Q-53 Security Training: Transmitting and Transporting Classified Information, Part I
Agenda

- Classified Information
- Dissemination
  - Outside of DoD
- Disclosure
- Handling
- Transmission and Transportation Requirements
  - Requirements By Level
  - Requirements for Top Secret Material
  - Requirements for Secret Material
  - Requirements for Confidential Material
- Electronic Communications
Classified Information and the Levels of Classification

- Classified information is official information owned and controlled by the US Government that has been determined by an Original Classification Authority (OCA) that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security that the OCA can identify and describe:
  - **Top Secret** – Information that the unauthorized disclosure of which reasonably could be expected to result in EXCEPTIONALLY GRAVE DAMAGE to the national security.
  - **Secret** – Information that the unauthorized disclosure of which reasonably could be expected to result in SERIOUS DAMAGE to the national security.
  - **Confidential** – Information that the unauthorized disclosure of which reasonably could be expected to result in DAMAGE to the national security.
Before disclosing, disseminating, or releasing classified information to **ANYONE**, all cleared personnel are always obligated to ensure that two standards are met:

1. Verify that the person to receive the disclosure is cleared at the level of information to be disclosed or higher;
2. Verify that the person to receive the disclosure has a **bona fide** **NEED TO KNOW**!

You must validate need to know before releasing CUI, too!
Dissemination of Classified Information Outside of 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:
  - The document was created on or after June 27, 2010
  - 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.
  - Use most cost effective means

- 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.
Disclosure of Classified Information

- Before giving a classified document to someone or disclosing classified information orally you must verify the recipient’s:
  - Identity
  - Clearance level
  - Need-to-know

- Do not disclose classified information over non-secure commercial telephones or in public places

- Be sure to inform the recipient of the classification level of information disclosed

- Only disclose classified information related to the specific purpose of the mission

- When you are visiting another location, contact the appropriate Security Office as soon as possible to pass your clearance information to the cleared facility you will be visiting.
When classified is in your possession:

- It **MUST** be under constant personal custody
- It **MUST** never be discussed in public places
- It **MUST** never be discussed on unsecure phones
- It **MUST** never be left unattended
- It **MUST** be stored in approved storage container
- It **MUST** never be processed on any computer not approved for classified processing by the Designated Approval Authority (DAA)

Handling classified should **NEVER** be routine.

**Always use cover sheets:**
Transmission of Classified Information

- According to DoD Manual 5200.01, Volume 3, Enclosure 4, DoD 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.
Transmission Requirements by Level

- The transmission methods and requirements for the different classification levels can be found in DoD Manual 5200.01, Volume 3, Enclosure 4.

- The methods approved for Top Secret materials may be also be used to transport Secret or Confidential materials; the methods approved for Secret materials may also be used to transport Confidential materials.

- **Approved** electronic transmission methods are preferred.

- **Hand carry is the last resort.**

- **Commercial aircraft will not be utilized at JBM.**
Transmission Requirements for Top Secret Material

- The following methods may be used to transmit Top Secret material:
  - Electronic means over an approved secure communications system (i.e., a cryptographic system authorized by the NSA, or a protected distribution system designed and installed to meet the requirements of NSTISSI 7003. This applies to voice, data, message (both organizational and e-mail), and facsimile transmissions.
  - The Defense Courier Service (DCS) or authorized U.S. Government agency courier services (e.g., Department of State Diplomatic Courier Service, authorized DoD Component courier service).
  - Appropriately cleared U.S. Military and Government civilian personnel specifically designated to hand-carry the information and traveling by surface transportation or **appropriately cleared U.S. Military and Government civilian personnel specifically designated to carry the information and traveling on scheduled commercial passenger aircraft within and between the United States, its territories, and Canada***.

***While this is an approved method, due to the risk of compromise at security checkpoints JBM employees will not be transporting classified material using commercial aircraft.

<table>
<thead>
<tr>
<th>Table 1: Transmitting and Transporting Top Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courier</td>
</tr>
<tr>
<td>DCS</td>
</tr>
<tr>
<td>Authorized DoD Component System</td>
</tr>
<tr>
<td>Department of State</td>
</tr>
</tbody>
</table>
Transmission Requirements for Secret Material

- The following methods may be used to transmit Secret material:
  - Any of the means approved for Top Secret material.
  - U.S. Postal Service (USPS) registered mail within and between the United States, the District of Columbia, and the Commonwealth of Puerto Rico. U.S. Postal Service registered mail through Military Postal Service facilities outside the United States and its territories, if the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection.
  - Carriers cleared under the National Industrial Security Program providing a protective security service. This method is authorized only within the continental United States (CONUS) when other methods are impractical.
  - Overnight delivery using a GSA approved carrier, provided the requirements of DoD Manual 5200.01, Volume 3, Enclosure 4, Paragraph 4.c. are met.

    - Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The sender is responsible for ensuring that an authorized person at the receiving end is aware that the package is coming and will be available to receive the package, verifying the mailing address is correct, and confirming that the package did in fact arrive within the specified time period. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified COMSEC information, NATO information, SCI, and FGI shall not be transmitted in this manner.

  - U.S. Government and U.S. Government contract vehicles including aircraft, ships of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis.

  - Appropriately cleared U.S. Military and Government civilian personnel specifically designated to hand-carry the information and traveling by surface transportation.
## Transmission Requirements for Secret Material

### Table 2: Transmitting and Transporting Secret Material

<table>
<thead>
<tr>
<th>Same as Top Secret</th>
<th>Registered Mail</th>
<th>Protective Security Service</th>
<th>USPS Express Mail</th>
<th>Holder Of GSA Contract For Overnight Delivery</th>
<th>Appropriate Escort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluding DCS (unless COMSEC or SCI; or DCS has given prior approval; or US control cannot be ensured)</td>
<td>W/in US and Puerto Rico</td>
<td>W/in US boundaries</td>
<td>W/in US and Puerto Rico used only when most effective means w/in security, time, cost, and accountability constraints</td>
<td>W/in US &amp; territories</td>
<td>Vehicle operator</td>
</tr>
<tr>
<td>Contractor handcarry w/in US and territories (for other areas, see requirements of DoD 5220.22-R and 5220.22-M)</td>
<td>APO/FPO (only if mail will not pass out of US control)</td>
<td>Only when size, bulk, weight, nature, or escort considerations dictate</td>
<td>“Waiver of Signature and Indemnity” will NOT be executed</td>
<td>Authorized personnel available to receive delivery</td>
<td>Officer of ship</td>
</tr>
<tr>
<td></td>
<td>Canadian registered system w/ receipts (between government installations)</td>
<td>Check w/ Military Traffic Management Command (MTMC)</td>
<td>Use of street-side collection box prohibited not authorized for APO/FPO addresses</td>
<td>Verify correct mailing address</td>
<td>Pilot of aircraft (each a US citizen w/ Secret clearance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>May be addressed by name</td>
<td>Protected distribution system (approved and accredited computer systems/network)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Release signature upon receipt” block not executed</td>
<td>On a:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Use of street-side collection box prohibited</td>
<td>Gov’t or gov’t contract vehicle (including a/c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not authorized for classified COMSEC info, NATO, &amp; foreign gov’t info</td>
<td>USN ship</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Applicable postal regulations must be met</td>
<td>Civil Service operated USN ship</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>US registry ships under observation or in authorized storage</td>
</tr>
</tbody>
</table>
**Transmission Requirements for Confidential Material**

- The following methods may be used to transmit Confidential material:
  - Any of the means approved for the transmission of Secret information.
  - U.S. Postal Service Registered Mail for:
    - Material to and from military post office addressees (i.e., Fleet Post Office or Army Post Office) located outside the United States and its territories.
    - Material when the originator is uncertain that the addressee’s location is within U.S. boundaries.
  - U.S. Postal Service certified mail (or registered mail, if required above) for material addressed to DoD contractors or non-DoD agencies.
  - U.S. Postal Service first class mail between DoD Component locations anywhere in the United States and its territories. The outer envelope or wrapper shall be endorsed: “Return Service Requested.”
  - Commercial carriers that provide a constant surveillance service, as defined in the NISPOM, within CONUS.
  - Commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters shall sign a receipt for the material and agree to:
    - Deny unauthorized persons access to the Confidential material, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection shall not be unloaded.
    - Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.
  - Alternative or additional methods of transmission the Head of the DoD Component approves.
# Transmission Requirements for Secret Material

## Table 3: Transmitting and Transporting Confidential Material

<table>
<thead>
<tr>
<th>Same as Secret</th>
<th>Registered Mail</th>
<th>First Class Mail</th>
<th>Certified Mail</th>
<th>Constant Surveillance Service (CSS)</th>
<th>Appropriate Escort</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>❖ For:</td>
<td>❖ Between DoD w/in US and territories</td>
<td>❖ W/in US and Puerto Rico used only when most effective means w/in security, time, cost, and accountability constraints</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>❖ APO/FPO outside US and territories</td>
<td>❖ “Do Not Forward” on outer wrapping</td>
<td>❖ “Waiver of Signature and Indemnity” will NOT be executed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>❖ When uncertain if location w/in US boundaries</td>
<td>❖ May not be used from DoD to DoD contractor or to other agencies outside DoD</td>
<td>❖ Use of street-side collection box prohibited not authorized for APO/FPO addresses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>❖ to DoD contractor or other Executive Branch agency, if appropriate</td>
<td>❖</td>
<td>❖ Commander/master of US registry ships (US citizen)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **For:**
  - APO/FPO outside US and territories
  - When uncertain if location w/in US boundaries
  - to DoD contractor or other Executive Branch agency, if appropriate

- **Between DoD w/in US and territories**

- **Certified Mail**
  - W/in US and Puerto Rico used only when most effective means w/in security, time, cost, and accountability constraints
  - “Waiver of Signature and Indemnity” will NOT be executed
  - Use of street-side collection box prohibited not authorized for APO/FPO addresses

- **Constant Surveillance Service (CSS)**
  - W/in US boundaries
  - Check w/ Military Traffic Management Command (MTMC)

- **Appropriate Escort**
  - Commander/master of US registry ships (US citizen)
Electronic Transmission Overview

- Electronic transmission of classified information using approved secure communications methods is preferred.

- If you need to discuss or send classified information via phone or fax, you need to understand that:
  - All telephone calls may be intercepted
  - All email traffic can be intercepted
  - Telephones transmit all background conversations (all!)
  - FAX machines by themselves are not secure

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

Transmission of DoD information shall comply, as appropriate, with the COMSEC measures and procedures identified in DoD Instruction 8523.01. Use of COMSEC materials requires an additional briefing.

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 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.

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.
Hand-Carry Procedures

- As an authorized courier you are expressly charged to exert every effort within your means and ability to ensure the safe delivery of the material entrusted to you. In order to discharge your responsibility, you must adhere strictly to the general instruction below.

- As the designated courier you will be responsible for the protection and proper delivery of classified information entrusted to you.

- Classified information will NOT be left unattended in vehicles (locked or unlocked), hotels, terminals or other unofficial public places.

- In the event of an accident while traveling, the designated courier will take all precautions practicable to prevent loss or compromise. If loss or compromise should occur, please report it immediately to the nearest Federal Bureau of Investigations (FBI) Office.

- The fact that classified information is being transported by designated courier shall not be divulged to any unauthorized person.

- Positive identification of the person to whom classified material is to be delivered will be established and confirmed prior to transfer of custody.

- Prior to departure, a receipt of classified material being hand carried must be prepared, one copy must be carried with the package and a second copy will remain with the FSO/CSSO.

- While transporting classified material, you must proceed directly to your delivery destination. You may not take breaks or make stops en route for any reason.

- Government customer requirements will prevail. You are only authorized to transport classified material in support of a government contract and between government facilities. The government security office is the agency responsible for the preparation and oversight of couriered information/material.
Summary

ALWAYS PROTECT FIRST!

- While in use, classified material must never be left unsecured or unattended.
- When not in use, classified material must be properly secured in an approved container, unless it is being guarded by another properly cleared person with a need-to-know.
- The transmittal of classified material outside of approved computer system and network channels will generally be performed by the on-site Security Manager. Security will ensure that the material is properly packaged and transmitted in accordance with DoD regulations and the NISPOM.
- Before you attempt to transmit any classified information, you must ensure that you fully understand the requirements for proper transmission.
- If you have questions, consult Security!
Points of Contact

- **JB Management FSO:**
  - David Chandler / Alexandria Office / 703-354-6550 / dchandler@gojbm.com

- **JB Management SSE Division and Alternate FSO:**
  - Holly Leadbeater / NJ Office / 732-720-6494 / hleadbeater@gojbm.com

- **DoD Hotline:**