and assessing their organization's day-to-day activities and operations.

As an individual, you also have a responsibility to support the DOD by being vigilant and taking steps to safeguard critical information.

We will discuss the OPSEC cycle and the important guidelines the DOD and you, as an individual, must follow to protect critical information.

Identify Critical Information

The first step of the OPSEC cycle is to Identify Critical Information. Critical information is information that the DOD has determined is valuable to an adversary. Information that is deemed "critical" may vary based on an organization's role.

Critical information is best identified by the personnel responsible for planning and executing the organization's mission. Under direction of the OPSEC program manager, a Critical Information List, or CIL, is created.

Are you familiar with your organization's critical information list?

What is Critical Information?

Let's dig deeper. Critical information is unclassified or controlled unclassified information, or CUI, that reveals information about DOD activities, intentions, capabilities, or limitations.

It often includes indicators that are sometimes revealed through publicly available information.

Indicators are facts or pieces of information that when merged together like pieces of a puzzle can be used to collect, analyze, and exploit information to gain an advantage.

Do you know what information must be protected? Do you understand why this information must be protected?

Examples of Critical Information

Let's review some examples of critical information. Adversaries collect information pertaining to U.S. DOD activities and technology to further their own agendas.

As previously mentioned, even unclassified information can hold great value to an adversary.

Some examples of critical information are deployment dates and location, military operations, training operations and missions, schedules and travel itineraries, acquisitions, Agency Program of Instructions (POI), Position, mission capabilities, and limitations.

CUI PII

We've just reviewed how to identify critical information that is unclassified. However, another form of critical information is Controlled Unclassified Information, or CUI. CUI is unclassified information that requires safeguarding and dissemination controls that are consistent with applicable law, regulations, or government-wide policies.

Sometimes the CUI an adversary seeks is personally identifiable information, or PII.

Types of PII adversaries might collect include:

- Usernames, passwords, network details, social security numbers, credit card information, and bank account information.
- Personal information that can be used alone or with other relevant information to confirm an individual's identity qualifies as PII. The Privacy Act of 1974 protects this information.

Remember adversaries can compile small details and indicators or "aggregations" to deduce enough information about day-to-day activities or U.S. military plans and operations to do us harm.

Other Vulnerable CUI

As mentioned earlier, CUI is unclassified information that requires protection by law. Besides PII, what are some other types of CUI that adversaries may try to collect?

Some other examples of vulnerable CUI are pre-decisional information and meeting minutes, investigation documents, inspection reports, agency budgetary information, and procurement bids or proposals.

Remember, critical information can be unclassified or CUI that may reveal specifics about DOD activities, intentions, capabilities, or limitations.

We have just reviewed the first step of the OPSEC cycle - Identify Critical Information.

Let's review the next step in the OPSEC cycle.

Identify Threats

The next step of the OPSEC cycle is to Identify Threats. A threat is an adversary that has the capability and intent to take actions that would be detrimental to the success of DOD activities or operations.
Remember, an adversary is an individual, group, organization, or government that we want to deny critical information per the DOD Directive Operations Security, or OPSEC, Program.

Common examples of adversaries are sworn enemies, foreign governments, or terrorists; however, a threat can be anyone with the intent and capability to take actions detrimental to the success of DOD activities and operations.

Threat Analysis

The DOD needs to collect information on threats to develop appropriate countermeasures.

This is done by performing a threat analysis to identify potential adversaries and their associated capabilities and intentions.

Remember, adversaries seek to collect, analyze, and exploit critical information and indicators.

Programs and organizations should seek support from their security, intelligence, and counterintelligence experts to identify threats.

Consider the following questions:

- Who is an adversary?
- What are the adversaries' intentions?
- What is the adversary capable of doing?

How is Information Collected?

So how is information collected? Organizations or individuals who are threats as well as adversaries seek to exploit our vulnerabilities to collect our critical information.

Information is collected in several ways as discussed in the following examples.

- Observing our actions to detect patterns and predict behavior.
- Using the internet to collect data from social media sites, web pages, blogs, chat groups, and other web-based platforms.
- Intercepting our unsecured communications, such as work or personal phone calls and unencrypted e-mails.
- Using people to collect information by listening to our conversations in public and through social engineering.

- Sifting through our trash at work and at home.
- Tracking the geolocation of DOD personnel through their personal devices to. identify and collect patterns of life and any deviations from that pattern.

It is your responsibility to be aware of these threats and collection methods.

Analyze Vulnerabilities

We have just reviewed ways to identify critical information and threats. Let's review the next step of the OPSEC cycle - Analyze Vulnerabilities.

An OPSEC vulnerability exists when an adversary is capable of collecting critical information to exploit the DOD.

Organizations are required to conduct assessments, perform security exercises, analyze operations to help identify vulnerabilities.

Consider this: What weaknesses can an adversary exploit to uncover critical information?

Let’s dig a little deeper. What is a vulnerability? A vulnerability exists when an adversary is capable of collecting critical information or indicators, analyzing that information, and then acting quickly.

Remember, a vulnerability can occur when data can be derived from friendly detectable actions and open-source information.

Critical Information Indicators

Critical information indicators, in short, are clues that an adversary can interpret to uncover critical information. They often reveal small portions of information about a mission. They provide one piece of a larger puzzle.

If an adversary collects and interprets enough indicators, they could develop a relatively clear picture of the mission.

Consider the following examples of vulnerabilities that an adversary could collect.

- Forgetting to remove your ID badge when you leave your facility.
- Posting or sending sensitive information over the web such as family members’ locations during deployment.
- Discussing sensitive information in public or over the telephone such as agency operational procedures.
- Photos you take with your smartphones and upload to the Internet that have been geotagged.

- Using a device, application, or services with geolocation capabilities such as fitness trackers, smartphones, tablets, smartwatches, and related software applications.

Remember, each of these critical information indicators could provide the adversary one piece of a larger puzzle, so be mindful of your actions.

Assess Risks

The next step in the OPSEC cycle is to Assess Risks. This is a key element in the OPSEC process. Risk assessment involves identifying and evaluating the risks to critical information.

This risk is determined by answering the following questions:

- How susceptible is the information to collection?
- What is the anticipated severity of the information's loss?

At this step in the OPSEC cycle once the risks are assessed, it is important to determine if any countermeasures need to be assigned to vulnerabilities. The decision to assign a countermeasure is based on the level of risk determined.

How do you assess risks?

Risk equals threat multiplied by vulnerability multiplied by impact.

(Risk = Threat x Vulnerability x Impact)

An important goal of risk assessment is to assess an adversary's ability to exploit vulnerabilities that may expose critical information.

Remember, if an adversary effectively: collects, analyzes, and exploits critical information, it could have an impact on DOD operations or activities, putting the mission at risk!

Apply OPSEC Countermeasures

The next step in the OPSEC cycle is to apply OPSEC countermeasures.

After conducting a risk assessment, if the amount of risk is determined to be unacceptable, you should implement countermeasures to mitigate risk and establish an acceptable level.

Countermeasures should be coordinated and integrated within other core program areas whenever possible.

It is important to use a cost-benefit analysis to justify actions to mitigate risks and implement countermeasures.

What exactly are countermeasures? Countermeasures are events and actions designed to prevent adversaries from detecting DOD critical information. This can be accomplished by deceiving the adversary by providing an alternative interpretation of the critical information they attempt to collect or by denying the adversary's collection system.

How do you apply countermeasures?

Countermeasures are designed to prevent an adversary from detecting critical information. You should identify and implement actions to protect critical information during both working and non-working hours.

Remember to think before you act.

- Ask yourself, how can an adversary use this information against me?
- Know what your agency considers critical information.
- Safeguard all sensitive, unclassified, and controlled unclassified information.
- Understand OPSEC and data aggregation.
- Be aware of your surroundings.
- Use social media with caution by limiting the amount of personal information that you post.
- Photos you take with your smartphones and upload to the internet may have been geotagged - so consider disabling geolocation capabilities on your devices or applications.
- Information you share in emails, online, or during conversations on the phone or in public could be at risk.
- Do not discuss details, such as timelines, detailed locations, or movements; limitations or capabilities; specific names, ranks, or job titles; budgets or current or future operations; or security procedures.
- Keep in mind if you identify any possible vulnerability to your organization's mission, you have the responsibility to report it.

Contact your Agency Security Manager or OPSEC Manager Representative if you have any questions or need additional information on OPSEC.

Periodic Assessment

The DOD conducts Periodic Assessment of the effectiveness of its programs through continuous oversight, repetition, assessment of the OPSEC cycle.

Become familiar with the OPSEC cycle and be mindful of it at all times - whether you are working or not. Remember to stay up to date on your agency's policies and procedures, including the Critical Information List, or CIL.

Always practice self-awareness and educate your family to be aware of OPSEC concerns. Continue to conduct self-assessments of the practices your agency has put into place, and always remain vigilant.

Foreign Travel

Foreign Travel - Official

All DOD government personnel must provide advance notice of foreign travel, both official and unofficial, 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 your Security Office for specific travel procedures.

Prior to Travel, you must:

- 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 provided steps. In addition to items previously discussed, you must:

- Complete a foreign travel questionnaire prior to proceeding on travel.
- Provide a complete copy of your itinerary; flight, hotel, and planned sites to visit (included in the foreign travel questionnaire).
- Upon return from travel, personnel shall 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 incur certain risks associated with travel to, through, and within foreign countries. Hence why a defensive security briefing is so important. These briefs acquaint the traveler with risks involved in traveling to foreign countries and to furnish travelers guidance that may enable them to minimize those risks.

You are also required to complete a travel briefing and or report for personal travel. Be sure to follow component or agency guidance.

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