Information Security Webinar Series

Transmission and Transportation Requirements

According to DoD Manual 5200.01, Volume 3, Enclosure 4, Components shall establish procedures for transmitting and transporting classified information. These procedures must do the following:

- Maximize accessibility of classified information
- Minimize risk of compromise
- Use most cost effective means

In addition, persons transmitting or transporting classified information are responsible for ensuring that the intended recipient(s) are authorized access, have a need-to-know, and have the capability to store classified information in accordance with requirements.

Dissemination Outside DoD

Classified information originating in another DoD Component or in a department or agency other than the DoD 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. The following criteria apply:

- DoD Manual 5200.01, Volume 3, Enclosure 2, Section 3 criteria for access must be satisfied.
- The classified information cannot be marked as requiring prior authorization for dissemination to another department or agency. The marking "ORCON" may be used to identify information requiring prior authorization for dissemination to another department or agency.
- The document was created on or after June 27, 2010.

If documents were created before June 27, 2010, they may not be disseminated outside of the Department of Defense without the originator's consent. Additionally, documents created on or after June 10, 2010 whose classification is derived from documents created prior to that date shall not be disseminated outside of DoD without the originator's consent.

Pursuant to Executive Order (E.O.) 13549, dissemination of classified information to state, local, tribal and private sector officials shall be in accordance with implementing guidance issued by the Department of Homeland Security.

Classified information originating in, or provided to, or by the DoD may be disseminated to a foreign government or an international organization of governments, or any element thereof, in accordance with E.O. 13526 and the DoD Manual 5200.01.

Dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued by the Director of National Intelligence.

Requirements by Level

Detailed transmission methods and requirements for the different classification levels such as Top Secret, Secret, and Confidential can be found in DoD Manual 5200.01, Volume 3, Enclosure 4. There are six approved methods for Top Secret materials, thirteen for Secret materials, and eighteen for Confidential materials.

Secure Communications

Transmission of DoD information shall comply, as appropriate, with the COMSEC measures and procedures identified in DoD Instruction 8523.01.

Computer to Computer Transmission

Transmission systems must be in accordance with Intelligence Community Directive (ICD) 503, as applicable, to operate at a level of classification commensurate with the data being transmitted. Electronic transmission of classified information over secure computer-to-computer links (e.g., via secure email) is preferable to physical transfer of hard copy documents. Classified information transmitted in this manner shall be marked in accordance with DoD Manual 5200.01, Volume 2.

Facsimile (Fax) Transmission

Only secure facsimile equipment shall be used for facsimile transmission of classified information. The individual transmitting the information shall ensure the recipient has the appropriate clearance and a need-to-know, and that the secure connection is at the appropriate level of classification for the information being transmitted.

Additionally, the header or cover sheets used to precede the transmission of classified material shall be conspicuously marked with the highest security classification of the transmitted information and any required control markings.

The cover sheet shall also include the originator's name, organization, phone number, an unclassified title, the number of pages, and the receiver's name, organization and phone number. When the cover sheet contains no classified information, it shall also note "Unclassified When Classified Attachment(s) Removed."

Documents transmitted by fax shall have all markings required for a finished document, and shall be controlled and safeguarded by the recipient accordingly.

Telephone Transmission

Only approved secure telephones, including cell phones and phones integral to personal electronic devices, authorized by the Director, National Security Agency (NSA), may be used for telephonic transmission of classified information. Users must ensure the secure connection is at the appropriate level of classification for the information being discussed.

Material Preparation

When transferring classified information, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers durable enough to properly protect the material from accidental exposure and facilitate detection of tampering.

Prepare, package, and securely seal classified material in ways that minimize the risk of accidental exposure or undetected deliberate compromise. To minimize the risk of exposure of classified information, package documents so that the classified material is not in direct contact with the inner envelope or container (e.g., fold so classified material faces together).

Using Envelopes, Wrappings, or Containers

Address the outer envelope or container to a U.S. Government activity or to a DoD contractor with a facility clearance and appropriate storage capability and show the complete return address of the sender.

Outer envelope does NOT show classification marking.

On the inner envelope, show the address of the receiving activity, the address of the sender, the highest classification of the contents (including, where appropriate, any special dissemination or control markings such as "Restricted Data" or "NATO"), and any applicable special instructions. The inner envelope may have an attention line with a person's name.

Inner envelope shows classification marking, if appropriate.

If the classified material is an accessible internal component of an item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information. If the classified information is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient enclosure provided observation of it does not reveal classified information.

If the classified material is an item of equipment that cannot be packaged and the shell or body is classified, it shall be concealed with an opaque covering hiding all classified features.

Using Briefcases or Zippered Pouches

A locked briefcase or zippered pouch made of canvas or other heavy-duty material and having an integral key-operated lock may be used for hand-carrying classified material outside an activity. Such cases may also be used to restrict access to classified material when the intended recipient is not immediately available.

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.

Ensure the activity authorizing use of the briefcase or pouch maintains an internal system to account for and track the location of the pouch and its key.

Hand-Carrying Classified Information

The heads of DoD Components are responsible for establishing procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose unacceptable risk to the information. Hand-carrying is permitted between locations when other means of transmission or transportation cannot be used.

Hand-carrying can only be authorized in the following situations:

- Information is not available at the destination, and it is operationally necessary or contractually required.
- Information cannot be sent via secure e-mail, facsimile transmission, or other secure means.
- The appropriate official authorizes the hand-carry according to procedures the Head of the DoD Component establishes.
- The hand-carry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the U.S. escort retains custody and physical control of the information.
- Arrangements have been made for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

Individuals hand-carrying or serving as couriers or escorts for classified information shall be informed of and acknowledge their security responsibilities, and classified hand-carried material shall be appropriately packaged.

Hand-Carrying Responsibilities

Individuals are required to read written instructions or be briefed on the following responsibilities:

1. The individual is liable and responsible for the material being carried or escorted.
2. The material is not, under any circumstances, to be left unattended. During overnight stops, arrangements shall be made for storage of the classified material at a U.S. military facility, embassy, or cleared contractor facility. Classified information shall not be stored in hotel safes.
3. The material shall not be opened en route except in the circumstances previously described.
4. The material shall not be discussed or disclosed in any public place.
5. The individual shall not deviate from the authorized travel schedule.
6. In cases of emergency, the individual shall take measures to protect the material.
7. The individual is responsible for ensuring that personal travel documents (passport, courier authorization (if required), medical documents, etc.) are complete, valid, and current.

Customs, Police, and Immigration

Arrangements shall be made in advance with customs, police, and/or immigration officials to facilitate movement through security. However, there is no assurance of immunity from search by the customs, police, and/or immigration officials of countries, including the United

States, whose border the courier may cross.

Therefore, if such officials inquire into the contents of the consignment, the courier shall present the courier authorization or orders and ask to speak to the senior customs, police, and/or immigration official. This action shall normally suffice to pass the material through unopened. However, if the senior official demands to see the actual contents of the package, it may be opened in his or her presence, but shall be done in an area out of sight of the public.

In that instance:

1. Precautions shall be taken to show officials only as much of the contents as satisfies them that the package does not contain any other item. The courier shall ask the official to repack the material or assist in repacking it immediately upon completing the examination.

2. The senior customs, police, or immigration official shall be requested to provide evidence of opening and inspection of the package by sealing and signing it when closed and confirming on the shipping documents (if any) or courier certificate that the package has been opened. Both the addressee and the dispatching security officer shall be informed in writing of the opening of the material.

3. Classified material to be carried by a courier shall be inventoried, a copy of the inventory shall be retained at the courier's office or duty location, and the courier shall carry a copy.

4. Upon return, the courier shall return all classified material in a sealed package or, for any classified material that is not returned, produce a receipt signed by the security officer of the addressee organization.

Authorization

Responsible officials, as determined by DoD Component procedures, shall provide a written statement to each individual who is authorized to escort, courier, or hand-carry classified material.

The authorization statement may be contained in a letter, a courier card, or other written document, including travel orders.

DoD (DD) Form 2501, "Courier Authorization," may be used to identify appropriately cleared DoD military and civilian personnel who have been approved to hand-carry classified material according to the following:

1. The individual has a recurrent need to hand-carry classified information.

2. An appropriate official in the individual's servicing security office signs the form.

3. As mentioned in the poll question, the form is issued for no more than 2 years at a time. The authorization to hand-carry shall be revalidated at least once every 2 years, and a new form issued.

4. The use of the DD Form 2501 for verification of authorization to hand-carry SCI or SAP information shall be according to policies and procedures established by the official having security responsibility for such information or programs.

Receipts

Receipts are required for all transfers of classified information and material to a foreign government. 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.

Most foreign governments waive the receipt requirement for their restricted information. Transmission of classified information to a foreign government by IT and communications systems shall, at a minimum, be audited to assure that the intended recipient receives the information.

How Can CDSE Help With Annual Briefings?

The Center for Development of Security Excellence (CDSE) produces and provides a wide range of information security training, education, and awareness products to support the DoD Activity Security Manager's mission.

This includes instructor-led training, eLearning courseware, and training products to address the entire range of responsibilities assigned to an activity security manager.

On the CDSE website you can find additional information about CDSE products, access eLearning courseware, register for instructor-led training, and download job aids and security awareness materials.

Learn more at cdse.edu.

Instructor-Led Training

DoD Security Specialist Course
Broad survey course that includes general, industrial, personnel, information, and physical security related-topics targeted to personnel with little or no security-related experience.

www.cdse.edu/catalog/classroom/GS101.html

Information Security Management Course
Mid-level course intended for personnel who have a functional working knowledge of the DoD Information Security Program.

www.cdse.edu/catalog/classroom/IF201.htm

STEPP Learning Management System

A wide array of information security-related eLearning can be accessed on CDSE's learning management system called STEPP.

The STEPP system not only provides multimedia-rich courseware but also retains and maintains learner records and transcripts. STEPP is available for use by DoD and other U.S. Government personnel and contractors within the National Industrial Security Program.

Job Aids and Awareness Media

CDSE also produces various job aids to assist security professionals. They can be accessed on the CDSE website.

Job aid topics include Marking Classified Information, Derivative Classification Training, a Procedural Guide for Conducting Classified Conferences, and aids for the operation of standard locks.

Job Aids
www.cdse.edu/resources/supplemental-job-aids.html
Awareness Posters
www.cdse.edu/resources/posters.html

Instructional Media

In addition to instructor-led and eLearning courses, CDSE also offers a wide variety of other instructional media in support of the DoD Information Security Program. This includes Security Shorts, which are targeted eLearning courses designed to be completed in less than 15 minutes. Other instructional media includes podcasts, which are audio-only based courses, and short training videos on various security processes and procedures.

Security Shorts
www.cdse.edu/shorts
Security Podcasts
www.cdse.edu/catalog/podcasts
Security Training Videos
www.cdse.edu/resources/training_videos.html

Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.