

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Course Introduction

Course Information

Purpose	Provide a thorough understanding of the Department of Defense (DoD) policy requirements for transmitting and transporting classified information
Audience	DoD civilian and military personnel responsible for the transmission and transportation of classified information
Pass/Fail %	75%
Estimated completion time	120 minutes

Course Overview

If you work with classified information, you are responsible for keeping it safe from accidental or intentional compromise. But classified information has little or no value unless you can share it with others who have a need to know. The responsibility for safeguarding classified information becomes especially important when you need to transfer it from one person or location to another. Several considerations come into play throughout the transmission and transportation process.

This course is about the factors you need to consider and the specific procedures you must follow in order to safeguard classified information that, if disclosed, could cause some level of damage to the national security of the United States.

Course Objectives

- Identify the policy documents that govern transmission and transportation of classified information
- Based on classification level; identify the authorized methods for transmission and transportation of classified information
- Identify the dissemination requirements for special types of information
- Identify the procedures to escort or hand-carry classified information

- Identify the procedures to prepare classified information for transmission and transportation

Course Structure

- Course Introduction
- Transmission and Transportation Basics
- Selecting an Authorized Transmission and Transportation Method
- Disseminating Special Types of Information
- Hand-carrying and Escorting Classified Information
- Preparing Materials for Transmission/Transportation
- Course Conclusion

Student **Guide**

Course: Transmission and Transportation for DoD

Lesson: Transmission and Transportation Basics

Lesson Introduction

Because protecting classified information from improper disclosure is so critical, there are specific policies and procedures governing how it can be transmitted or transported. These procedures apply to all phases of the transfer process, from the point of origin to the final destination. You must be familiar with these procedures and know where to look for guidance so you can successfully implement and execute them.

The lesson objectives are:

- Identify the sources of policy guidance for transmitting and transporting classified information
- Identify key issues to consider prior to transmitting or transporting classified information

Understanding Transmission and Transportation Procedures

1. Definitions

The terms transmission and transportation refer not only to the physical transfer of classified material from a sender to a recipient, but also to the transmission of classified information via connective methods, such as cable, or wire, as well as via non-connective methods – for example via radio, microwave, or laser.

Today's technological environment presents increasing challenges, as the material that is transported may also include portable computing devices and media. Classified materials are vulnerable to compromise while they are being transferred because they are not protected within an authorized storage container or location. They must be continuously protected to prevent unauthorized access. Vigilance and strict adherence to transmission and transportation policy are the keys to providing that protection.

2. Policy

Guidance on how to protect classified information during transmission and transportation ranges from national-level policy to command or activity level procedures.

At the national level, Executive Order 13526, Classified National Security Information, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information related to defense against transnational terrorism.

At the Department of Defense, or DoD, level, DoD Instruction 5200.01, DoD

Information Security Program and Protection of Sensitive Compartmented Information (SCI), and DoD Manual 5200.01, Volumes 1-4, DoD Information Security Program, provide implementing guidance, including requirements and minimum standards for transmitting and transporting classified information.

DoD 5220.22-M, National Industrial Security Program (NISPOM), provides implementing guidance, including requirements and minimum standards for transmitting and transporting classified information for contractors cleared under the National Industrial Security Program (NISP). For more information on contractor requirements concerning transmission and transportation of classified materials, please see CDSE course “Transmission and Transportation for Industry” (IS107.16).

DoD component heads are responsible for establishing *procedures* for transmitting and transporting classified material. These procedures should aim to minimize the risk of compromise, while promoting the most cost-effective method.

Depending on your situation, local command or activity level authorities may issue additional guidance.

These policies and procedures will cover many, but not all, circumstances. As you will see later in this course, some information may require enhanced protection, special handling, or dissemination controls.

In addition to the requirements prescribed by DoD *policy*, this course will also highlight some *best practices* for the transmission and transportation of classified information.

3. Process

The process of transmitting or transporting classified material has several phases.

First the sender of the information has to determine whether it is appropriate to transmit the materials at all. There are some important considerations you need to think about before you decide to send classified information. For example, is the intended recipient authorized to receive it and will the recipient be able to store it properly?

Then you need to make some advance preparations before the transmission. For example, you have to select which method you are authorized to use to transmit the information.

In addition, you will need to prepare the materials properly before they can be transported. Once the materials are on their way, there may be some special handling procedures you need to be aware of.

Finally, the recipient has certain responsibilities once the materials arrive at their destination.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

Transmission/transportation of classified materials is appropriate when:

- The sender has the authority to share the material
- The receiver has a legitimate need to know, clearance or access level, and appropriate secure storage for the level of material.

Here are some ways to ensure the receiver's ability to protect the classified information:

- To determine the storage capability at a **U.S. government facility**, contact the appropriate security official in advance.
- To determine the facility clearance and storage capability of a **contractor** facility:
 - Review contractor data in the Industrial Security Facilities Database (ISFD)
 - Contact the Defense Security Service (DSS) Field Office that oversees the recipient facility
 - Contact the recipient's Facility Security Officer (FSO) or security staff for large shipments

Review Activity

Try answering the following question. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Which of the following provides guidance for transmitting and transporting classified material within DoD? Select all that apply.

- DoDM 5200.01, DoD Information Security Program
- DoDI 5200.01, Information Security Program and Protection of Sensitive Compartmented Information (SCI)
- DoD 5220.22-M, The National Industrial Security Program Operating Manual (NISPOM)
- Component-level procedures

Question 2

Which of the following must you consider when deciding whether to transmit or transport classified material? Select all that apply.

- Whether you are authorized to share the material
- Whether the receiver has the appropriate level clearance
- Whether the receiver has a legitimate need to know
- Whether the receiver can store the material securely

Lesson Conclusion

In this lesson, you learned about the sources of policy guidance for transmitting and transporting classified material. You also learned about the overall transmission and transportation process, including issues you should consider when you are deciding whether to transmit or transport classified material.

Answer Key

Question 1

DoD Manual 5200.01, DoD Information Security Program and DoD Instruction 5200.01, Information Security Program, Protection of Sensitive Compartmented Information (SCI), and Component-level procedures provide implementation guidance for transmitting and transporting classified materials. DoD components are required to establish specific transmission and transportation procedures that minimize the risk of compromise, while promoting the most cost-effective manner

Question 2

Before you decide to transmit or transport classified materials, you must consider **whether you are authorized to share the material, the recipient has the appropriate level clearance, has a legitimate need to know, and can store the material securely.**

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Selecting an Authorized Transmission/Transportation Method

Lesson Introduction

When you have a need to transfer classified materials from one location to another, a variety of authorized methods are available to you. The method you choose should minimize the risk of compromising classified information, yet still be cost-effective.

This lesson will help you understand the factors you need to take into account when sending classified information, and how to decide what method to use.

The lesson objectives are:

- Identify the factors affecting the choice of authorized method for transmission/transportation of classified material
- Based on classification level, identify the authorized transmission/transportation methods
- Identify when the escorting or hand-carrying of classified information is authorized

Selecting an Authorized Method

1. Relevant Factors

Multiple factors affect the decision for choosing the transmission or transportation method most appropriate for a given situation. Consideration of these factors will help you manage risk when sending classified information.

The primary factor you need to consider when selecting a method is the classification level of the information you need to send. Classification level – that is, whether the information is Top Secret, Secret, or Confidential – is so important because it is based on the degree of damage to national security if the information was compromised. For this reason, you *must* select a transmission method that is authorized for the classification level of the material you are sending.

For each classification level, there are several authorized methods. Then, when you are trying to decide which of *those* methods to use, you can take the other factors into account to help narrow your choices. These include the nature of the information to be transmitted – that is, whether it is especially sensitive or is a special type of information. The size, weight, and type of material may also affect which transmission method is best. For example, although Secret materials are authorized to be sent via U.S. Postal Service Registered Mail, a large object might be too big or too heavy to be sent that way, so you will need to use a different authorized method.

Other factors you need to take into account are geographic considerations, time constraints, and whether there are any restrictions on disseminating the information.

If, after taking all of these risk management factors into account, there is still more than one appropriate authorized method of transmission, you should use the most cost-effective one.

2. Policy Guidance

DoD Manual 5200.01, Volume 3, Enclosure 4, DoD Information Security Program, defines the specific methods that are authorized for transmitting classified information based on its classification level. As you might expect, as the sensitivity of the information increases, there are fewer authorized methods you can use. This is because the more protection the information needs, the stricter the requirements for safeguarding it during transmission.

Methods authorized for sending Top Secret information are *always* authorized for sending information of a lesser classification level; specifically Secret or Confidential materials. Methods authorized for sending Secret information are *always* authorized for sending Confidential materials.

Now let's look in detail at the authorized methods by classification level for transmission and transportation of classified materials.

Authorized Methods by Classification Level

1. Top Secret Information

DoDM 5200.01 Volume 3, Enclosure 4, identifies six methods to transmit Top Secret information. These methods can be grouped into four categories: direct contact between cleared personnel, cryptographic systems, courier services, including Defense, DoD components and diplomatic, and designated couriers or escorts cleared for access to Top Secret information.

a. Direct Contact

When two or more cleared people have a discussion or meeting in which classified information is exchanged, that is a form of transmission.

Before you allow classified information to be transmitted in this way, you must consider the location, the people involved, and the information to be transmitted. The physical location should be appropriate for a Top Secret classified discussion. You should be able to control access to the location and the location should not have any prohibited electronic devices in it.

The people involved in the discussion should have clearances appropriate to the material to be discussed, and a valid need to know the information.

Finally, consider whether there are any special access requirements for the information to be discussed, such as a special access program or sensitive compartmented information.

As you consider these issues, you may need to make accommodations based on the number of participants in the meeting and your local command or activity guidance.

b. Cryptographic Systems

Electronic transmission of classified information has the advantage of providing secure, real-time delivery. To be authorized, electronic transmission of classified information must be processed through a cryptographic system authorized by the Director of the National Security Agency (DIRNSA) or a Protected Distribution System (PDS) designed and installed to meet the requirements of the Committee on National Security Systems Instruction (CNSSI) No. 7003.

This requirement applies to voice, data, message, and facsimile transmissions. Common cryptographic devices include the Secure Terminal Equipment, or STE secure telephones. These devices are also used as secure interfaces for fax machines when classified information is transmitted in this manner.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

Before using a secure telephone to transmit classified information, you must ensure:

- Classification level of discussion does not exceed classification level of the device
- Sender and receiver both have appropriate clearance and need to know for the information being transmitted
- Equipment is secure
- Ability exists to control access to physical location

Computers accredited or authorized to process classified information can also be used to transmit classified data. They use cryptographic data networks, such as the Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS). The JWICS is authorized for information up to the Top Secret, Sensitive Compartmented Information (SCI) level. The SIPRNET is authorized for information up to the Secret level. Telecommunication message traffic is also transmitted via a cryptographic system.

If you have any type of cryptographic equipment at your activity, a Communications Security (COMSEC) custodian has been appointed and can provide additional guidance. Your COMSEC custodian may also be a source for identifying emerging secure communications technology.

c. Courier Services

There are two large government courier services authorized to transmit Top Secret materials: the Defense Courier Service (DCS) and the Department of State Diplomatic Courier Service.

The Defense Courier Service (DCS) maintains and operates an international network of couriers and courier stations for the expeditious, cost-effective, and secure transmission of qualified classified documents and material. DCS transports classified material under the provisions of DoDI 5200.33, Defense Courier Operations. This regulation contains information about the DCS regarding establishing an account, material authorized for shipment, prohibited material, locations, and preparing material for shipment.

Prohibited Material: the following material is not authorized for entry into the Defense Courier Service (DCS) system, regardless of classification or other qualifying criteria:

- Contraband, including controlled substances (particularly narcotics and dangerous drugs), as defined in Section 812 of 21 U.S.C.
- Explosives, ammunition, firearms, and their components
- Radioactive material, etiological, or other material hazardous to personnel
- Flammables
- Liquids
- Batteries (prohibited from air shipments by the Federal Aviation Administration or international regulations), except as coordinated with the Commander, DCS, in advance
- Currency, military payment certificates, bonds, securities, precious metals, jewels
- Postage stamps or other negotiable instruments

The Department of State Diplomatic Courier Service provides regularly scheduled classified deliveries to Foreign Service missions via commercial aircraft. It also provides special State Department military support flights to transport heavy, oversize pouch material.

The DCS and the Department of State Diplomatic Courier Service have a reciprocal agreement. The DCS coordinates the use of the State Department service when the DCS does not provide services for a particular geographical area.

DoD personnel assigned to U.S. embassies and consulates should follow Department of State Diplomatic Courier Service procedures for transmitting and transporting classified materials. In addition to these two international courier services, DoD activities may establish local or regional courier services for the transmission and transportation of classified information.

d. Designated Hand-carrier/Escort

Cleared U.S. military and civilian employees may transmit or transport classified material from one location to another via a courier or an escort. When authorized, defense contractors may also transmit or transport classified information and should follow the guidance in the National Industrial Security Program Operating Manual (NISPOM). Further training on this topic is offered in the CDSE Transmission and Transportation for Industry eLearning Course.

Couriers carry small, classified items and escorts accompany larger shipments of classified materials. Since hand-carrying and escorting could pose an unacceptable risk of compromise, they are authorized only when the classified information is not available at the destination and is required by operational necessity or a contractual requirement, when information cannot be sent via a secure facsimile or by other secure means, and when arrangements have been made for secure storage of the material at a U.S. Government or cleared U.S. contractor facility. In addition, couriers and escorts must meet requirements about location, mode of transportation, and authorization to transport.

Who may be couriers/escorts?

- U.S. military personnel
- Government civilian employees
- DoD contractors (guidance under the NISPOM)

What **mode of transport** may they use?

Surface	Owned, controlled, or chartered by the U.S. Government or DoD contractors
Air	Scheduled commercial passenger aircraft, or foreign carrier if no U.S. carrier is available. The information is to remain in the custody and physical control of the U.S. escort at all times.

Where may they courier/escort classified materials?

U.S. military, Government civilians	Anywhere in the world
DoD contractors	Within and between the U.S. and its Territories

What **authorization** is required?

U.S. military, Government civilians	Cleared, with written authorization by issuance of DD Form 2501 or Authorization Letter
DoD contractors	Cleared, with written authorization from the appropriate <u>Cognizant Security Agency (CSA)</u>

2. Secret Information

All of the methods you just learned about for sending Top Secret materials can also be used to transmit Secret materials. Note however, unlike Top Secret materials, cleared contractor employees may act as a courier for Secret material transmitted outside the United States or its territories provided it is authorized under a classified contract or by the Government Contracting Activity (GCA).

DoD Manual 5200.01 identifies seven additional methods that can be used to transmit Secret information. These methods can be grouped into five categories. You can use some U.S. and Canadian mail services to transmit Secret material. You can transmit Secret materials via a commercial carrier, or a General Services Administration, or GSA-approved overnight delivery company. You can use government-owned and government-contract vehicles, aircraft, and ships to transport Secret materials and in exceptional circumstances, you can use a cleared Civilian Reserve Air Fleet participant.

a. Mail

The United States Postal Service (USPS) offers two services that you may use for transmission of Secret material: Priority Mail Express and Registered Mail.

Priority Mail Express is the fastest USPS service for delivery of time-sensitive material. Within the DoD, use of Priority Mail Express is authorized for transmission of Secret material *only* within the fifty states, the District of Columbia, and the Commonwealth of Puerto Rico.

It is important to note that the Priority Mail Express label requires that you actually check the "signature is required" box.

USPS Registered Mail is the most secure service that USPS offers. Material shipped by this method remains under lock and key until delivered by the carrier, whereas Priority Mail Express is not.

When purchased, both offer a system of receipts, to monitor the movement of mail from the point of acceptance to delivery. They provide the sender with a mailing receipt, allow for verification of delivery or delivery attempts, and are tracked at each delivery point.

Remember, however, the Priority Mail Express receipt system can only validate that the package was physically received. It does not ensure the material inside reached the intended recipient and was properly safeguarded.

For U.S. Registered mail, however, the package must be delivered to the addressee direct. Registered Mail service is available within the 50 states, the District of Columbia, and the Commonwealth of Puerto Rico. Army Post Office, or APO, and Fleet Post Office, or FPO, locations worldwide are also serviced by USPS Registered Mail, although users must verify the mail remains under U.S. control. Canadian Registered Mail with Registered Mail receipt may be used only between U.S. Government and Canadian government installations in the U.S. and Canada.

Procedures for using USPS Priority Mail Express:

- *NEVER* execute Block 11-B of label (Waiver of Signature and Indemnity)
- A cleared employee must give the parcel directly to USPS personnel (use of street-side boxes is prohibited)
- To bring your parcel back under government control in a timely manner, it is recommended to transmit the material on a day that will ensure the recipient will be available for receipt on the following day.
- CHECK the "signature is required" box

b. Commercial Carrier

Commercial carriers may be used for delivery of Secret bulk material if they meet certain conditions.

The commercial carrier must be cleared under the National Industrial Security Program (NISP) and provide a protective security service (PSS).

National Industrial Security Program (NISP): A partnership between the federal government and private industry to safeguard classified information. The NISP was established by Executive Order 12829 to achieve cost savings and protect classified information held by contractors, licensees, and grantees of the United States Government. The Order was signed by President Bush in January of 1993.

Redundant, overlapping, or unnecessary requirements impede the technological and economic interests of the U.S Government. Executive Order 12829 calls for a single, integrated, cohesive system for safeguarding classified information held by industry.

Consistent with the goal of achieving greater uniformity in security requirements for classified contracts, the four major tenets of the NISP are:

- Achieving uniformity in security procedures.
- Implementing the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances.
- Eliminating duplicative or unnecessary requirements, particularly agency inspections.
- Achieving reductions in security costs.

The NISP affects all executive branch agencies. The major signatories to the program are the:

- Department of Energy
- U.S. Nuclear Regulatory Commission
- Department of Defense
- Director of National Intelligence
- Director of Homeland Security

Protective Security Service: A transportation protective service provided by a commercial carrier qualified by the Surface Deployment and Distribution Command (SDDC) to transport Secret shipments.

General requirements:

- Carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives
- Carrier must maintain a signature and tally record

Air movement requirements:

- If shipment *IS NOT* accessible to an unauthorized person, observation is not required
- If the shipment *IS* accessible to an unauthorized person, it must remain under the constant surveillance of a cleared escort or qualified carrier representative

Using a commercial carrier is authorized only within the continental United States (CONUS) when other methods are impractical. This method is also authorized between U.S. and Canadian government-approved locations documented in a transportation plan. The plan must be approved by U.S. and Canadian government security authorities.

You must coordinate the use of commercial carriers through your local transportation, supply, or logistics department.

c. GSA-Approved Delivery Company

When you must deliver Secret material overnight to a DoD component within the U.S. and its territories, you may use one of the companies with a General Services Administration (GSA) contract for overnight delivery.

You can access a list of the companies currently approved by GSA for domestic express delivery services through the GSA website. The companies on this list meet the criteria for overnight domestic transmission of Secret information as prescribed in 32 CFR Parts 2001 and 2003 Classified National Security Information; Final Rule. They are U.S. owned and operated, provide automated in-transit tracking, and ensure package integrity during transit.

If you wish to use the companies identified on the GSA Schedule, you must follow specific procedures.

Procedures for Using a GSA-Approved Overnight Delivery Service:

- Verify the correct mailing address
- Ensure that an authorized person will be available to receive the delivery
- *NEVER* execute the release signature block on the receipt label
- *NEVER* use an external (street-side) collection box
- Classified COMSEC, NATO, foreign government information (FGI), and other special types of information may not be authorized for transmission this way
- To facilitate delivery, the service may require a street address, the recipient's name, and a telephone number
- To bring your parcel back under government control in a timely manner, it is recommended to transmit the material on a day that will ensure the recipient will be available for receipt on the following day.

d. Government-Owned or Government-Contract Vehicle

You may use Government-owned and Government-contract vehicles, including aircraft, U.S. Naval ships, civil service-operated U.S. Naval ships, and ships of U.S. registry, to transmit Secret information.

A vehicle operator, ship officer, or aircraft pilot may be designated as an escort provided he or she is an appropriately cleared U.S. citizen, and control of the carrier is maintained on a 24-hour basis. Escorts must protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, as long as the shipment is loaded into a specialized secure, safe-like container or a compartment that is not accessible to unauthorized persons.

e. Civilian Reserve Air Fleet

In exceptional circumstances, with the written approval of the recipient government security authorities, you may transmit Secret material outside of the U.S. and its Territories in the hold of a cleared U.S. registered air carrier without an appropriately cleared escort. These carriers are participants in the Civilian Reserve Air Fleet.

The shipment must be sent between two specified points with no intermediate stops. The carrier must agree in advance to permit cleared and specifically authorized persons to observe placement and removal of the classified shipment from the air carrier. The shipment must be placed in a compartment that is not accessible to any unauthorized person, or in the same type of specialized shipping container used by the DCS.

Activity 1

Which of the following are authorized methods for transmitting Secret material? Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- USPS Registered Mail
- Courier
- USPS Priority Mail Express
- USPS Certified Mail
- Commercial carrier that provides Protective Security Service (PSS)
- Secure telephone
- Commercial carrier that provides Constant Surveillance Service (CSS)

3. Confidential Information

All of the methods you have learned about for sending Top Secret and Secret materials can also be used to transmit Confidential materials.

DoDM 5200.01 identifies five additional methods that can be used to transmit Confidential information. In some cases, you may send Confidential information via USPS Certified or First Class mail delivery. You also may use a commercial carrier that provides a constant surveillance service to transmit bulky Confidential material, or you may transmit Confidential cargo via ships of U.S. registry with U.S. citizen operators, such as commanders or masters of ships. Finally, with the approval by the Head of the DoD Component, alternative or additional transmission methods for Confidential material may be available to you.

a. USPS Mail

There are two methods by which Confidential information may be transmitted via the USPS.

USPS Certified Mail is an authorized method for sending Confidential information to DoD contractors or non-DoD agencies *within* the U.S. and its Territories. Certified mail provides proof of mailing to the sender at the time of mailing. It provides tracking of the package en route, and the recipient's post office maintains a record of delivery.

USPS First Class Mail may be used for Confidential information between DoD Component locations anywhere in the U.S. and its Territories. Confidential information being transmitted in this manner must also contain the following statement on the outer wrapper: "Return Service Requested".

b. Commercial Carrier

To send Confidential bulk material via commercial freight carrier, a facility security clearance is not required. Rather, as long as the commercial freight carrier can provide a constant surveillance service (CSS) you may use it to send Confidential material within the continental United States. A qualified carrier representative must provide constant surveillance of the shipment at all times. However, a facility clearance is not required for the carrier.

Constant Surveillance Service (CSS): A transportation protective service provided by a commercial carrier qualified to transport Confidential shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, a facility clearance (FCL) is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

c. U.S. Citizen Operators of U.S. Registered Ships

Confidential material may be transmitted in the custody of commanders or masters of ships of U.S. registry who are U.S. citizens. The Confidential cargo on U.S. registered ships may not pass out of U.S. Government control. The ship commander or master must sign a receipt for the material and agree to deny access to the Confidential material by unauthorized persons. This includes customs inspectors with the understanding that the Confidential cargo that would be subject to customs inspection will *not* be unloaded. Ship commanders also agree to maintain control of the cargo until a receipt is obtained from an authorized representative of the person to whom the material is being shipped.

Activity 2

For each transmission/transportation method listed, select the classification level(s) for which it is authorized. Check your answers in the Answer Key at the end of this Student Guide.

	Top Secret	Secret	Confidential
USPS Certified Mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Defense Courier Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
USPS Registered Mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Commercial carrier that provides CSS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Escort	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Government-owned and government-contract vehicles, aircraft, and ships	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Job Aid

Take a moment to review this table, which summarizes the authorized transmission and transportation methods by classification level for the Department of Defense.

Transmission Method	Classification Level		
	Top Secret	Secret	Confidential
Direct Contact	X	X	X
Cryptographic Systems	X	X	X
Defense Courier Service	X	X	X
DoD Component Courier Service	X	X	X
Department of State Courier Service	X	X	X
Cleared Designated Courier/Escort	X	X	X
USPS Registered Mail		X	X
USPS Priority Mail Express		X	X
Canadian Registered Mail		X	X
GSA-Approved Overnight Delivery Company		X	X
Commercial Carrier that provides PSS		X	X
Government-owned and Government-Contract Vehicles, Aircraft & Ships		X	X
Civilian Reserve Air Fleet		X	X
USPS Certified Mail			X
USPS First Class Mail			X
Commercial Carrier that provides CSS			X
U.S. Citizen Operators of U.S. Registered Ships			X
Alternative/Additional Methods Approved by Head of DoD Component			X

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
All methods authorized to send Secret information may also be used to transmit Top Secret information.	<input type="radio"/>	<input type="radio"/>
The classification level of information is the primary factor that determines the method for sending it.	<input type="radio"/>	<input type="radio"/>
The urgency of the need for classified information may affect the transmission method.	<input type="radio"/>	<input type="radio"/>
All methods authorized to send Secret information may also be used to transmit Confidential information.	<input type="radio"/>	<input type="radio"/>

Question 2

You are required to transmit Top Secret information to another DoD Component.

For each method listed, identify whether it is appropriate. Check your answers in the Answer Key at the end of this Student Guide.

	Yes	No	Maybe
USPS Priority Mail Express	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Designated courier or escort	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure fax	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Commercial carrier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 3

You have wrapped a package containing hardware classified Secret. The package measures 2" x 4" x 14" and weighs 5 pounds. The material must arrive at another DoD Component destination within 24 hours. You are located within the United States, and the destination of the package is also within the United States.

For each method listed, identify whether it is appropriate. Check your answers in the Answer Key at the end of this Student Guide.

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Registered Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Priority Mail Express	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
GSA Contract Holders for Overnight Delivery	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 4

You are tasked to transmit a legal-size envelope containing a Confidential memorandum. Your Component facility is located within the United States and the destination is the cleared facility of the prime contractor with which you have a classified contract.

For each method listed, identify whether it is appropriate. Check your answers in the Answer Key at the end of this Student Guide.

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Certified Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Commercial Carrier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Overnight Domestic Express Delivery	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 5

Your facility is within Washington, DC and you have a contractual requirement to expedite the delivery of 25 copies of a 100-page Secret document to the office via offices of your prime contractor within the same geographical area. The information is urgently required for a high-level briefing by 10:00am the next day, and the information must be ready for immediate dissemination to attendees.

For each method listed, identify whether it is appropriate. Check your answers in the Answer Key at the end of this Student Guide.

	Yes	No	Maybe
Defense Courier Service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cryptographic secure communications system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hand-carry by cleared U.S. military, civilian employee, or contractor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Certified Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 6

A cleared employee at your facility has wrapped a package containing hardware classified Secret. The package measures 14" x 16" x 16", and weighs 72 pounds. To meet a contractual requirement, you must transmit the material to arrive at its destination within 24 hours. You are located within the United States, and the destination of the package is also within the United States.

For each method listed, identify whether it is appropriate. Check your answers in the Answer Key at the end of this Student Guide.

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Registered Mail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Priority Mail Express	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
GSA Contract Holders for Overnight Delivery	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Lesson Conclusion

In this lesson, you learned about how to select an authorized method for transmitting or transporting classified materials, and where to find guidance for doing so. You learned about the risk management factors that you must take into account in making that decision, the most important of which is classification level. Finally, you learned which methods are authorized for sending Top Secret, Secret, and Confidential information.

Answer Key

Activity 1

Authorized methods for transmitting Secret material are **USPS Registered Mail, courier, USPS Priority Mail Express, Commercial carrier, and secure telephone.**

Activity 2

	Top Secret	Secret	Confidential
USPS Certified Mail	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Defense Courier Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
USPS Registered Mail	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Commercial carrier that provides CSS	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Escort	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Government-owned and government-contract vehicles, aircraft, and ships	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Review Activity

Question 1

	True	False
All methods authorized to send Secret information may also be used to transmit Top Secret information.	<input type="radio"/>	<input checked="" type="radio"/>
The classification level of information is the primary factor that determines the method for sending it.	<input checked="" type="radio"/>	<input type="radio"/>
The urgency of the need for classified information may affect the transmission method.	<input checked="" type="radio"/>	<input type="radio"/>
All methods authorized to send Secret information may also be used to transmit Confidential information.	<input checked="" type="radio"/>	<input type="radio"/>

Question 2

	Yes	No	Maybe
USPS Priority Mail Express	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Designated courier or escort	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure fax	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Commercial carrier	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Question 3

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
USPS Registered Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
USPS Priority Mail Express	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
GSA Contract Holders for Overnight Delivery	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Question 4

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
USPS Certified Mail	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Commercial Carrier	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Overnight Domestic Express Delivery	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Question 5

	Yes	No	Maybe
Defense Courier Service	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cryptographic secure communications system	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Hand-carry by cleared U.S. military, civilian employee, or contractor	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
USPS Certified Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Question 6

	Yes	No	Maybe
USPS First Class Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
USPS Registered Mail	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
USPS Priority Mail Express	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
GSA Contract Holders for Overnight Delivery	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Dissemination of Special Types of Information

Lesson Introduction

In addition to the basic requirements for the transmission and transportation of classified information based on its classification level, there are additional, special dissemination requirements for certain types of information. It is important to be aware of these types of information and their associated special requirements.

The lesson objectives are:

- Describe Dissemination Requirements Outside the DoD
- List the special types of information with dissemination controls prior to transmission and transportation
- Identify the sources of guidance for the transmission and transportation of special types of information

Information Types and Guidance

Overview of Special Types of Information

There are several types of special information you need to be aware of. These types of special information include:

- Communications Security (COMSEC) Information
- Sensitive Compartmented Information (SCI)
- Special Access Program (SAP) Information
- International Program Information

The nature of certain types of information requires enhanced protection, special handling restrictions, or limitations on how it can be disseminated. In all cases, a designated official is required for coordination and authorization before disseminating this information.

Dissemination Requirements Outside the DoD

Suppose a person from the State Department is working on a joint project with you and he provides you with a classified source document for the project. Further, suppose someone in the Treasury Department asks you for some data in that report. What should you do?

Classified information originating in another DoD Component or in a department or agency other than the Department of Defense may be disseminated to other DoD Components, to other U.S. departments or agencies, or to a U.S. entity without the consent of the originating Component, department, or agency, as long as the recipient possesses the appropriate clearance eligibility, a signed Nondisclosure Agreement (NDA), and has a need to know. There are exceptions to this, however. For example, consent of the Original Classification Authority (OCA) is required for documents created

prior to June 27, 2010 or that are derived from source document(s) dated prior to June 27, 2010. For more information on these exceptions, please see DoDM 5200.01, Vol. 3, Enclosure 4, Section 2.

Now let's look at the dissemination requirements for special types of information.

1. COMSEC

COMSEC is a program designed to deny unauthorized individuals information of value they might derive from possessing or studying telecommunications, and to ensure such communications are authentic. COMSEC includes crypto security, emission security, transmission security, and physical security of COMSEC material and information.

Transmission of COMSEC information must be approved by a designated COMSEC custodian. The Committee on National Security Systems Instruction (CNSSI) No. 4001, Controlled Cryptographic Items is a Controlled Unclassified Information (CUI) instruction that further amplifies DoD Manual 5200.01, DoD Information Security Program, Volume 3, procedures for transmission of classified and unclassified COMSEC material. COMSEC custodians must follow CNSSI 4001 for protecting, safeguarding, transmitting, and marking COMSEC information.

2. Sensitive Compartmented Information (SCI)

SCI is classified information handled within formal access control systems established by the Director of National Intelligence (DNI). Transmission and transportation of SCI must be approved by the local SCI security official. This official can be the Special Security Officer (SSO) the Special Security Representative (SSR), or another designated individual. These officials follow the procedures prescribed by DoD Manual 5105.21, Volumes 1-3, Sensitive Compartmented Information Administrative Security Manual, for the protection, safeguarding, transmission, and marking of SCI.

3. Special Access Program (SAP) Information

SAPs are established for specific types of classified information having safeguarding and access requirements exceeding those normally required for information at the same classification level. SAPs are established only when the program is required by statute; or when there is a specific finding that the vulnerability of, or threat to, specific information is exceptional; *and* the normal criteria for determining access to information classified at the same level are insufficient.

Dissemination of SAP information is *always* coordinated through the Program Security Officer (PSO) or by the guidance provided in the Program Security Guide (PSG) prior to its transmission outside a SAP facility.

SAPs are governed by policies and procedures found in Section 119, Title 10 (USC), Special Access Programs: Congressional Oversight, Executive Order 13526, Classified National Security Information, DoDM 5205.07, Volumes 1-4, DoD Special Access Program (SAP) Security Manual, and other applicable DoD policies and regulations.

U.S. Code, Title 10, Section 119	Special Access Programs: Congressional Oversight
Executive Order 13526	Classified National Security Information
DoD Manual 5200.01	DoD Information Security Program
DoD Directive 5205.07	Special Access Program (SAP) Policy
DoD Instruction 5205.11	Management, Administration, and Oversight of DoD Special Access Programs (SAPs)
DoD Manual 5205.07	DoD Special Access Program (SAP) Security Manual

International Programs Information

1. Policy

As international cooperation becomes an increasing part of our everyday life, providing high-quality security for sensitive information and technologies is a real and growing challenge.

The issues involved in the security management of international programs are often difficult and subtle. The potential consequences for our national security are significant, and the laws and policy documents that establish the requirements are many and complex. The risk of this information being exploited and falling into the wrong hands must be taken into consideration. DoD officials must understand how to protect sensitive information and technologies, while at the same time providing support to international programs.

Legal and national policy for security in most DoD international programs is derived from the Arms Export Control Act (AECA), Executive Order 13526 and the National Security Decision Memorandum (NSDM) 119.

Security Assistance is a group of programs (including Foreign Military Sales) authorized by law, that allows the transfer of military articles and services to friendly foreign governments. Security Assistance programs must follow the same DoD policies concerning the disclosure of classified and controlled unclassified information as other international programs.

Based on these documents, the DoD has issued implementing guidance in DoD Directives.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

International program security incorporates these policies for safeguarding information and technology requiring controls when generated by, provided to, or transferred in an international program. This includes the export and disclosure decision as well as any security arrangements.

National Policy	Arms Export Control Act (AECA)	
	Executive Order 13526, Classified National Security Information	
	National Security Decision Memorandum (NSDM) 119	
Security Assistance Programs	Foreign Assistance Act (FAA) of 1961, as amended	
	Executive Order 11958, Administration of Arms Export Controls	
	DoD Directive 5105.65	Defense Security Cooperation Agency (DSCA)
	DoD 5105.38-M	Security Assistance Management Manual (SAMM)
DoD Implementing Guidance	DoDD 5100.55	United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)
	DoDD 5230.11	Disclosure of Classified Military Information to Foreign Governments and International Organizations
	DoDD 5230.20	Visits and Assignments of Foreign Representatives
	DoDD 5530.3	International Agreements

2. Types

International programs require sharing technology, classified military information (CMI), and controlled unclassified information (CUI) with allies and other friendly countries. Now let's look in more detail at three types of international transfers of sensitive or classified information.

a. U.S. Classified Information

An official who has been specifically delegated as the disclosure authority for a component or command may authorize disclosures of classified military information to foreign governments.

U.S. classified information may be shared with foreign governments only when there is a clearly defined benefit to the U.S. and there is a demonstrated intent and capability on the part of the prospective foreign recipient to safeguard the information. All international transfers must take place through government-to-government channels or channels agreed upon by the governments involved with the transfer.

DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, stipulates the means for ensuring proper transfer and the roles and responsibilities of the delegated disclosure authority.

DoD Manual 5200.01, Information Security Program, identifies the procedures and methods for transmitting and transporting classified information to foreign governments.

b. Foreign Government Information

Foreign Government Information (FGI) is information the U.S. *receives* from a foreign government or international organization. FGI may be classified or unclassified.

In addition to Top Secret, Secret, and Confidential, many foreign governments have a fourth level of security classification called Restricted, for which there is no U.S. equivalent. Some governments also have unclassified information protected by law or national regulations that is treated, and provided to other governments, as “in confidence” information.

DoD Manual 5200.01, DoD Information Security Program, provides basic guidance for FGI. However, the responsible national security authority of the originating government may alter the control and safeguarding requirements of FGI through treaties or international agreements. Bilateral and multinational security and program agreements ensure that FGI receives protection *equivalent to* that provided by the originating government or international organization. This protection is also accomplished through the NATO security agreement and U.S. national policy. The U.S. applies separate security procedures to protect FGI, using NATO standards as the baseline for U.S. procedures.

Procedures and methods for transmission and transportation of FGI must be coordinated with the Designated Security Authorities and Cognizant Security Office of the countries involved. To transfer FGI within the U.S. and its territories, use the same channels as for U.S. classified information of an equivalent classification, with one important exception. Never use express commercial carriers.

As a general rule, receipts are required for *all* international transfers of classified and Foreign Government Information, wherever they occur, although exceptions are made for Restricted information. There are no receipts for CUI. Commonly known as the “third-country transfer,”

the release or disclosure of FGI to any third-country requires the prior written consent of the originating government.

c. NATO Classified Information

As a member of NATO, the U.S. has agreed to protect NATO classified information in accordance with the mandatory security principles, standards, and procedures in NATO security policy documents. The NATO Security Policy is referred to as C-M (2002)49, Security within the North Atlantic Treaty Organization.

United States Security Authority for NATO Affairs (USSAN) Instruction 1-07, Implementation of NATO Security Requirements, describes the policy for transmitting and transporting NATO classified information. This instruction is available from your NATO representative.

Individuals requiring access to NATO classified information must receive a security briefing on how to protect it and must complete a statement acknowledging receipt of the briefing. Before sending out NATO classified information, you must ensure the recipients are authorized to receive it. Classified NATO information can be transmitted *only* through government-to-government channels unless both the sending *and* receiving governments agree in writing to an alternative.

Finally, you need to make sure that the markings on NATO classification information ensure it receives the degree of protection that the originator of the information requires.

Job Aid

Take a moment to review this table. This is a summary of the types of information, key contacts, and guidance for dissemination.

Types of Information with Special Controls on Dissemination	Key Contact for Transmission / Transportation	Key Guidance Documentation
Communications Security (COMSEC)	COMSEC Custodian	<ul style="list-style-type: none"> • CNSSI No. 4001: Controlled Cryptographic Items • DoDM 5200.01, DoD Information Security Program
Sensitive Compartmented Information (SCI)	SSO, SSR, or other designated individual	<ul style="list-style-type: none"> • DoDM 5105.21, Sensitive Compartmented Information Administrative Security Manual
Special Access Program (SAP)	PSO	<ul style="list-style-type: none"> • Program Security Guide • DoDM 5205.07, DoD Special Access Program (SAP) Security Manual
International Programs		<p>National Policy:</p> <ul style="list-style-type: none"> • Arms Export Control Act (AECA) • Executive Order 13526 • National Security Decision Memorandum (NSDM) 119 <p>Security Assistance Programs:</p> <ul style="list-style-type: none"> • Foreign Assistance Act (FAA) of 1961, as amended • Executive Order 11958 • DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA), DoD 5105.38-M, Security Assistance Management Manual (SAMM) <p>DoD Implementing Policy:</p> <ul style="list-style-type: none"> • DoDD 5230.20: Visits and Assignments of Foreign Representatives • DoDD 5530.3 International Agreements

Types of Information with Special Controls on Dissemination	Key Contact for Transmission / Transportation	Key Guidance Documentation
<ul style="list-style-type: none"> U.S. Classified Information 	Designated Authority	<ul style="list-style-type: none"> DoDM 5200.01, DoD Information Security Program
<ul style="list-style-type: none"> U.S. Classified Military Information 		<ul style="list-style-type: none"> DoDD 5230.11: Disclosure of Classified Military Information to Foreign Governments and International Organizations
<ul style="list-style-type: none"> Foreign Government Information (FGI) 	<ul style="list-style-type: none"> Designated Security Authorities Cognizant Security Office 	<ul style="list-style-type: none"> DoDM 5200.01, DoD Information Security Program
<ul style="list-style-type: none"> NATO Classified Information 	Designated Authority	<ul style="list-style-type: none"> USSAN Instruction 1-07: Implementation of NATO Security Requirements DoDD 5100.55: United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

What is the DoD policy requirement for disseminating classified information from another Department or Agency in the U.S. Government? Select the best answer.

- You must comply with the COMSEC procedures in Committee on National Security Systems Instruction (CNSSI) No. 4001.
- You must have the approval of your supervisor and comply with CNSSI No. 4001.
- You may share information with other agencies outside of DoD without additional approval unless the document was created before June 27, 2010 or otherwise stated.
- You must comply with procedures in the National Security Decision Memorandum 119.

Question 2

Can you list the types of information that have special dissemination requirements?
Write your answer here.

Question 3

For each information type, do standard transmission and transportation procedures apply or are there additional special procedures?

	Standard Procedures	Special Procedures
Sensitive Compartmented Information	<input type="radio"/>	<input type="radio"/>
Unclassified COMSEC materials	<input type="radio"/>	<input type="radio"/>
Top Secret aircraft capabilities data shared with a DoD contractor	<input type="radio"/>	<input type="radio"/>
NATO Classified Information	<input type="radio"/>	<input type="radio"/>
Foreign Government Information (CMI and CUI)	<input type="radio"/>	<input type="radio"/>

Question 4

- a.** You need to ship a package that contains foreign government information (FGI). Which of the following source(s) of guidance should you consult to make sure you follow appropriate transmission and transportation procedures?

- (SSO) or (SSR)
- Designated Authority
- COMSEC Custodian
- Designated Security Authorities/Cognizant Security Office
- DoDM 5200.01
- CNSSI No. 4001
- DoDM 5105.21
- PSG and DoDM 5205.07
- DoDD 5230.11

- b.** You need to ship a package that contains sensitive compartmented information (SCI). Which of the following source(s) of guidance should you consult to make sure you follow appropriate transmission and transportation procedures?

- Special Security Officer (SSO), or Special Security Representative (SSR)
- Designated Authority
- COMSEC Custodian
- Designated Security Authorities/Cognizant Security Office
- DoDM 5200.01
- CNSSI No. 4001
- DoDM 5105.21
- PSG and DoDM 5205.07
- DoDD 5230.11

- c. You need to ship a package that contains COMSEC materials. Which of the following source(s) of guidance should you consult to make sure you follow appropriate transmission and transportation procedures?
- (SSO) or (SSR)
 - Designated Authority
 - COMSEC Custodian
 - Designated Security Authorities/Cognizant Security Office
 - DoDM 5200.01
 - CNSSI No. 4001
 - DoDM 5105.21
 - PSG and DoDM 5205.07
 - DoDD 5230.11
- d. You need to ship a package that contains U.S. classified military information (CMI) to Japan. Which of the following source(s) of guidance should you consult to make sure you follow appropriate transmission and transportation procedures?
- (SSO) or (SSR)
 - Designated Authority
 - COMSEC Custodian
 - Designated Security Authorities/Cognizant Security Office
 - DoDM 5200.01
 - CNSSI No. 4001
 - DoDM 5105.21
 - PSG and DoDM 5205.07
 - DoDD 5230.11
- e. You need to ship a package that contains Special Access Program (SAP) information. Which of the following source(s) of guidance should you consult to make sure you follow appropriate transmission and transportation procedures?
- (SSO) or (SSR)
 - Designated Authority
 - COMSEC Custodian
 - Designated Security Authorities/Cognizant Security Office
 - DoDM 5200.01
 - CNSSI No. 4001
 - DoDM 5105.21
 - PSG and DoDM 5205.07
 - DoDD 5230.11

Lesson Conclusion

In this lesson, you learned about some special types of information that have additional protection requirements. All of these require coordination and authorization by a designated official prior to dissemination. You also learned about some of the documents that define the procedures for the transmission and transportation of these kinds of information.

Answer Key

Question 1

The DoD policy requirement for disseminating classified information from another Department or Agency in the U.S. government states that **you may share information with other entities outside of DoD without prior consent of the Original Classification Authority (OCA) unless the document was created before June 27, 2010 or otherwise stated on the document or SCG.**

Question 2

All of the following types of information have special controls on dissemination.

- Communications Security (COMSEC)
- Sensitive Compartmented Information (SCI)
- Special Access Program (SAP)
- International Programs
 - U.S. Classified Military Information (CMI)
 - Foreign Government Information (FGI)
 - Classified
 - Controlled Unclassified Information (CUI)
 - NATO Classified Information

Make sure you understand what each type is, so you can recognize when to look for additional guidance on its transmission and transportation.

Question 3

	Standard Procedures	Special Procedures
Sensitive Compartmented Information	<input type="radio"/>	<input checked="" type="radio"/>
Unclassified COMSEC materials	<input type="radio"/>	<input checked="" type="radio"/>
Top Secret aircraft capabilities data shared with a DoD contractor	<input checked="" type="radio"/>	<input type="radio"/>
NATO Classified Information	<input type="radio"/>	<input checked="" type="radio"/>
Foreign Government Information (CMI and CUI)	<input type="radio"/>	<input checked="" type="radio"/>

Question 4

- a. Before shipping foreign government information (FGI) you should consult the **Designated Security Authorities/Cognizant Security Office** and **DoDM 5200.01** to make sure you follow appropriate transmission and transportation procedures.
- b. Before shipping SCI you should consult the **SSO or SSR, the Designated Authority**, and **DoDM 5105.21** to make sure you follow appropriate transmission and transportation procedures.

- c.** Before shipping COMSEC materials you should consult **COMSEC Custodian, CNSSI No. 4001**, and **DoDM 5200.01** to make sure you follow appropriate transmission and transportation procedures.
- d.** Before shipping U.S. CMI for Japan you should consult the **Designated Authority, DoDD 5230.11**, and **DoDM 5200.01** to make sure you follow appropriate transmission and transportation procedures.
- e.** Before shipping SAP information, you should consult the **PSO, PSG, DoDM 5205.07** to make sure you follow appropriate transmission and transportation procedures.

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Procedures for Escorting or Hand-carrying Classified Information

Lesson Introduction

When classified materials must be transported by courier from one location to another, special procedures are required to ensure the security of the information. DoD Manual 5200.01, Volume 3, DoD Information Security Program, includes requirements for escorting or hand-carrying classified materials.

In this lesson, you will learn what the requirements are for authorized couriers of classified materials. You will learn what must be included in a courier briefing so that individuals understand and acknowledge their security responsibilities. You will also learn what documents are required and what additional procedures are needed when traveling aboard a commercial passenger aircraft.

The lesson objectives are:

- Identify who can escort or hand-carry classified materials
- Identify the requirements for escorting or hand-carrying classified materials
- Identify the required contents of a courier briefing

Authorized Individuals

1. Who is Authorized?

When the decision has been made that transporting classified materials requires hand-carrying or escorting, who is authorized to perform the task?

An authorized person is an individual who has a favorable determination of eligibility for access to classified information at an appropriate level. This individual has signed a non-disclosure agreement and has a need-to-know for the specific classified information in the performance of official duties. In this case, need-to-know is satisfied by virtue of the officially assigned duty to escort classified information, although the individual may not otherwise require access to the information.

There are regulatory requirements that must be satisfied before the authorized individual can hand-carry or escort classified materials. First, the individual must receive a courier briefing. Second, the individual must be given the proper authorizing documentation.

The remainder of this lesson will address these two requirements as well as special considerations when travel is necessary on a commercial passenger aircraft.

Briefing Requirements

1. Introduction

Once the decision is made to have the materials escorted or hand-carried and an individual is selected, there are regulatory requirements that must be met.

One of those requirements is for the designated individual to receive a courier briefing. Individuals escorting or hand-carrying classified information must be informed of and acknowledge their security responsibilities *before* they are authorized to serve as a courier. Heads of specific Components may require written acknowledgement of this briefing for program oversight. The entire briefing must be given before the courier performs the assignment. The objective of the briefing is to provide couriers with the appropriate procedures to safeguard the classified information so as to ensure its integrity while in transit.

To identify the timeline of a courier's responsibilities, the content for the briefing can be sectioned into:

- Pre-trip considerations
- En route considerations
- Post-trip considerations

In this topic we will cover the baseline briefing as required by DoD Manual 5200.01, Volume 3. Note that individual Components may have additional requirements.

2. Pre-Trip Considerations and Requirements

The requirements and procedures for hand-carrying and escorting classified materials do not start when a courier leaves the building. There are many *pre-trip* considerations.

Before leaving a secure facility with classified materials, couriers must make sure their personal travel documents are in order. Depending on the task, personal travel documentation may include passports, courier authorizations, medical records, travel itineraries, or other documents. It is the individual's responsibility to ensure that his or her personal travel documents are complete, valid, and current.

The system for keeping track of the classified materials begins *before* the materials leave the facility. Couriers need an inventory of the classified materials. One copy of the inventory stays in the courier's security office, and the courier carries a copy.

If disclosure of the classified information to foreign nationals is involved, the DoD Component official responsible for approving the hand-carry is also responsible for obtaining disclosure authorization.

Couriers should also be knowledgeable about the regulatory requirements for packaging classified materials for transmission or transport and their responsibility to report any suspicious contacts that may occur during the course of the trip.

3. En Route Considerations and Requirements

During the trip, couriers are responsible and liable for the materials they are transmitting. In cases of emergency, couriers must take measures to protect the classified materials. If it is necessary for a trip to include an overnight stop, couriers must store the classified materials at a prearranged or cleared facility in a manner appropriate for the classification level of the materials.

While en route, couriers are encouraged to promptly report to cognizant security officials any suspicious contacts or any act or incident that might jeopardize or compromise the security of the classified materials.

There are some things that couriers should *not* do while transmitting classified materials. They must *not* discuss or disclose classified material in public. They must not deviate from the authorized travel schedule. They should also be advised not to make any unnecessary stops, but to proceed directly from the point of departure to the destination. Couriers must never, under any circumstances, leave classified materials unattended or unsecured. During overnight stops, they *must not* store classified materials in hotel rooms, hotel safes, private residences, public lockers, unattended vehicles, or use any other unauthorized storage means. Couriers must not open the materials en route, except under circumstances involving a border crossing.

4. En Route Border Crossings

Advise couriers of their responsibilities if a border crossing with another country is involved.

There is no assurance of immunity from search by the customs, police, or immigration officials. If such an official inquires about the contents of the materials, the courier must present their courier orders and ask to speak to the senior customs, police, or immigration official. This action will normally suffice to pass the material through unopened.

However, if the senior official demands to see the package contents, the package maybe opened in their presence, but this should be done in an area out of sight of the general public. Couriers should take precautions to show officials only as much of the contents as will satisfy them that the package does not contain any other item.

Upon completion of the examination, couriers will need to ask the official to repack the material or volunteer to assist in repacking. Then couriers must request that the senior official provide evidence of the opening and inspection of the package.

The senior official should sign shipping documents, if there are any, or the courier certificate confirming that the package was opened. Couriers must inform both the dispatching security officer and addressee in writing that the material was opened.

5. Post-Trip Considerations and Requirements

Couriers are not finished with their tasks until the classified materials have been accounted for at their point of origin.

If a courier is returning the materials to the original facility, then he or she must return them in a properly sealed package. The materials will be re-inventoried to make sure they are all there.

If the materials are not being returned, then the courier may be required to produce a receipt signed by the security officer from the organization to which they were delivered.

6. Recap of Briefing Requirements

This concludes the discussion of the briefing requirements. The importance of the courier briefing cannot be over emphasized.

Couriers are entrusted with the protection of classified information in their role of escorting or hand-carrying classified information.

You have seen the minimum requirements for these phases of the trip. Components or programs may have additional enhanced requirements

Here is a Job Aid that summarizes the courier briefing requirements:

Requirements for a Courier Briefing

Courier briefing for escorting or hand-carrying classified information

(not using commercial passenger aircraft)

The briefing must take place before the assignment. Couriers must be informed of and acknowledge their security responsibilities as described below.

Pre-Trip Considerations

- Courier ensures personal travel documents are complete, valid, and current
- Courier has one copy of inventory (another copy of inventory stays in security office)
- Courier has disclosure authorization, if disclosure of the classified information to foreign nationals is involved

Tip: Couriers should understand packaging requirements for classified materials.

Tip: Couriers should be briefed on their responsibility to report suspicious contacts or incidents.

En Route Considerations

- Couriers are liable and responsible for materials.
- Couriers must protect materials in case of emergency.
- Couriers must use appropriate storage, if necessary, in pre-arranged U.S. military facility, U.S. government facility, U.S. embassy, or cleared U.S. contractor facility.
- Couriers must NOT discuss the materials in public.
- Couriers must NOT deviate from authorized travel schedule.
- Couriers must NOT leave materials unattended or unsecured.
- Couriers must NOT store the materials in an unauthorized way. (This includes: hotel rooms,

hotel safes, private residences, public lockers, unattended vehicles, and any other unauthorized storage means.)

- Couriers must NOT open material en route (except as described below).

Tip: Couriers should report suspicious contacts or incidents.

Tip: Couriers should make no unnecessary stops en route to their delivery point.

En Route Considerations – Border Crossing

There is no assurance of immunity from search by customs, police, or immigration officials.

- If an official inquires about the material:
 - Courier must show courier authorization orders.
 - Courier must ask to speak to the senior official.
- If senior official demands opening package:
 - Courier may open package in the official's presence away from public view.
 - Couriers should show only as much of contents as will satisfy the official that the package does not contain any other item
 - Couriers must ensure package is repackaged.
 - Courier must have senior official sign the package and shipping documents or courier certificate.
 - Courier must inform both addressee and dispatching security officer in writing that materials were opened.

Post-Trip Considerations

- Receipt – If courier is not returning materials, courier may be required to produce receipt signed by security officer of receiving organization.
- Re-inventory – If couriers is returning materials to original facility, courier must return materials in properly sealed package. Materials will be re-inventoried.

Other Requirements

1. Authorization Documentation

In addition for the requirement for a courier briefing, written authorization must be issued for the individual.

If the mission involves commercial air travel, a letter of authorization for travel aboard commercial passenger aircraft is required. This letter must be on agency letterhead. You will need to issue an authorization letter *each time* an individual is required to escort or hand-carry classified information aboard a commercial passenger aircraft. Provide the courier with the original letter. A reproduced copy is not acceptable. Also provide the courier enough authenticated copies to give to each airline involved.

If travel on a commercial airline is not involved, a DD Form 2501 may be used if there is a continuing need for hand-carry or escort services, or a written authorization statement may be included in official travel orders. Neither of these documents can be used to authorize hand-carry or escort of classified materials when traveling on commercial aircraft.

The appropriate documented authorization is not only a regulatory requirement, but it also provides justification for individuals to have classified information in their possession.

a. Letter of Authorization

An original letter of authorization on agency letterhead is required *each time* an individual is required to escort or hand-carry classified information aboard a commercial passenger aircraft.

The letter must include:

- The full name of the individual and his or her employing agency or company
- A description of the type of identification the individual will present
- A description of materials being carried, such as the number of packages, the dimensions of each package, and the addressee and addressor

The letter must specify:

- The point of departure
- The destination
- Any known transfer points

Note that Components may require, and others may find it useful, to provide additional flight itinerary information.

The letter must have:

- A date of issue and expiration date
- The name, title, and signature of the official issuing the letter

Each package or carton to be exempt shall be signed on its face by the official who signed the letter. There must be contact information on the letter for confirmation purposes. If foreign travel is involved, the letter must be translated into the official language of the country the courier will be traveling to.

b. DD Form 2501

DD Form 2501, Courier Authorization Card may be issued when there is a continuing need to escort or hand-carry classified information.

Certain safeguards apply when the form is used. It must be signed by an appropriate official in the individual's servicing security office. Stocks of the form are controlled to preclude unauthorized use. The form is issued for no more than two years at a time. After the form expires, the requirement for authorization to hand-carry is reevaluated and a new form issued, if appropriate. Only the last four (4) digits of the individual's social security number shall be used in completing the DD Form 2501. Currently valid DD Forms 2501 shall be updated when renewed according to policies and procedures established by the official having security responsibility for such information or programs.

c. Authorization Statement

If DD Form 2501 is not being used, an authorization statement may be issued. The authorization statement may be a separate document, or the statement may be included in official travel orders, except for travel aboard commercial passenger aircraft. The authorization statement should contain the same information provided in DD Form 2501.

2. Use of Commercial Passenger Airline

It is sometimes necessary for a courier to take classified materials on a commercial passenger aircraft. Since employees carrying classified materials are subject to routine processing by airline security agents, this mode of transporting classified information presents special risks and challenges.

If it is necessary to travel by commercial passenger aircraft, all airlines involved should be U.S. carriers. Only if a U.S. carrier is not available may a foreign carrier be used.

The DoD information Security Program provides specific guidance on how to handle these challenges, including special pre-trip planning considerations and issues to consider at the airport.

a. Pre-Trip Considerations

To facilitate processing through airline ticketing, screening, and boarding procedures, coordinate in advance with airline and departure terminal officials, and when possible, with intermediate transfer points. Local Transportation Security Administration (TSA) offices can often be of assistance. During this coordination, specific advice should be sought regarding the nature of the required documentation.

The courier must carry an original authorization letter on agency letterhead stationery. The courier must have a DoD or contractor-issued identification card including a photograph, descriptive data, and signature. If the identification does not contain date of birth, height, weight, and signature, these items must be included in the written authorization letter.

If the courier will be escorting bulk materials, make advance arrangements with the airline regarding the observation of loading and unloading of the materials.

As you prepare the classified materials for transporting aboard commercial passenger aircraft, visit the TSA website first to obtain a current list of prohibited items. Use this list to prevent prohibited items from being inadvertently included in the materials, thereby minimizing the likelihood of a security concern.

b. En Route Considerations

Couriers who are hand-carrying classified materials should proceed through normal airline ticketing and boarding procedures. They should offer classified packages for routine inspection without drawing attention to the fact that they are transporting classified material. If they are challenged by airport security screening officials, they should discretely disclose their status, produce the authorization letter, and, if necessary, ask to speak to the senior screening official. Remember that there is no immunity from inspection by official government authorities.

Couriers who are escorting classified bulk material must ensure the integrity of the classified bulk material during loading and unloading. This is accomplished by the courier or appointed representative physically observing the loading and unloading of the classified bulk material, and the closing and opening of the cargo compartment.

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

What conditions or requirements must be satisfied before an individual can hand-carry or escort classified materials? Select all that apply.

- Has a favorable determination for eligibility for access to classified information
- Has signed a non-disclosure agreement
- Has a need-to-know for performance of official courier duties
- Has received a courier briefing
- Has examined the classified materials before they are packaged
- Has received an authorizing letter, statement, or form

Question 2

What are some pre-trip considerations for couriers? Select all that apply.

- The courier must ensure personal documents are complete, valid, and current.
- The courier must have a copy of the inventory of the classified materials.
- The courier must have an authorization letter, form, or statement.
- The courier must have a disclosure authorization if disclosure of the classified information to foreign nationals is involved.

Question 3

Which of the following statements are true? Select all that apply.

- Couriers are responsible for the classified materials.
- Couriers are not liable for the classified materials.
- Couriers must take measures to protect the classified materials in cases of emergency.
- Couriers may be required to obtain a receipt for any classified materials delivered.

Question 4

What are courier requirements and guidelines while hand-carrying or escorting the materials? Select all that apply.

- Couriers must never leave the materials unattended.
- Couriers must discuss the materials only with other couriers.
- Couriers may make a detour for personal reasons when en route as long as they arrive on schedule at the destination.
- Couriers must open the materials at least once to ensure they are intact.

Question 5

If an overnight stay is required, which of the following are authorized for storing classified materials? Select all that apply.

- A U.S. military facility
- A U.S. embassy
- A cleared contractor facility
- A hotel safe in a locked hotel room

Question 6

If a border crossing is required, and an official at the border questions the contents of the materials, what must the courier do? Select all that apply.

- Request immunity from search
- Present the courier authorization papers
- Ask to speak to a senior official
- Agree to open the package but only in public view so there are witnesses

Question 7

Select True or False for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	True	False
If traveling by commercial passenger aircraft, the courier must carry the <i>original</i> of the authorization letter.	<input type="radio"/>	<input type="radio"/>
A separate authorization letter must be issued each time a courier has an assignment that involves travel on a commercial passenger aircraft.	<input type="radio"/>	<input type="radio"/>
DD Form 2501 must be used if the courier will travel using a commercial passenger aircraft.	<input type="radio"/>	<input type="radio"/>
An authorization statement for the assignment may be included in travel orders if the courier is not traveling via commercial passenger aircraft.	<input type="radio"/>	<input type="radio"/>
DD Form 2501 may be issued for a period up to two years if there is a continuing need to escort or hand-carry classified materials.	<input type="radio"/>	<input type="radio"/>

Question 8

When traveling by commercial passenger aircraft, to whom should the courier show the authorization letter? Select all that apply.

- To the airline agent at the ticket counter before checking in
- To the senior TSA official when going through security
- To any TSA official that challenges the contents of the materials
- To the airline agent at the gate before boarding
- To the flight attendant when on board

Lesson Conclusion

In this lesson, you learned about who can escort or hand-carry classified materials. You learned about the requirement for a courier briefing and its contents. You learned about courier authorization documents, and you learned about special considerations when couriers must travel by commercial passenger aircraft.

Answer Key

Question 1

To hand-carry or escort classified materials, an individual must have a favorable determination for eligibility for access to classified information, a signed a non-disclosure agreement, a need-to-know for performance of official courier duties, and received a courier briefing and an authorizing letter, statement, or form.

Question 2

Pre-trip considerations for couriers include:

- The courier must ensure personal documents are complete, valid, and current.
- The courier must have a copy of the inventory of the classified materials.
- The courier must have an authorization letter, form, or statement.
- The courier must have a disclosure authorization if disclosure of the classified information to foreign nationals is involved.

Question 3

The following statements are true:

- Couriers are responsible for the classified materials.
- Couriers must take measures to protect the classified materials in cases of emergency.
- Couriers may be required to obtain a receipt for any classified materials delivered.

Question 4

While hand-carrying or escorting the materials, **couriers must never leave the materials unattended.**

Question 5

If an overnight stay is required, the following are authorized for storing classified material:

- A U.S. military facility
- A U.S. embassy
- A cleared contractor facility

Question 6

If a border crossing is required, and an official at the border questions the contents of the materials, the courier must **present the courier authorization papers** and **ask to speak to a senior official.**

Question 7

	True	False
If traveling by commercial passenger aircraft, the courier must carry the <i>original</i> of the authorization letter.	<input checked="" type="radio"/>	<input type="radio"/>
A separate authorization letter must be issued each time a courier has an assignment that involves travel on a commercial passenger aircraft.	<input checked="" type="radio"/>	<input type="radio"/>
DD Form 2501 must be used if the courier will travel using a commercial passenger aircraft.	<input type="radio"/>	<input checked="" type="radio"/>
An authorization statement for the assignment may be included in travel orders if the courier is not traveling via commercial passenger aircraft.	<input checked="" type="radio"/>	<input type="radio"/>
DD Form 2501 may be issued for a period up to two years if there is a continuing need to escort or hand-carry classified materials.	<input checked="" type="radio"/>	<input type="radio"/>

Question 8

When traveling by commercial passenger aircraft, the courier may show the authorization letter only **to any TSA official that challenges the contents of the materials.**

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Preparing Materials for Transmission and Transportation

Lesson Introduction

No matter which authorized method of transmission or transportation you use, you must take steps to protect classified materials from unauthorized access during transit. DoD Manual 5200.01, Volume 3, DoD Information Security Program, includes requirements for packaging, addressing, and tracking classified materials in preparation for transmission and transportation for DoD entities.

In this lesson, you will learn the baseline requirements for preparing classified material for transmission and transportation. Some facilities or components may have more stringent requirements than those presented here.

The lesson objectives are:

- Identify the purpose of and the basic concepts involved in properly preparing classified material for transmission and transportation
- Identify the requirements for wrapping envelopes and parcels that contain classified material
- Identify how proper packaging requirements are met when using alternate forms of wrapping materials.

Brief Packaging Concepts

1. Purpose

Classified packages must be prepared for transmission and transportation by packaging and sealing them in a way that minimizes the risk of accidental exposure and facilitates the detection of deliberate tampering.

2. Overview of Procedures

You can minimize these risks by following some basic packaging procedures.

It is recommended you always verify the recipient's clearance and access level. It is also recommended to verify the receiving activity's mailing address prior to transmission because some activities may have a specific mailing address for the receipt of classified material, or their address may have changed. Once all the information has been verified, the classified material must be protected with *two* layers of durable, opaque wrapping or packaging material.

Double wrapping ensures the classified material is not exposed if the outer wrapper is damaged in transit or opened by someone other than the intended recipient. It is not necessary to double-wrap materials being transmitted *within* a facility but the material must be protected adequately to prevent any unauthorized disclosure of classified information.

Receipts are required for all transfers of classified information and material to a foreign government, except in two instances: (1) Most foreign governments waive the receipt requirement for their restricted information; (2) Transmissions of classified information to a foreign government by information technology (IT) and communications systems meeting the requirements of DoDM 5200.01, Volume 3 shall, at a minimum, be audited to assure that the intended recipient receives the information. The audit procedures for verifying receipt shall be commensurate with those specified in DoDI 8500.01. The receipts serve two important purposes. First, they document the transfer of security jurisdiction between the governments. Second, they alert the recipient government that the information or material has been transferred, and that it is responsible for protecting the information or material in compliance with the pertinent security or program agreement or arrangement.

Let's look more closely at procedures for double-wrapping and keeping track of classified materials that are small enough to fit in an envelope or a small parcel.

Applying Packaging Concepts

1. Envelopes and Small Parcels: Inner Wrapper

Inner wrappers provide the first layer of protection for classified information being transmitted or transported, but if classified text comes in direct contact with the inner wrapper, there is a risk of exposure through image transfer or the surreptitious use of technology that can render the wrapper translucent. You can prevent classified text from coming in contact with the inner wrapper by placing something between the document and the envelope or by folding the document in on itself.

It is important to mark the inner wrapper properly because at some government activities and DoD contractor facilities, the outer wrapper may be removed by someone other than the intended recipient. Inner wrapper markings must include the receiving government activity or cleared contractor mailing address and the sender's return address. The inner envelope may have an attention line with a person's name.

Make sure the mailing address is legible so the classified material is not delivered into the wrong hands! To facilitate timely delivery, it is recommended the inner wrappers include the name or office symbol of the intended recipient. Note, however, classified information intended only for U.S. elements of international staffs or other organizations must be addressed specifically to those elements.

The inner wrapper must also be labeled with the highest classification level of the contents, and any special markings, such as *Restricted Data* or *NATO*. It is recommended these markings appear on all sides of the inner wrapper.

DoD Manual 5200.01, Volume 3, Appendix to Enclosure 4, DoD Information Security Program, addresses the subject of receipts for classified information during transmission and transportation. It is recognized that receipt systems may be prescribed in most situations by heads of the DoD Components when transferring classified to foreign



governments. The receipts serve two important purposes. First, they document the transfer of security jurisdiction between the governments. Second, they alert the recipient government that the information or material has been transferred, and that it is responsible for protecting the information or material in compliance with the pertinent security or program agreement.

When a receipt *is* necessary, it should be attached to or enclosed in the inner wrapper. The receipt must identify the sender, the addressee, and the contents of the package.

This regulation also does not dictate how to seal the inner wrapper. However, to facilitate the detection of tampering and to prevent accidental exposure that may occur during transit, the use of reinforced gummed tape is recommended.

The information in boxes like the one below is supplemental content that you may find useful; however, it will not be addressed in the course examination.

To avoid direct contact between classified text and inner wrapper:

-  Use:
 - Document cover sheets (SF 703, 704, 705)
 - Cover transmittal letters
 - Opaque paper
 - Cardboard
-  Fold the document in on itself

2. Envelopes and Small Parcels: Outer Wrapper

The outer wrapping is the second layer of protection for classified information being transmitted. It is also the first line of defense against a potential threat.

Once the classified package is in transit, the only physical protection of the material inside is the integrity of its wrapping. The outer wrapper must be durable. It is recommended you use corrugated cardboard or heavy-weight craft paper.

The size of the outer wrapper should minimize the movement of the inner wrapper. This prevents the weight of the inner wrapper from shifting and compromising the seams of the outer wrapper.

Like the inner wrapper, the outer wrapper must be marked with the receiving government activity or DoD contractor's mailing address approved for receipt of classified information. It must also include the sender's return address.

The outer wrapper may include office codes, numbers, or phrases in the Attention line, but it should *not* include individual names unless it is being sent via General Services Administration contract overnight delivery service.

The outer wrapper should *not* bear any classification markings or special handling instructions indicating its contents are classified.

Like the inner wrapper, the outer wrapper should be sealed to prevent accidental exposure during transit. The use of reinforced tape is recommended.

When confidential information is transmitted via United States Postal Service (USPS) First Class Mail, the outer wrapper must contain the following statement: "Return Service Requested."

Now that you understand the basic requirements for wrapping classified materials, let's consider some alternate ways these requirements can be met.

3. Classified Components

Encased equipment items with classified internal components may be relatively small, such as a hard drive, or they may be bulky, such as a mission data recorder. When the outside shell or housing of a small packageable component does not expose the internal classified information, the outer casing can be considered the *inner* enclosure packaging.

If someone wrote or attached something classified to the hard drive, it would, however, require double wrapping. If the classified material is an inaccessible internal component of a bulky item of equipment, it may not be easily packaged.

In these cases, the outside housing of the item may be considered a sufficient enclosure provided it does not reveal classified information. Additionally, the classified internal components of bulky equipment must be inaccessible.

4. Hand-carried Materials: Briefcases and Zippered Pouches

When classified materials are being hand-carried, locked briefcases or zippered pouches made of canvas or other heavy-duty material with an integral lock may be used as the outer wrapper. Let's consider marking requirements for these types of wrappers.

Although a briefcase does not need to be addressed in the same way that a package does, the sender's mailing address must be displayed prominently on the outside of the briefcase or pouch. This could be accomplished by placing the required information under the clear protection label area offered by some manufacturers, attaching a luggage tag to the handle, or embroidering the information directly onto the pouch. To avoid drawing attention to the material during transit, don't place markings, seals, or labels on the outside that identify its affiliation with the Department of Defense.

Zippered pouches must have the name and address of the sending organization and the name and telephone number of a point of contact, or POC, displayed prominently on the outside. Some activities meet this requirement by affixing a business card to the pouch.

Another way to meet this requirement is to embroider the information directly onto the pouch. The pouch must also have a serial number displayed conspicuously on its exterior. The pouch must be locked and its key must be kept in a separate, sealed envelope. The activity authorizing the use of the pouch must maintain an internal system to account for and track the location of the pouch and its key.

Use a briefcase or pouch only to assist in enforcing need to know. Its use shall in no way abrogate personal responsibility to ensure that the classified material is delivered to a person who has an appropriate security clearance and access for the information involved.

Additional Guidance for Use of Briefcases or Zippered Pouches for Hand-carrying Classified Material:

- Clearly and recognizably display the name and street address of the organization sending the classified material, and the name and telephone number of a point of contact within the sending activity, on the outside of the briefcase or pouch.
- Serially number the pouch or briefcase and clearly display this serial number on its exterior surface.
- Lock the briefcase or pouch and place its key in a separate sealed envelope.
- Store the briefcase or pouch, when containing classified material, according to the highest classification level and any special controls applicable to its contents.
- The activity authorizing use of the briefcase or pouch must maintain an internal system to account for and track the location of the pouch and its key.
- Use a briefcase or pouch only to assist in enforcing need to know. Its use shall in no way abrogate personal responsibility to ensure that the classified material is delivered to a person who has an appropriate security clearance and access for the information involved.
- Any act or incident involving the pouch that might jeopardize or compromise the security of its classified contents must be reported promptly to cognizant security officials.

5. Large, Bulky Items

Some classified material is of a size, weight, or nature that is not *reasonably* packageable, such as some military equipment. Yet, because its exposure reveals classified information, alternative packaging must be used.

The covering materials must be opaque to hide all classified features and durable enough to ensure the protection while the material is in transit. A satellite array or a weapons system could be securely draped with a tarp, canvas shroud, or similar covering. Specialized shipping containers, including closed cargo transporters, the igloos used with defense courier service for air transport, or palletized containers for military air cargo shipments may be considered the outer wrapping for this type of shipment.

In these circumstances, the mode of transport becomes very important. The freight should be shipped in closed vehicles when required. Additional safeguards, such as escorts, may be needed.

Movement of this type of material is often complex, and may require coordination with supply or logistics elements. A transportation plan may also be required.

Additional procedures include notifying the consignee of the shipment, identifying any transshipment activities, and identifying actions to be taken in case of non-delivery or unexpected delay in delivery.

It is recommended that security personnel coordinate with their supply or logistics elements to determine the authorized mode of transit.

Transportation plans support the movement of bulky classified material. The development of this plan requires research and coordination with various officials, including local, state, and federal authorities. Following this coordination, a transportation plan is developed and approved. As with any complex task, advanced planning is critical.

T Topic areas to be considered in the development of a transportation plan may include, among other areas:

<i>Title of Plan</i>
<i>Date of movement</i>
<i>Authorization/Approval</i>
A. Purpose
B. Description of consignment
C. Identification of responsible government and/or company representatives
D. Identification of commercial entities to be involved in each shipment
E. Packaging the consignment
F. Routing of the consignment
G. Couriers/escorts
H. Recipient responsibilities
J. Return of material
K. Other information as required

Review Activity

Try answering the following questions. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Question 1

What is the purpose of the procedures for preparing classified material for transmission and transportation? Select all that apply.

- Minimize the risk of accidental exposure if the outer layer is damaged.
- Facilitate the detection of deliberate tampering.
- Decrease the risk of theft because the outer layer does not indicate it contains classified material.
- Protect material from weather-related damage.

Question 2

Scenario: You need to send a Confidential document from Ft. Eustis to Jennifer Brody, who works in the Pentagon.

Which of the following should appear on the **inner** envelope? Select all that apply.

- Ft. Eustis return address
- Ms. Jennifer Brody / Address at the Pentagon
- CONFIDENTIAL
- SECRET
- TOP SECRET
- Address at the Pentagon

Which of the following should appear on the **outer** envelope? Select all that apply.

- Ft. Eustis return address
- Ms. Jennifer Brody / Address at the Pentagon
- CONFIDENTIAL
- SECRET
- TOP SECRET
- Address at the Pentagon

Question 3

Scenario Update: The sender of the Confidential document would like to include a receipt. What information should be included on the receipt? Select all that apply.

- The name of the sender
- The name of the recipient
- The name of the Confidential document
- A Confidential summary of the document contents

Question 4

Scenario Update: Your inner and outer layers are properly marked, including classification marking on the inner envelope and a verified address on both layers. You have prepared a receipt, and you have plenty of reinforced tape. Can you think of anything else you might need before you package your Confidential document?

Write your answers in the space provided.

Question 5

True False

Select True or False for each statement.

Classified documents must be double-wrapped inside a locked briefcase or zippered pouch when they are hand-carried.

Large, bulky items are exempt from double-wrapping requirements for transmission and transportation.

Lesson Conclusion

In this lesson, you learned about the purpose of and basic procedures for properly preparing classified material for transmission and transport, the baseline requirements for wrapping envelopes and parcels that contain classified materials, and how these requirements can be met with alternate wrapping materials.

Answer Key

Question 1

Two layers of durable, opaque material will **minimize the risk of accidental exposure** if the outer layer is damaged, **facilitate the detection of deliberate tampering**, and **decrease the risk of theft** because the outer layer does not indicate it contains classified material

Question 2

Scenario: You need to send a Confidential document from Ft. Eustis to Jennifer Brody, who works in the Pentagon.

The **inner** envelope should be marked with the following:

- Ft. Eustis return address
- "Ms. Jennifer Brody / Address at the Pentagon"
- "CONFIDENTIAL"

The **outer** envelope should be marked with the following:

- Ft. Eustis return address
- Address at the Pentagon

Question 3

The receipt should identify **the sender, the recipient, and the contents of the package**.

Question 4

It is important that you prevent the text on your document from coming in direct contact with the inside of the inner wrapper. You need a cover sheet, transmittal form, piece of opaque paper, or piece of cardboard to go between your document and the inside of the envelope. Alternatively, you could fold your document in on itself before you put it into the inner wrapper.

Question 5

Classified documents must be double-wrapped inside a locked briefcase or zippered pouch when they are hand-carried.

Large, bulky items are exempt from double-wrapping requirements for transmission and transportation.

True **False**

Student Guide

Course: Transmission and Transportation for DoD

Lesson: Course Conclusion

Course Summary

The transmission and transportation of classified materials involves many considerations at all phases of the process -- from the preliminary decision about whether to send the information in the first place, all the way up to its receipt and storage at its destination. You should now know the factors you need to consider and the procedures you need to follow in order to send and receive classified information. You should also know the sources of guidance you can refer to for greater detail about specific situations.

Lesson Review

Here is a list of the lessons in the course:

- Transmission and Transportation Basics
- Selecting an Authorized Transmission and Transportation Method
- Dissemination of Special Types of Information
- Procedures for Escorting or Hand-carrying Classified Information
- Preparing Materials for Transmission and Transportation

Course Objectives

You should now be able to:

- ✓ Identify the policy documents that govern transmission and transportation of classified information
- ✓ Based on classification level, identify the authorized methods for transmission and transportation of classified information
- ✓ Identify the dissemination requirements for special types of information
- ✓ Identify the procedures to escort or hand-carry classified information
- ✓ Identify the procedures to prepare classified information for transmission and transportation

Conclusion

Congratulations. You have completed the Transmission and Transportation for DoD Course.

To receive course credit, you *must* take the Transmission and Transportation for DoD examination. Please use the STEPP system to register for the online exam.