TSA Cargo Security

CHOICE AVIATION SERVICES

Changelog

- 9/15/2020 – **CHOICE.Training.TSA.v4**
  1. Added Change log in the beginning of the file.
  2. Added Instruction on how to secure a file to be shared (SSI locking and password sending separate)
  3. Change the wording to “TSA Monthly Master List” in multiple areas in document
  4. Removed Slide 28 to update Valid Unexpired ID clarification
  5. Removed Slide 37 to update with 1546.213 B1 details
  6. Removed Slide 51 to update the correct SSE requirements
  7. Removed Slide 55 to update checking on current TSA Monthly Master List and check if its valid.
  8. Removed Slide 90 to update escort process [make this term more generic and applicable to all stations]
  9. Added Diplomatic pouches details

- 9/17/2020 – **CHOICE.Training.TSA.v4.1**
  1. Added Slide 34 Instructions on how to protect SSI file.
  2. Updated Slide 56 - include type of CCSF tender and check
  3. Added Slide 57 - defined DIP ID Requirement by courier or rep
  4. Update Slide 57 - change the wording to read “Verify IAC tendering screened cargo against the Attachment 3 or 001 on the TSA Monthly Master List”
  5. Update verbiage on slide 57 with notes from 9/17

TRAINING OVERVIEW

- Security updates & threat levels
- New Updates
- Identification of valid forms of ID from shippers
- Confidentiality of personal information
- Shipper's Security Endorsement (SSE) Requirements
- Accepting and transferring cargo
- Identification of unauthorized weapons, explosives, incendiaries and other destructive devices, items or substances
- Notification - who to contact if support is needed
- Questions and Answers

Security Updates & Threat Levels

SENSITIVE SECURITY INFORMATION

WARNING:

THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR (Code Federal Regulations) PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW", AS DEFINED IN 49 CFR PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE IS GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

What is a covered person?

The topics covered in this training are considered Sensitive Security Information (SSI) and can be shared with covered persons according to Title 49 Code of Federal Regulations (CFR) 1520.7.

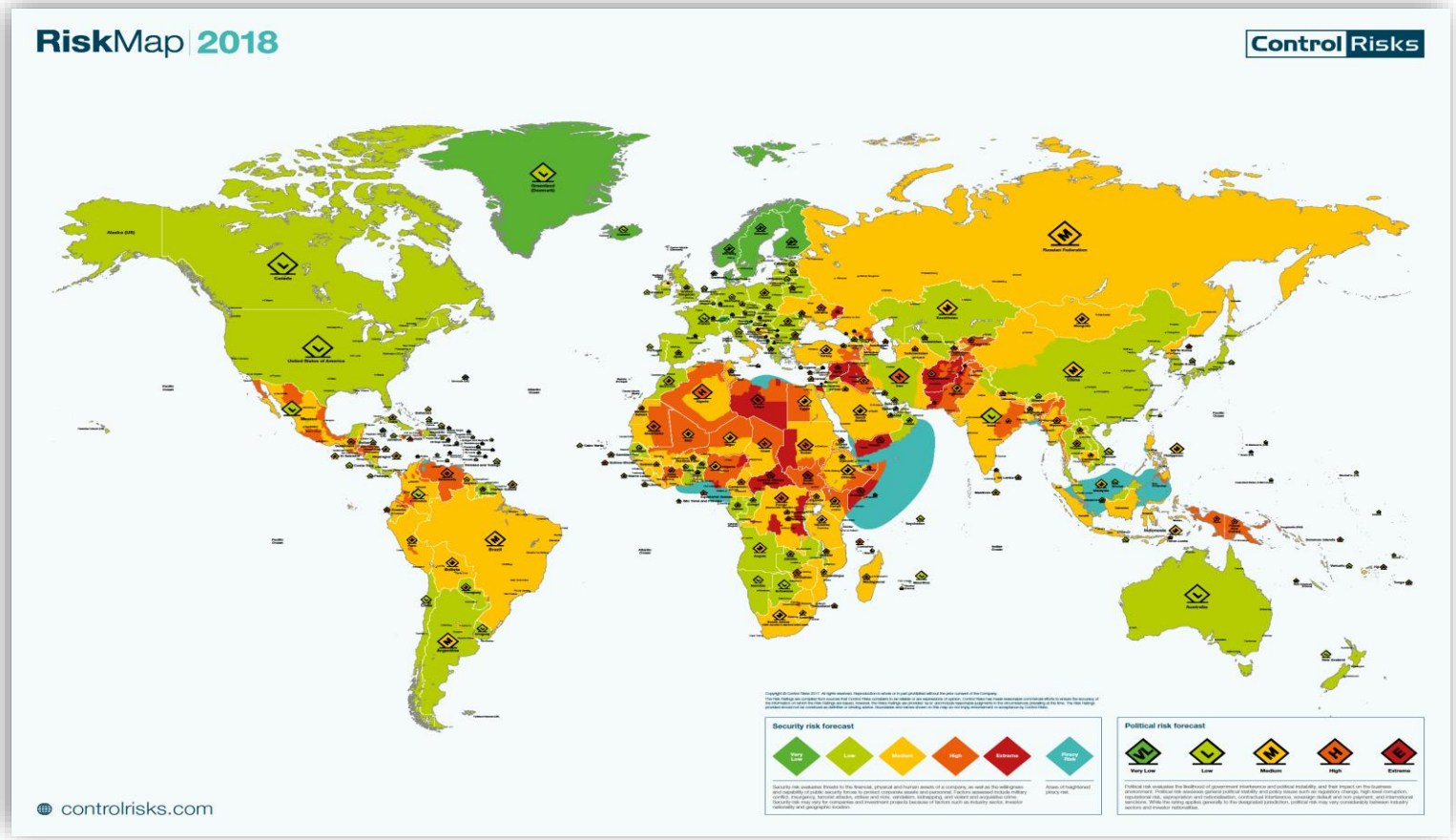
A covered person means any organization, entity, individual, or other person described in CFR section 1520.7. In the case of an individual, covered person includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered person includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in section 1520.7. According to the CFR 1520.7, “covered persons” may access SSI. These include Airport and Airline Officials, Maritime Operators, Federal Employees, Vendors, Contractors, and Grantees, among others, subject to the requirements of section 1520.

Security Responsibilities of Employees and other personnel

No person may:

- Tamper or interfere with any TSA security systems , measures or procedures
- Enter or be present within a secure area without complying with TSA procedures
- Use or allow to be used any airport ID in any other manner than that for which it was issued
- Allow unauthorized access to restricted areas

Security Updates and Threat Level
2020 Terrorism & Political Violence Map



Threat: What is the relationship between Threat, Vulnerability and Risk?

- Threat: The probability or possibility of an attack against a target in particular. It is defined as the probability of an attack is attempted against a target within a specific time frame. Threat is 'owned' the attacker's, we cannot control it.
- Vulnerability: Is defined as those characteristics of a target that could be exploited in an attack. We are owners of this and we can control it.
- Risk: A measure of probability that an attack will be attempted and that will succeed in exploiting the targets Vulnerability.

PAN AM FLIGHT 103

Previous Threats to Aviation

- In December of 1988, a Pan American Airways.
- On April 7, 1994, Federal Express Flight 705 (Auburn Calloway)
- In September of 2001
- In September of 2003, Mr. Charles McKinley
- In December of 2005, TSA at John F. Kennedy International Airport (New York) found multiple gun parts hidden inside several computer laptops. While checking a passenger's bag using the X-ray

Threat Incidents

- Yemen Toner Cargo bombs October 2010
- JFK bomb plot convictions August 2010
- Osama Bin Laden Killed May 2011
- Bomb found on Libyan Airlines Jan 2012
- Us Embassy Libya September 11, 2012
- Underwear Bomber December, 2009

FedEx
Federal Express

Threat Incidents

Shipment of Personal Effects containing the second–hand printer

The Printer Cartridge & Circuit board

Lead Azide in Detonator

300-400g of PETN

What is Terrorism?

The unlawful use of force and violence against persons or property to intimidate a government and/or the civilian population in order to achieve a political, religious, or ideological goal.

- Premeditated - to think out or plan (an action, especially a crime) beforehand.
- Political - motivated or caused by a person's beliefs or actions concerning politics

The below are some troubling terror stats:

- 2001: September 11 - 2996 persons were killed (Most Deaths).
- 1988: PAN AM Flight 103 - approx. 300 Deaths.
- 1998: East Africa Embassy bombing also around 300 Deaths.
- 1995: Oklahoma City bombing around 166 Deaths.
- 1993: First World Trade Center attack, killing 6 people and around 1000 injured.

Based on all of these events should you be concerned?

- Brussels Airport bombing - 32 killed, 300 injured.
- Paris terror attack - 130 killed.
- Orlando terror shooting - 49 killed, 53 injured.
- San Bernardino shooting - 14 killed, 22 injured.

September 11, 2001

19 hijackers on 4 aircraft carrying 213 passengers, 25 flight attendants, and eight pilots. They carried legal instruments: box cutters and homemade knives fashioned with blades shorter than the FAA limit of 4 inches. Conducted practice runs, videotaped crew routines and even rode in cockpit ''jump seats'' usually reserved for legitimate airline pilots.

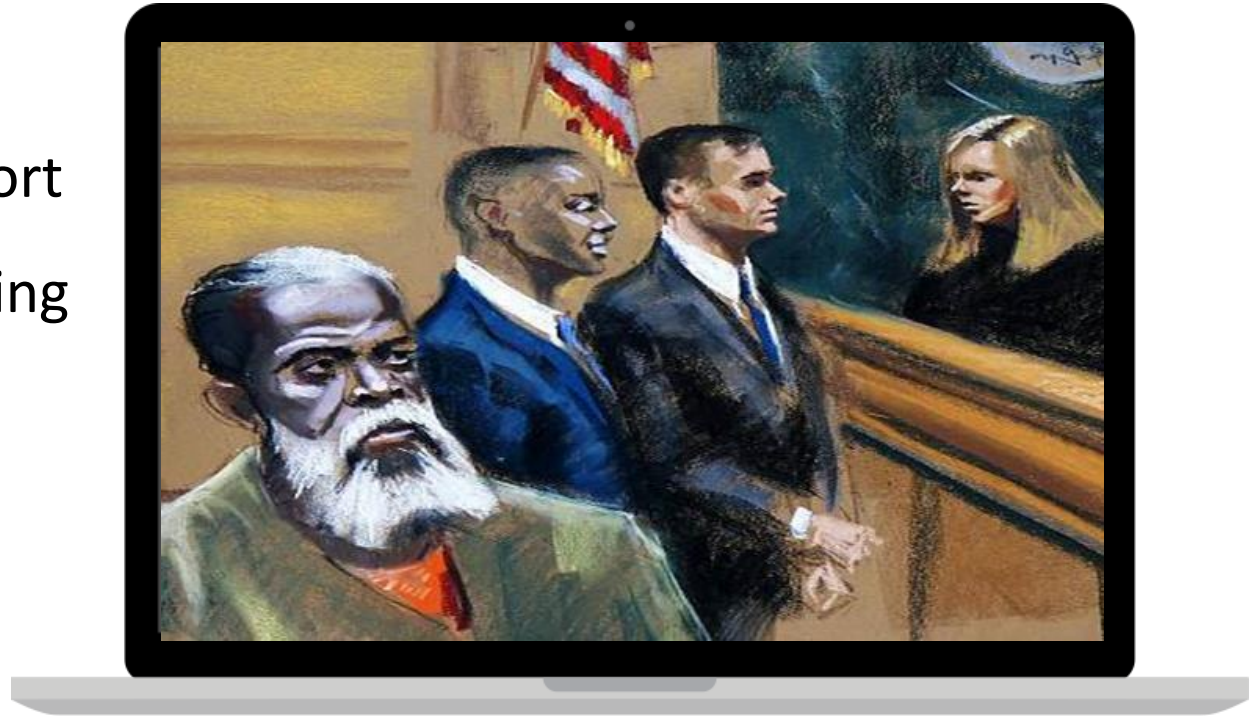
- Two years in the planning.
- Four countries where subjects were involved.
- 0759-0810-0814-0843 Less than one hour.
- Taken from three different states.

What signs would make you seem suspicious?

- People hanging around outside the premises
- Cars left in the car park or wrong place
- People asking about the security measures
- People taking pictures
- Customer behavior (reluctance to allow screening, undue concerns)
- Discrepancies in the cargo paperwork
- Signs of tampering with the packages
- Broken seals on vehicles or containers

JFK Bomb Threat 2007

- Attempt to blow up JFK fuel storage/buildings:
- Russell De Freitas, 67, worked at the airport
- Kadir was an engineer Advantages of having an engineer and airport employee involved?
- Currently serving life sentences



Organizations who may pose a 'Threat' to Civil Aviation.

- Terrorists
- Political Groups
- Religious Groups
- Environmental Groups

Individuals who may pose a 'Threat' to Civil Aviation.

- Criminals
- Politically motivated people
- Mentally ill
- Those with revenge motives

In 2011 DHS has replaced the color coded threat advisories with the National Terrorism Advisory System (NTAS).

- ALERT Bulletins – Elevated or Imminent
- Summary — Duration
- Details — Affected Areas
- How You Can Help — Stay Prepared — Stay Informed

New Updates Security Program

- Model Security Programme – Updates
- All-Cargo International Security Program - Updates

MSP – Updates 2020

6/24/2020

Change 46: Creates a new screening document, the Standard Screening Procedures for Air Cargo (SSPAC), and implements corresponding changes to each respective TSA Standard Security Program. Removed the cargo screening attachments from the MSP and consolidates the existing cargo screening procedure attachments into a single document to serve as a central cargo screening attachment.

Effective date: September 7, 2020

ACISP – Updates 2020

6/24/2020

Change 8 creates a new screening document, the Standard Screening Procedures for Air Cargo (SSPAC), and implements corresponding changes to each respective TSA Standard Security Program. Removed the cargo screening attachments from the ACISP and consolidates the existing cargo screening procedure attachments into a single document to serve as a central cargo screening attachment.

Effective date: September 7, 2020

Identification of Valid Forms of ID

Valid forms of Identification from Shippers

ID Check

- ID information to be held on station for 30 days from uplift of cargo date & available to TSA
- Unauthorized disclosure of the ID information is strictly prohibited
- When ID requirements are not met, reject the cargo. If cargo is rejected because we believe there was an attempt to provide false information or ID, we must immediately notify:
  - SSR, LEO, IIR and TSOC
- Advise above if there is other cargo on the premises from same shipper

Valid Forms of ID

- At the time of acceptance we must request valid photographic ID issued by the federal government
- The ID must be examined to confirm that it is authentic and must verify the identity of the individual
- ID information must be annotated on the ID check form and to be held for at least 30 days from date of uplift

Valid Form of Identification

At the time of acceptance we must request a valid ID from each individual tendering cargo for transport. An expired ID is not valid for this check. Only the following two options are deemed valid forms of ID.

- Option 1: A photo ID issued by a government authority or a SIDA ID media issued by an airport operator within the United States. The air carrier representative must verify the ID is a true representation of the individual tendering cargo.
- Option 2: Two other forms of ID, at least one of which must be issued by a government authority. ---

ID Verification Form

All boxes must be completed.

The terms “none” or “N/A” must be used to indicate information not required or applicable.

No spaces may be left blank

Air Waybill Number_____

Type of first ID reviewed:			
Matching photo on ID? Indicate:	Yes	No	
Type of second ID reviewed (if the first was not a photo ID issued by a government authority):			
Matching photo on ID? Indicate:	Yes	No	N/A
Printed name of individual from whom the cargo shipment was accepted:			
Company name (where applicable):			
Name of foreign air carrier employee or authorized foreign air carrier representative who verified ID information:			

Fraudulent or Intentionally False Statement

No person may make or cause to be made any fraudulent or intentionally false statement regarding :

- Application for any TSA security program or ID medium;
- Any record or report that is kept, made or used to show compliance with TSA requirements;
- Any reproduction or alteration of any report, record, security program, access or ID medium under TSA regulations.

It is a crime to falsify, conceal or make a false statement regarding these matters, subject to fines or up to 5 years; imprisonment, 8 years if terrorism is involved, or both.

HOW TO HANDLE SENSITIVE SECURITY INFORMATION:

MARK IT	• using the header and footer.
LOCK IT	• whenever not using SSI material.
SHARE IT	• only with covered persons that has a need to know.
SHRED IT	• when destroying SSI use a cross-cut shredder.

Confidentiality of Personal Information

Choice Aviation Services policy is that only a MANAGER is to transmit SSI information by e-mail to an authorized receiver.

Managers NOTE: 2 separate emails are to be sent one that contains the requested document which is password protected and a second email only containing the assigned password.

Passwords must be sent separately and should:

- Be at least eight characters in length;
- Contains at least one letter capitalized;
- Contains at least one number;
- Contains at least one special character.

Instructions on how to lock a file

These steps will work with the tools we currently use in Microsoft (Word,Powerpoint)

1. Click File
2. Click Save as Adobe PDF
    1. Check the box "Restrict Editing"
    2. Check the box "Require a password to open the document"
    3. Type the password desired under "Document Open Password"
    4. Uncheck the box under Permissions "Restrict editing and printing of the document"
    5. Click Ok
    6. Retype the password for confirmation in the propmt.
    7. Click Ok
3. Type the file name
4. Click Save

This will ensure any user will have to enter the password to view the file.
If you have any questions, contact your superior or IT department.

HOW TO HANDLE SENSITIVE SECURITY INFORMATION:

When not under direct control or when you are not using SSI records such as: (on lunch break, or at the end of your shift etc.) Always store SSI record in a locked desk drawer or in a locked room to prevent unauthorized access by person who does not have a “need to know”.

Taking SSI home is not recommended however, if taking SSI out of the office is necessary, employees SHOULD have the permission of their supervisor.

Discussing SSI in public areas is not recommended

All personnel must be very careful when discussing SSI in public areas.
You never know who is listening, and not everyone has a " need to know" the information.
Terrorist could use the information to plan an attack, terrorist do not care how or where they receive SSI, as long as they have the information they need to plan an attack.

EVERYONE IS RESPONSIBLE FOR PROPERLY MARKING, HANDLING,PROTECTING, STORING, AND DESTROYING SSI.

Consequences of unauthorized disclosure of SSI:

- Loss of lives – terrorists could use the information they receive to plan an attack.
- Loss of job – for federal employees or personnel with access to SSI, there may be a letter of reprimand, suspension, or even dismissal, depending on the circumstances.
- Loss of money – the government can impose a civil penalty per offense.

What is a Security Threat Assessment (STA)

An STA consists of a background check against federally maintained databases to establish any link to terrorism. Persons required to undergo an STA includes but not limited to:

- Persons obtaining an airport issued ID granting them access to the secure area.
- CCSF employees and owners.
- Persons with unescorted access to cargo.

Security Threat Assessments for Cargo Personnel in the US

Each individual who has unescorted access to cargo and access to information that such cargo will be transported on a passenger aircraft: or who has unescorted access to cargo that has been screened for transport a passenger aircraft; or who performs certain functions related to the transportation, dispatch or security of cargo for transport on a passenger aircraft or all-cargo aircraft, as specified in the foreign aircraft operators or foreign air carriers security program. Must have an STA before performing any functions directly to any of the job functions listed above.---

The following is an alternative/ equivalent for a security threat assessment:

- Commercial Driver's License with HAZMAT endorsement.
- Current FAST Driver's Card.
- Current Transportation Worker Identification Credentials (TWIC).
- SIDA Badge.

Security

The TSA has established security requirements for cargo and mail acceptance on passenger and cargo aircraft. These requirements ensure that cargo and mail, from any source, will undergo appropriate security measures before being loaded on a passenger aircraft. This module is designed to provide you with the skills needed for all aspects of cargo and mail security, including your responsibility concerning security awareness.

The Purpose of Access Control & Cargo Protection

- To ensure only authorized people and vehicles gain access to areas where cargo is subjected to security controls
- To protect Cargo from unauthorized interference
- To permit entry by persons who have a legitimate right of entry, providing they are on duty

Access Control

Correct procedure for checking a Pass

1. Take the pass from the person presenting it
2. Check that it is valid
3. Compare the photograph with the holder. A good representation
4. Check for alterations and any tampering.
5. Put the pass through the automated checking system if applicable to check granted access.

Data Confidentiality

- All staff need to be conscious and respectful of the fact that personal identification information collected is sensitive and that unauthorized disclosure is prohibited.
- Where release would constitute an invasion of privacy in accordance with 49 CFR Part 1520 Penalties for the release of such information are covered in CFR title 49

Shippers Security Endorsement

Shipper’s Security Endorsement (SSE)

Shipper's Security Endorsement (SSE)

- The foreign air carrier must ensure the SSE contains the language and information outlined below and that each question or request for information is addressed or acknowledged and no spaces remain blank. The terms "none" or "N/A" must be used to indicate omitted information.
- The required SSE and ID information may appear on any document (for example, an air waybill or Shipper's Letter of Instruction) associated with the cargo shipment being offered by the shipper.
- The foreign air carrier must obtain a copy of the SSE and ID information with every applicable cargo shipment.
- The foreign air carrier must maintain all required SSE and ID information at the accepting station for a minimum of 30-calendar days from the date the cargo was transported from the accepting station and make them available to TSA upon request.

Shippers Security Endorsement

"I certify that this cargo does not contain unauthorized explosives, incendiaries, or other destructive substances or items. I am aware that this endorsement and original signature and other shipping documents will be retained on file for a minimum of 30 calendar days."

Shipper's name:	*Date:*
Shipper's Address:	*Telephone:*
Air waybill number:	
Signature of shipper or authorized foreign air carrier representative tendering the cargo: *Print/type name of individual whose signature appears as shipper or authorized foreign air carrier representative:*	

+

Air Waybill Number_____

Type of first ID reviewed:			
Matching photo on ID? Indicate:	Yes	No	
Type of second ID reviewed (if the first was not a photo ID issued by a government authority):			
Matching photo on ID? Indicate:	Yes	No	N/A
Printed name of individual from whom the cargo shipment was accepted:			
Company name (where applicable):			
Name of foreign air carrier employee or authorized foreign air carrier representative who verified ID information:			

Accepting and Transferring Cargo

Accepting and Transferring Cargo

Accepting Cargo - From any person

- Inspect cargo for signs of tampering, modification and other suspicious conditions.
- Collect ID information from the individual delivering the cargo.
- Any signs of tampering or modifications must be resolved prior to transport.
- Upon discovering cargo which has been tampered with, modified or appears suspicious:
    - Do not transport the cargo, maintain positive control of the cargo
    - Notify the appropriate authorities

Screening at US Stations

- The US government passed a law, know as HR1, requiring 100% screening of cargo uplifted on passenger aircraft from August 2010. All cargo must be screened.
- Screening will be done by shippers, agents and airlines – massive investment required in screening equipment.

Certified Cargo Screening Program

Accepting Cargo – from Another Passenger Airline

- Obtain written Airline Certification stating – All cargo is from a Known Shipper or Unknown Shipper according to TSA Requirements
- Ensure the carrier appears on the current TSA Monthly Master List and the certificate is signed and dated by the Airline Representative
- Ensure the Certificate is kept on file for 30 days from uplift and made available to the TSA
- We can transport cargo, although originated from an Unknown Shipper, when it contains:
- AVI (Live Animals) Human Organs, blood, Diagnostic Specimens, life saving drugs.
  - The Cargo contents must be listed and the Shipper should be of an affiliated institution such as a hospital, research institute.

Accepting Cargo - From an All-Cargo Airline

- The all-cargo airline must operate under the ACISP or Full All-Cargo Aircraft Operator Standard Security Program
- Check that the all-cargo airline appears on the Current TSA Monthly Master List which is issued monthly list or secure written proof that the airline has implemented a TSA approved program
- Can only accept Known Shipper cargo from them under MSP. Otherwise it must go on freighter. Obtain a dated & signed written airline certification on shipment acceptance & keep it on station for 30 days from uplift.

Accepting Cargo - From a Known Shipper

- Known Shippers status must be confirmed using the Known Shipper Management System (KSMS) or the Manual Method
- Airlines makes Shippers Known according to the TSA MSP standards
- The Known Shipper or its authorized representative must tender the cargo to us.
- Alternatively, airlines authorized representative must collect the cargo from the Known Shipper's facility under certain conditions

Accepting Cargo - From an Unknown Shipper

- Obtain fully completed SSE for each shipment
- Only accept the cargo from an Unknown Shipper authorized to ship according to regulations & transport it on a Passenger Aircraft if there is ID and SSE
- Obtain the ID information following the measures for each shipment
- Keep SSE & ID information on station for 30 days from uplift

Accepting Cargo - From an Indirect Air Carrier (IAC)

- Determine the IAC appears on the current TSA Monthly Master List which is updated monthly
- Obtain the written, dated & signed IAC certification & ID check for each shipment accepted. Keep on file for 30 days from uplift
- Determine that the IAC either appears on the current TSA Monthly Master List or secure written proof (current approval or re-approval letter) that they have adopted & implemented a TSA-approved program.

Accepting Cargo For transport or transfer to another Passenger Airline

- Determine the air carrier or aircraft operator appears on the Current TSA Monthly Master List which is updated monthly.
- We may accept and transfer cargo originating from another TSA-approved entity
- Must provide other airline with dated & signed Airline Certification when transferring shipment
- For human organs etc we must also - verify details from the institution; keep a record of the contact; & maintain the record for 30 days from uplift
- We can accept & transport, or transfer, cargo originating from an Unknown Shipper to another passenger airline when it contains:
- AVI (Live Animals), Human Organs, blood, Diagnostic Specimens, life saving drugs
- The Cargo contents must be listed and the Shipper should be of an affiliated institution such as a hospital, or research institute

Accepting Certified Cargo Screening Facility (CCSF) Cargo

Verify that the entity tendering CCSF-screened cargo appears on the TSA-approved Monthly Master List

- from a CCSF directly or from a CCSF that is also an IAC. (Verification of under approved CCSFs)
- from an IAC authorized to tender another entity's screened cargo (Verification under 001 Amendment is required)

Cargo must arrive on Secure Conveyance – Locked, sealed or escorted

- Chain of custody procedures must be verified for each conveyance transporting CCSF-screened cargo
- When CCSF-screened cargo is transported in a conveyance with an escort or lock. Verification of the Tamper-Evident Technology on the largest level of configuration is required.
- When the tamper-evident numbered seal is missing or broken or the escort cannot be verified for the conveyance., and there is no TET used at the configuration level, the foreign air carrier must not consider the cargo as screened
- Verification that the screened cargo has a screened cargo identifier affixed to the largest configuration (for example, screened ULD pallet, ULD container, skid, or piece containing
- screened cargo) is required. NOTE: Verification of SCIs on pieces or skids within a ULD is not required
- When none of the screened cargo identifiers can be verified, the foreign air carrier must not consider the cargo as screened

Documentation must be fully completed with the appropriate CCSF Certification Statement and maintained on file for a minimum of 30-calendar days

Please see workbook for examples

Accepting Diplomatic Pouches

Identifying a valid diplomatic pouch: Verify that item is properly marked as a diplomatic pouch. If all the following features are not present, the item is not a valid diplomatic pouch and it must not be accepted for transport.

1. The exterior of the pouch, bag, envelope, crate, or container must have readily visible markings that clearly identify it in English as a “Diplomatic Pouch.”
2. The pouch must externally bear the official seal of the government or public international organization sending the pouch. This may be a lead or plastic seal attached to a tie that closes the bag or a seal affixed to the exterior of the pouch.
3. The pouch must be addressed to a government ministry or department of foreign affairs, embassy, legation, or consular post, or to the headquarters or offices of a public international organization.
4. When applicable for unaccompanied pouches, all associated shipping documents, such as bills of lading and air waybills, should describe the shipment in English as a “Diplomatic Pouch.”

Diplomatic Pouch Acceptance Guide

Sensitive Security Information
Diplomatic Pouch Acceptance Guide

AWB: _____

Checked By:

_____

Identifying a valid diplomatic pouch: Verify that item is properly marked as a diplomatic pouch. If all the following features are not present, the item is not a valid diplomatic pouch and it must not be accepted for transport.

- **The exterior of the pouch, bag, envelope, crate, or container must have readily visible markings that clearly identify it in English as a "Diplomatic Pouch."**
- **The pouch must externally bear the official seal of the government or public international organization sending the pouch. This may be a lead or plastic seal attached to a tie that closes the bag or a seal affixed to the exterior of the pouch.**
- **The pouch must be addressed to a government ministry or department of foreign affairs, embassy, legation, or consular post, or to the headquarters or offices of a public international organization.**
- **When applicable for unaccompanied pouches, all associated shipping documents should describe the shipment in English as a "Diplomatic Pouch."**

<table>
<tr><th colspan="2">Unaccompanied Pouch(es) Accepted from the US Department of State</th><th>Unaccompanied pouch(es) accepted from a courier or representative of the sending government or international organization</th></tr>
<tr><td colspan="2">Unexpired ID Card Issued by the Department of State</td><td>Diplomatic Passport</td></tr>
<tr><td>Yes</td><td>No</td><td>Yes / No</td></tr>
<tr><td colspan="2" rowspan="3">Pouches tendered from the Department of State must be accompanied by a US Government transportation request or bill of lading that identifies the pouch(es) being tendered for shipment</td><td>Plus one of the following issued by the US Department of State
Driver's License, Protocol Identification Card or Diplomatic Tax Exemption Card
Yes / No</td></tr>
<tr><td colspan="2">Name of Bearer _____
ID number _____</td></tr>
<tr><td colspan="2">Pouches tendered from a courier or representative of the sending government must be accompanied by courier letter that meets the following criteria
(a) The document must be an original on appropriate letterhead and bear the seal of the sending government's ministry or department of affairs, or the headquarters or offices of a public international organization.
(b) The document must clearly identify the courier by name as either a diplomatic or nonprofessional courier for the government or public international organization sending the pouch.
(c) The document must list the courier's diplomatic passport number, unless the courier presents a U.S. diplomatic passport.
(d) The document must include the signature, job title, and telephone number of a responsible official of the sending government or public international organization
(e) The document must contain information that identifies the diplomatic pouch(es) being escorted and state the quantity and total approximate weight of the pouch(es), unless this information is provided on a separate document.</td></tr>
</table>

***For Unaccompanied Pouches accepted from Indirect Air Carriers or airlines ***

- Photocopies of the identification required in either of the two columns above **or** a statement to the fact that the ID was checked. The statement must contain the name of the bearer, name of issuing government agency or international organization and any ID number present.
- A copy of the US Government Transportation Request, bill of lading or courier letter listed in either of the two columns above

Diplomatic Pouch Acceptance Guide

Unaccompanied pouch(es) accepted from a courier or representative of the sending government or international organization

1 Required ID

Diplomatic Passport	
Yes	No
Plus, one of the following issued by the US Department of State	
Driver's License, Protocol Identification Card or Diplomatic Tax Exemption Card	
Yes	No

2 Pouches tendered from a courier or representative of the sending government must be accompanied by courier letter that meets the following criteria

(a) The document must be an original on appropriate letterhead and bear the seal of the sending government's ministry or department of affairs, or the headquarters or offices of a public international organization.

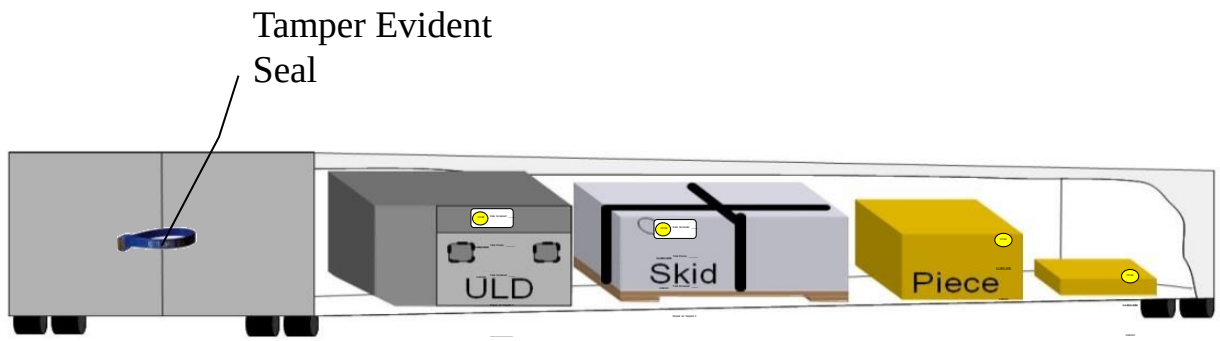
(b) The document must clearly identify the courier by name as either a diplomatic or nonprofessional courier for the government or public international organization sending the pouch.

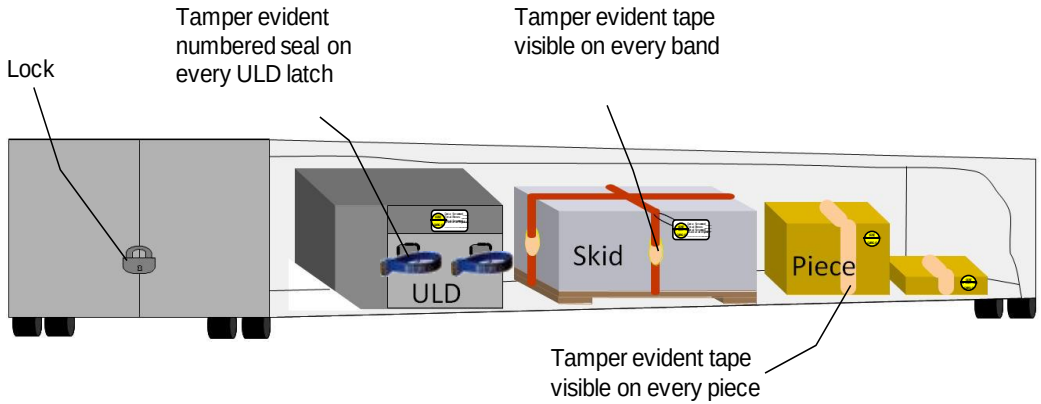
(c) The document must list the courier's diplomatic passport number, unless the courier presents a U.S. diplomatic passport.

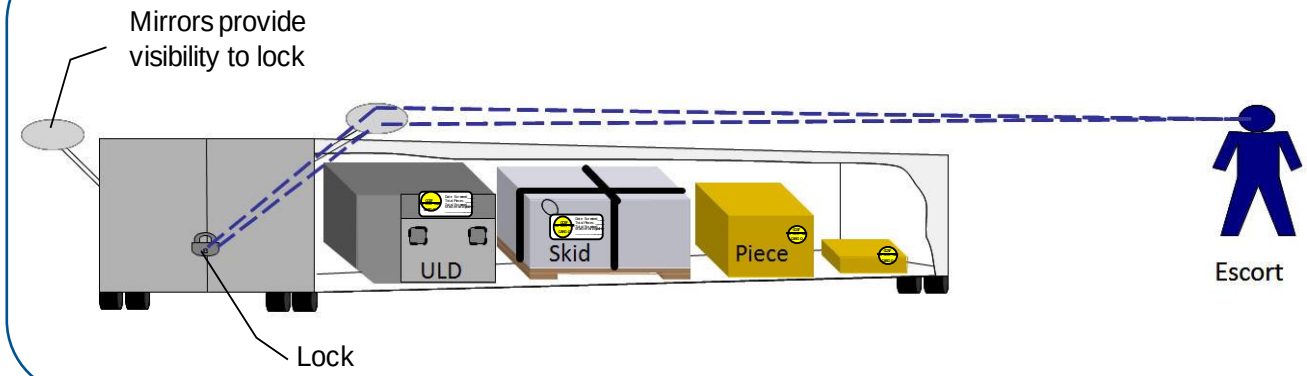
(d) The document must include the signature, job title, and telephone number of a responsible official of the sending government or public international organization

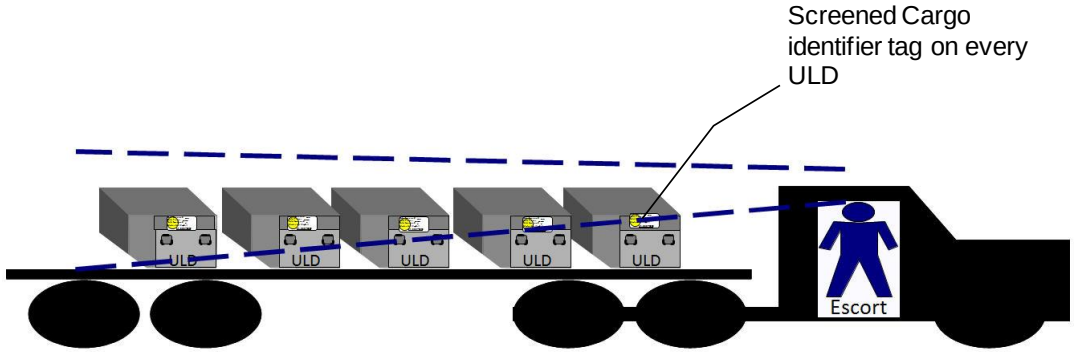
The document must contain information that identifies the diplomatic pouch(es) being escorted and state the quantity and total approximate weight of the pouch(es), unless this information is provided on a separate document.

CCSF - Acceptance Chain of Custody

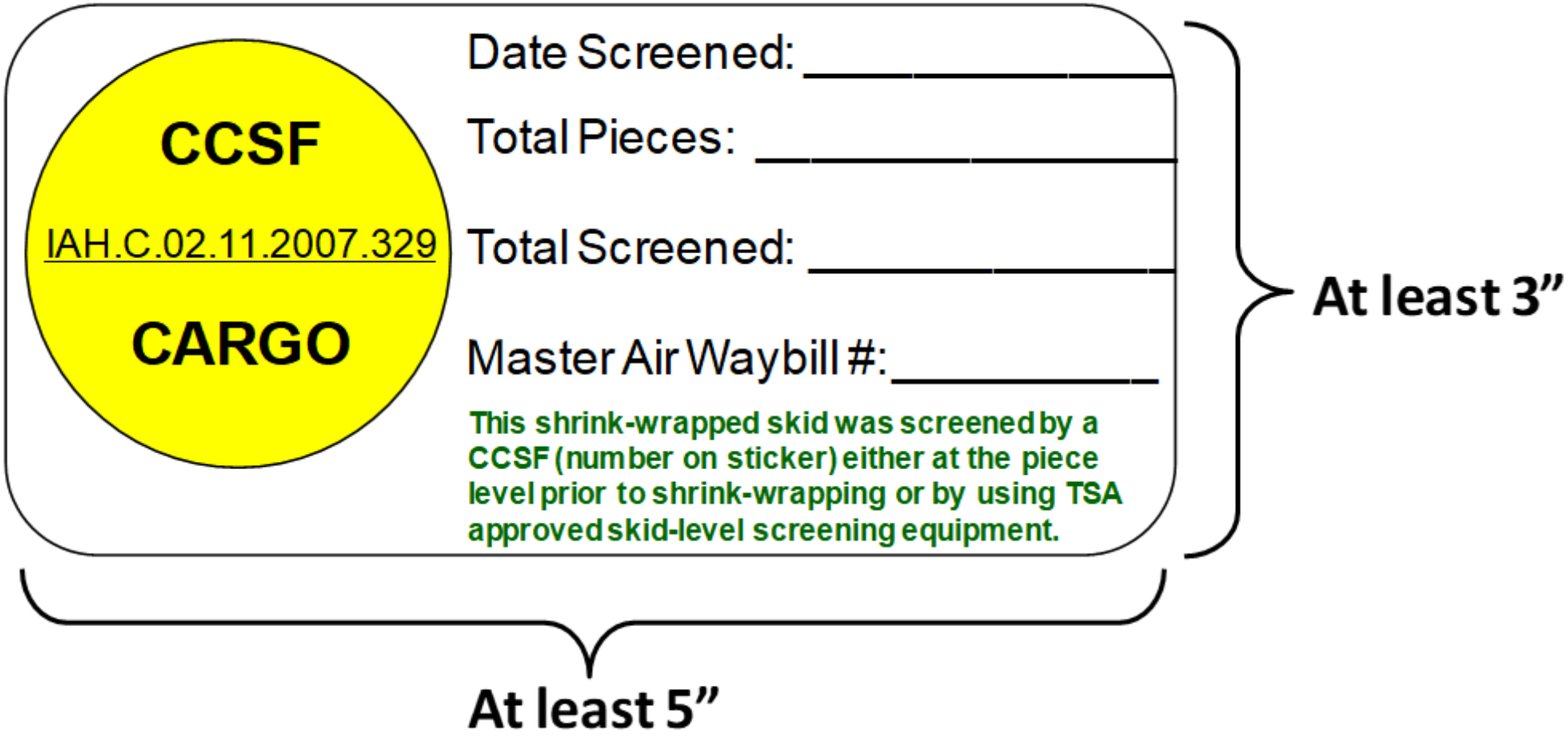




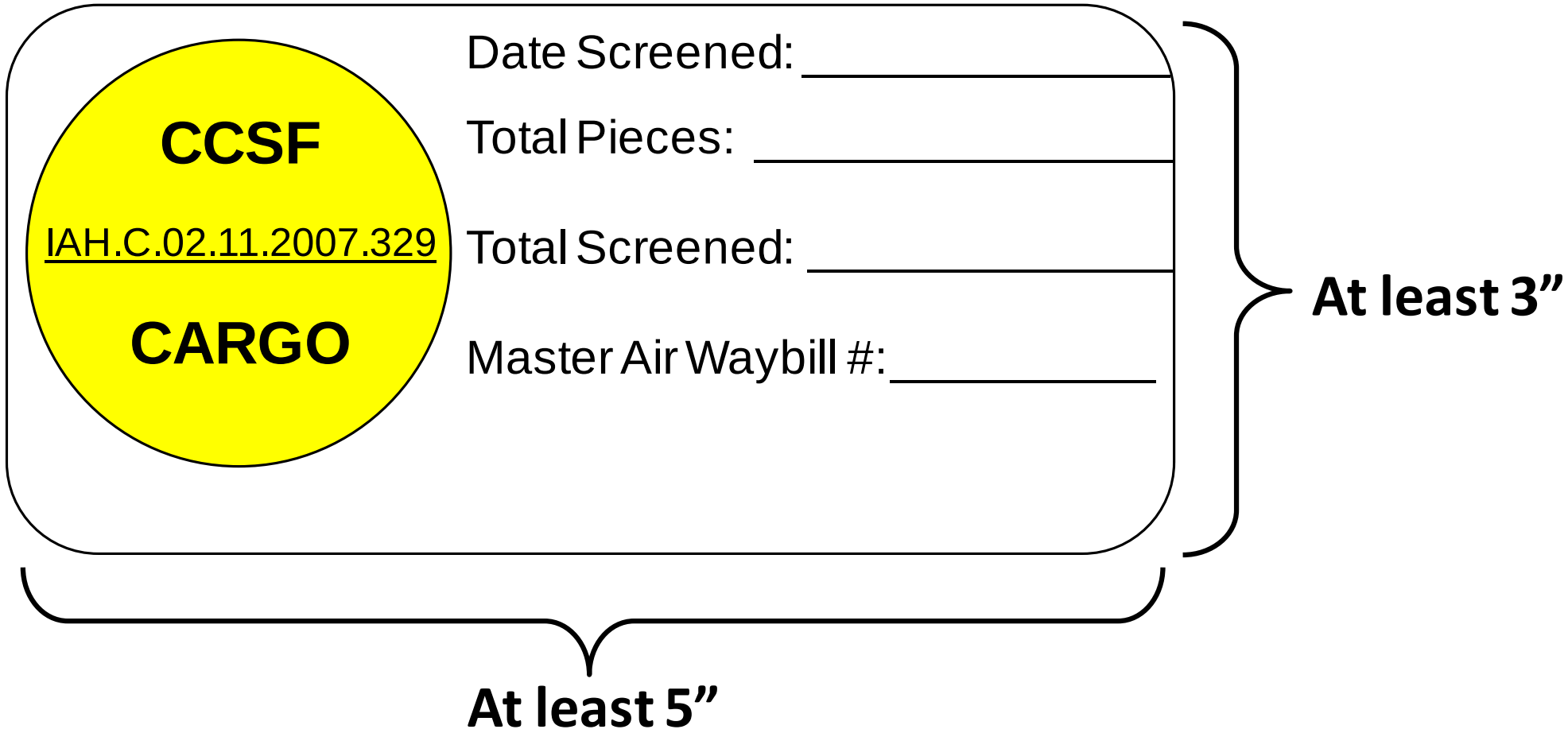




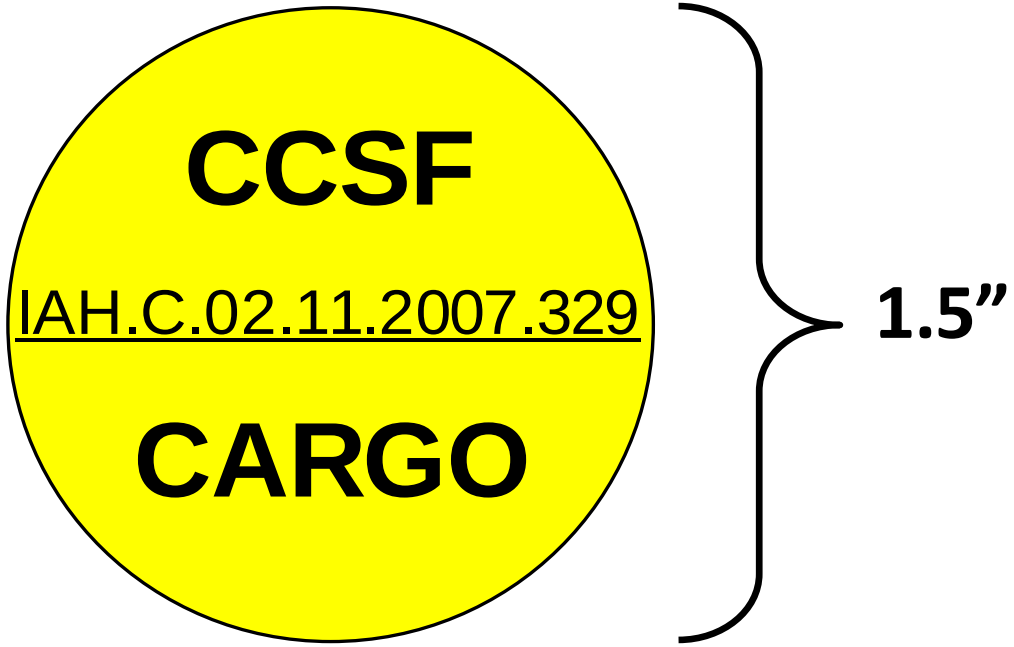
Accepting CCSF Cargo



Accepting CCSF Cargo



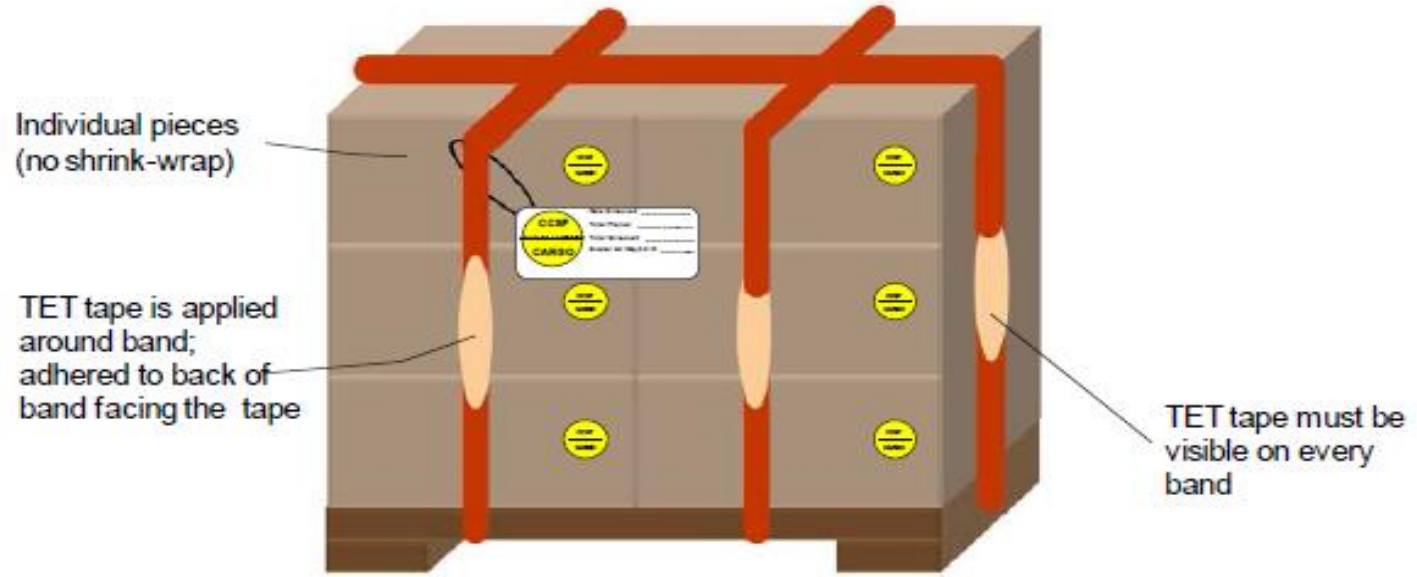
Accepting CCSF Cargo



Tamper Evidence Technology (TET)

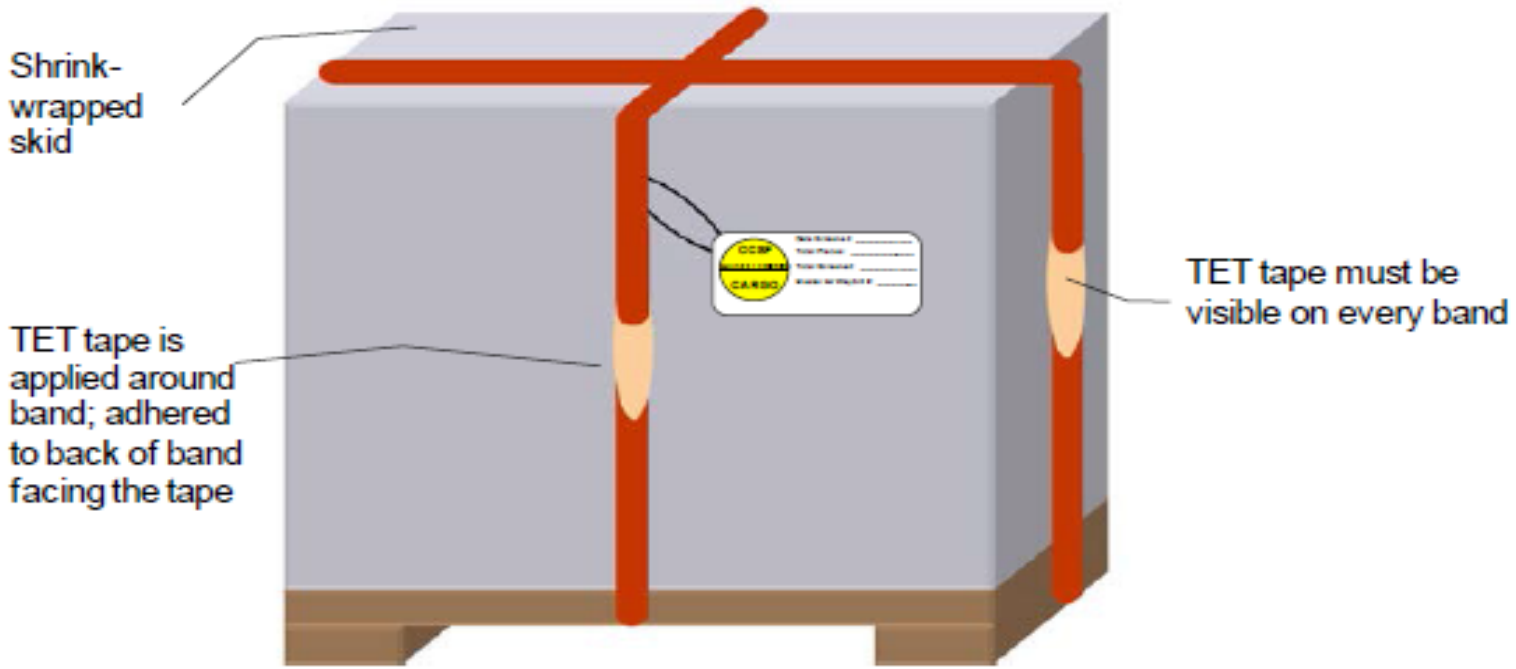
B. Skid, No Shrink-wrap

1. Bands must be used
2. TET tape must be applied on at least one side (not on top of the configuration) of each band to prevent removal of any piece
3. The screen cargo identifier tag must be fastened to a band (and not on top of the skid).



Tamper Evidence Technology (TET)

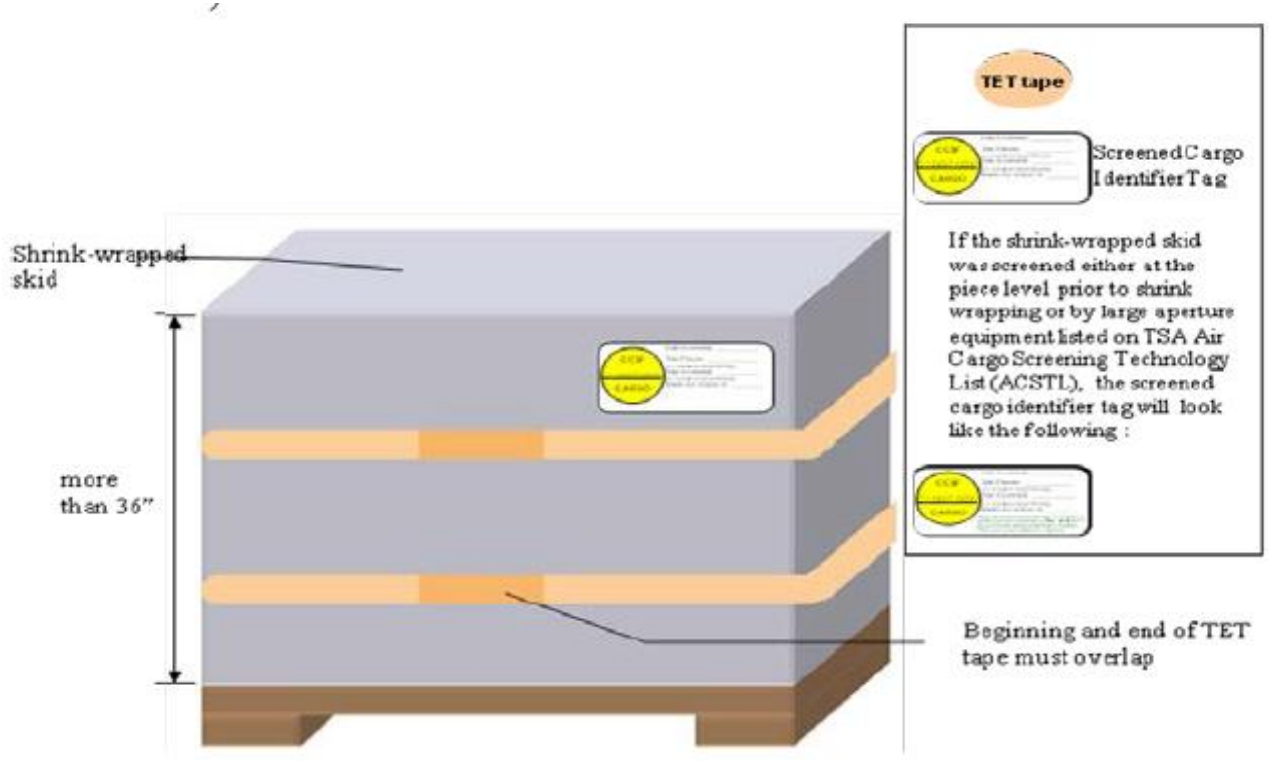
C. Skid, Shrink-wrapped, Using Bands in Lieu of Tape (Any Size Skid)
1. A minimum of one band per direction must be used.
2. TET tape must be applied on at least one side (not on top of the configuration) of each band.
3. The screened cargo identifier tag must be fastened to a band or applied to the shrink-wrap with adhesive (not on top of the configuration).



Tamper Evidence Technology (TET)

D. Skid, Shrink-wrapped, More than 36 inches

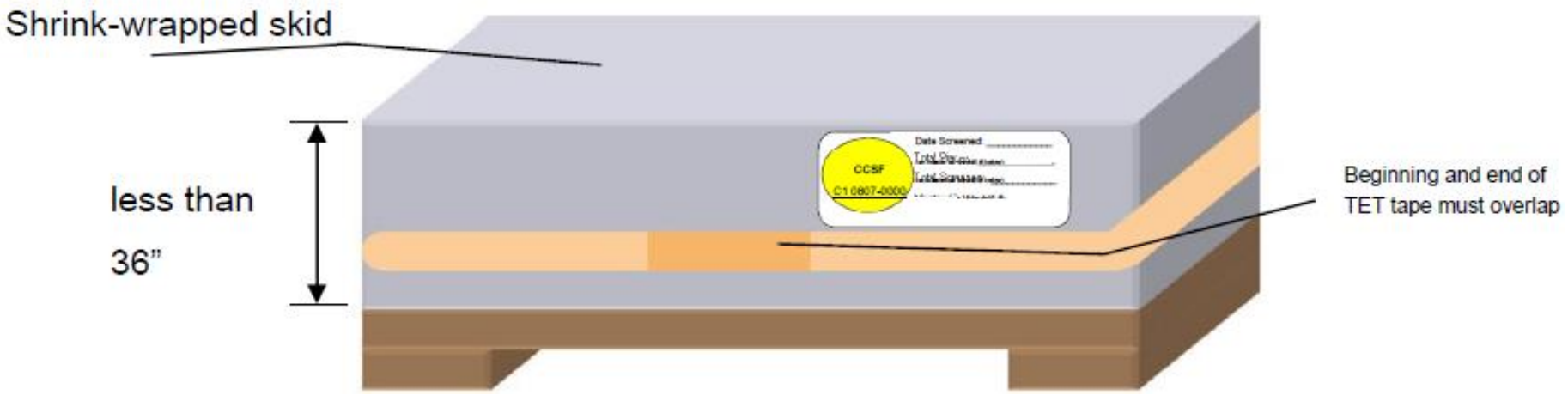
1. Must use a minimum of two full courses of tape, each course no more than approximately 12 inches from top to bottom of goods.
2. Must overlap beginning and end of TET tap
3. The screened cargo identifier tag must be applied to the shrink-wrap with adhesive (not on top of the skid).



Tamper Evidence Technology (TET)

E. Skid, Shrink-wrapped, Less than 36 inches

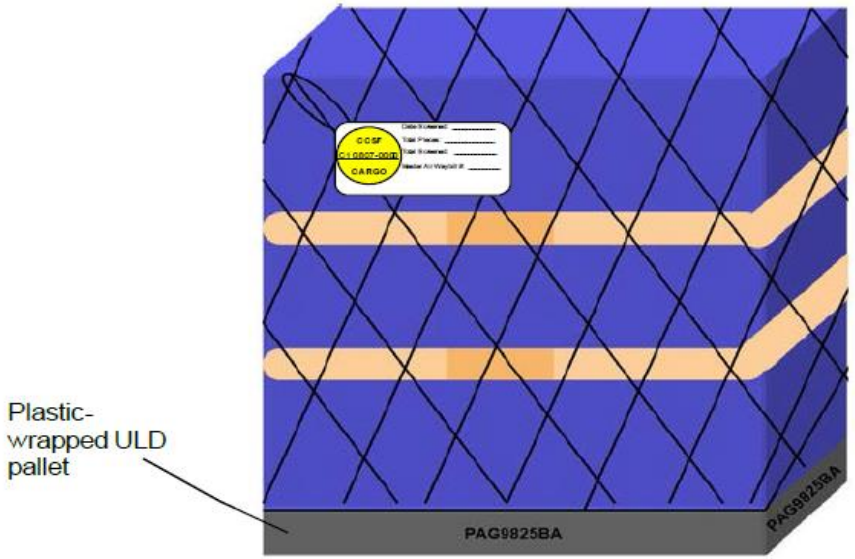
1. Must use a minimum of one full course of TET tape
2. Must overlap beginning and end of TET tap
3. The screened cargo identifier tag must be applied to the shrink-wrap with adhesive (not on top of the skid).



Tamper Evidence Technology (TET)

F. Netted ULD Pallet with Tamper-Evident Tape

1. Must use plastic wrap/vinyl covering (weatherproofing, not shrink-wrap material) under the netting and around entire shipment
2. Must use minimum of two full courses of tape, each course no more than approximately 12 inches from top or bottom of goods; tape must be over plastic and under netting
3. Must overlap beginning and end of TET tape
4. The screened cargo identifier tag must be fastened to the netting (not on top of the pallet).



Identification of Unauthorized Weapons, Explosive, Incendiaries and other destructive devices

Identification of Prohibited or Suspicious Items

IED Components

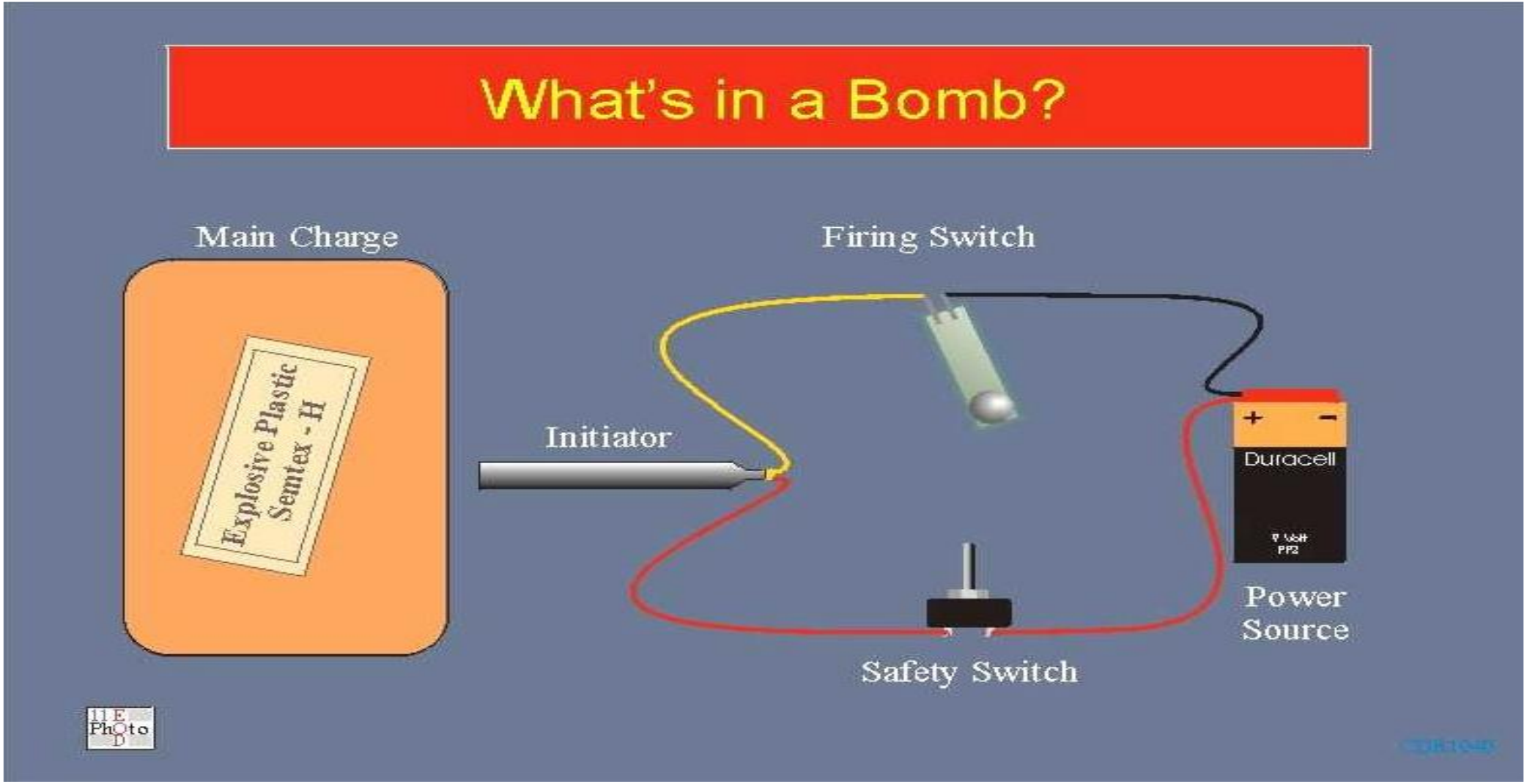
(Improvised Explosive Device)

- Explosive material (main charge) RDX
- Detonator (Initiator)
- Power source
- Timer/delay mechanism
- Wiring

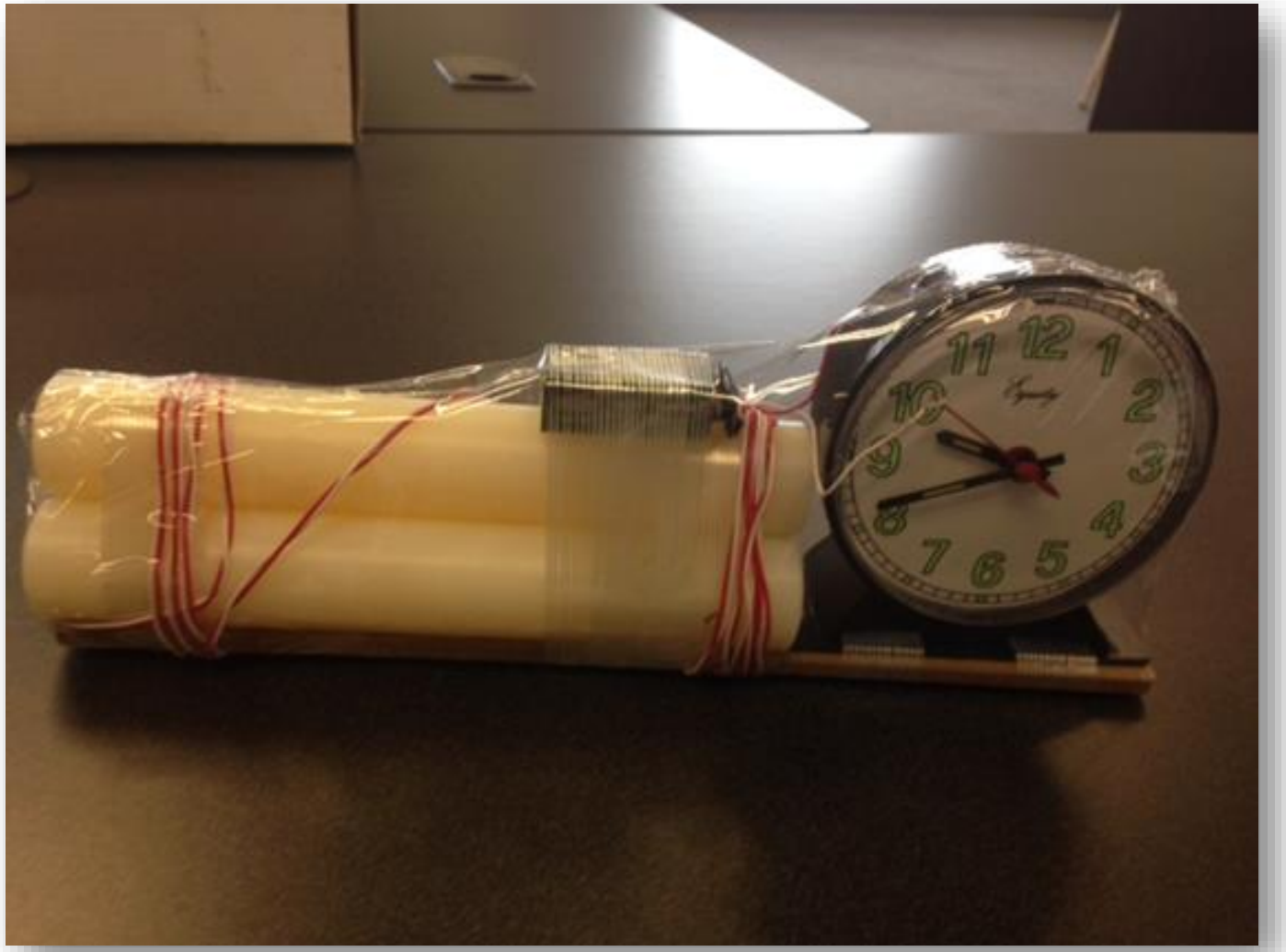
Explosive Groups

- Military or Plastic Explosive
  - PETN,
  - PE4,
  - RDX,
  - C4
  - Semtex
- Commercial Explosive
  - Dynamite (Greek for power)
  - Gelamex
  - Semtex
- Improvised (Home made) Explosives
  - Sugar/Weedkiller,
  - ANFO (Ammonium Nitrate with Fuel Oil)
  - TATP

An Improvised Explosive Device



Time Bomb

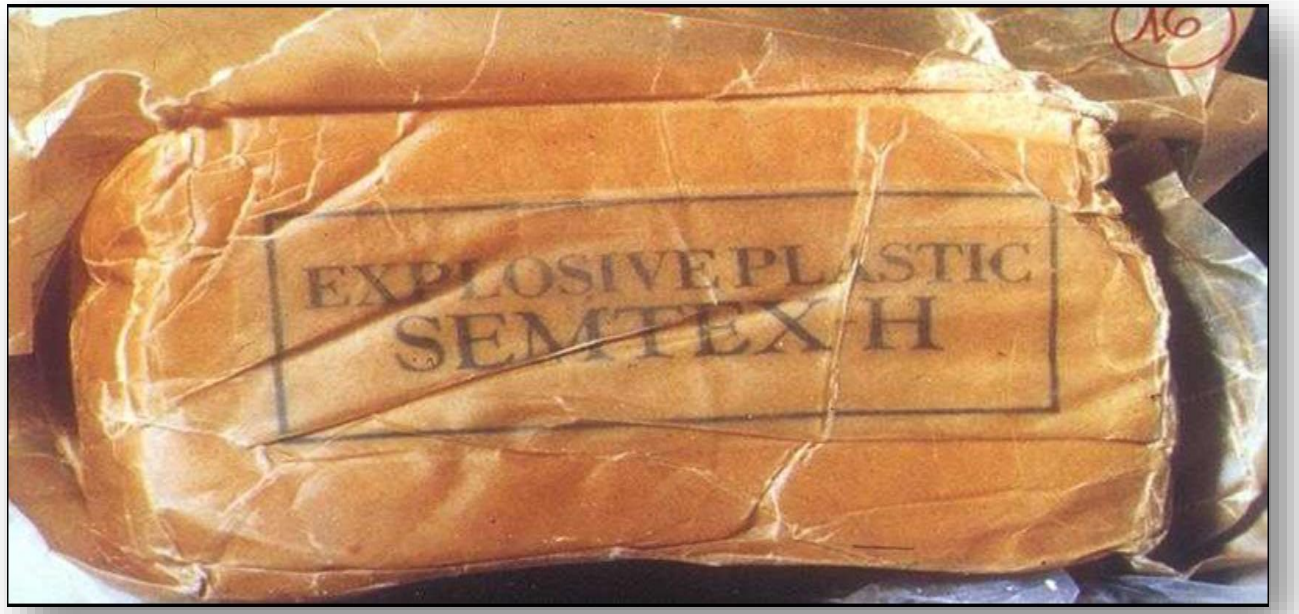


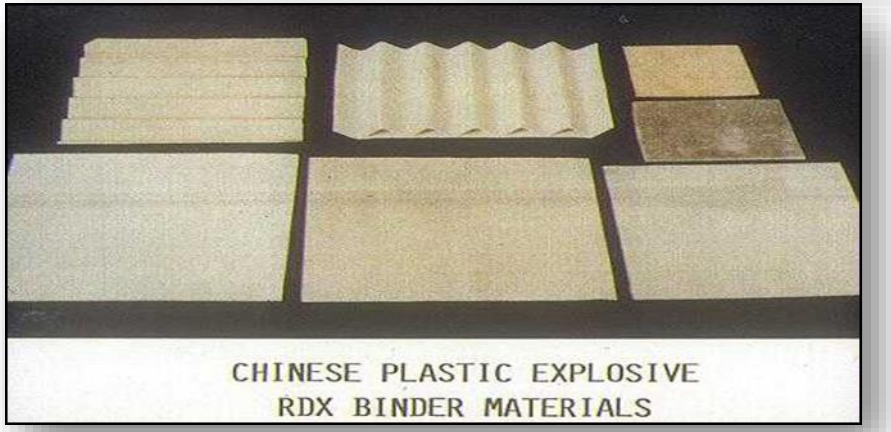
Hand Grenade

Is a small bomb that can be thrown by hand. A variety of types of hand grenades exists, the most common being explosive grenades

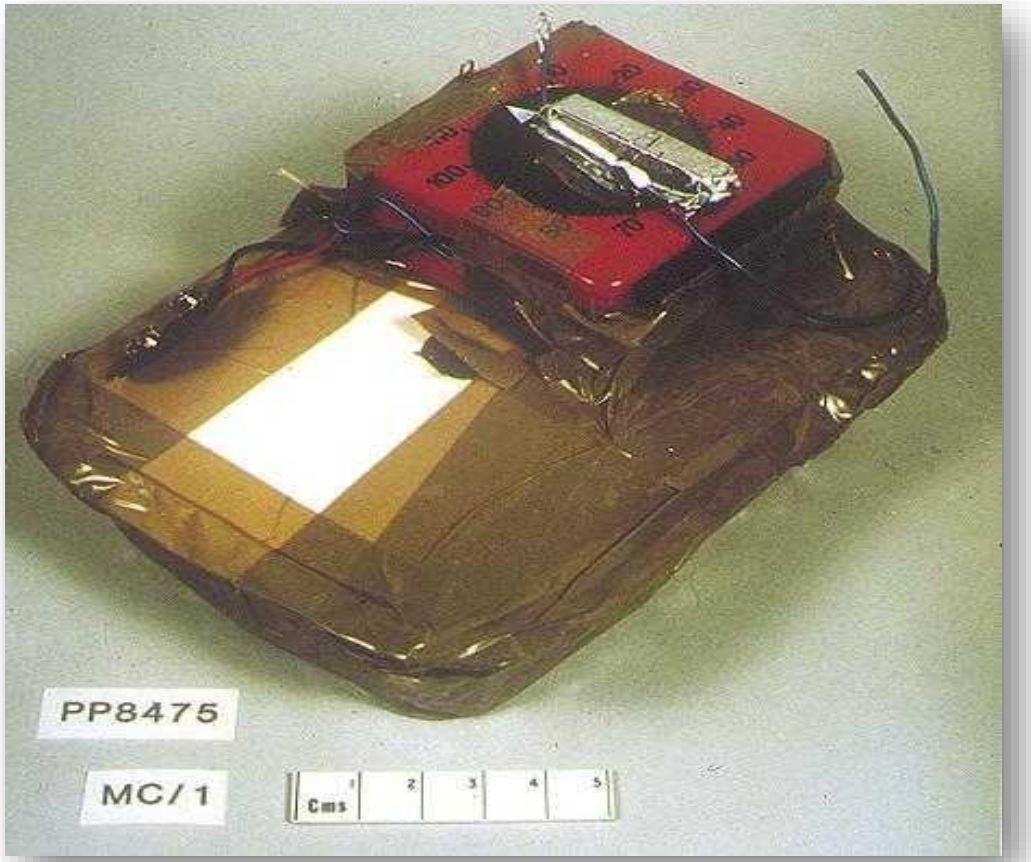
Pipe Bomb

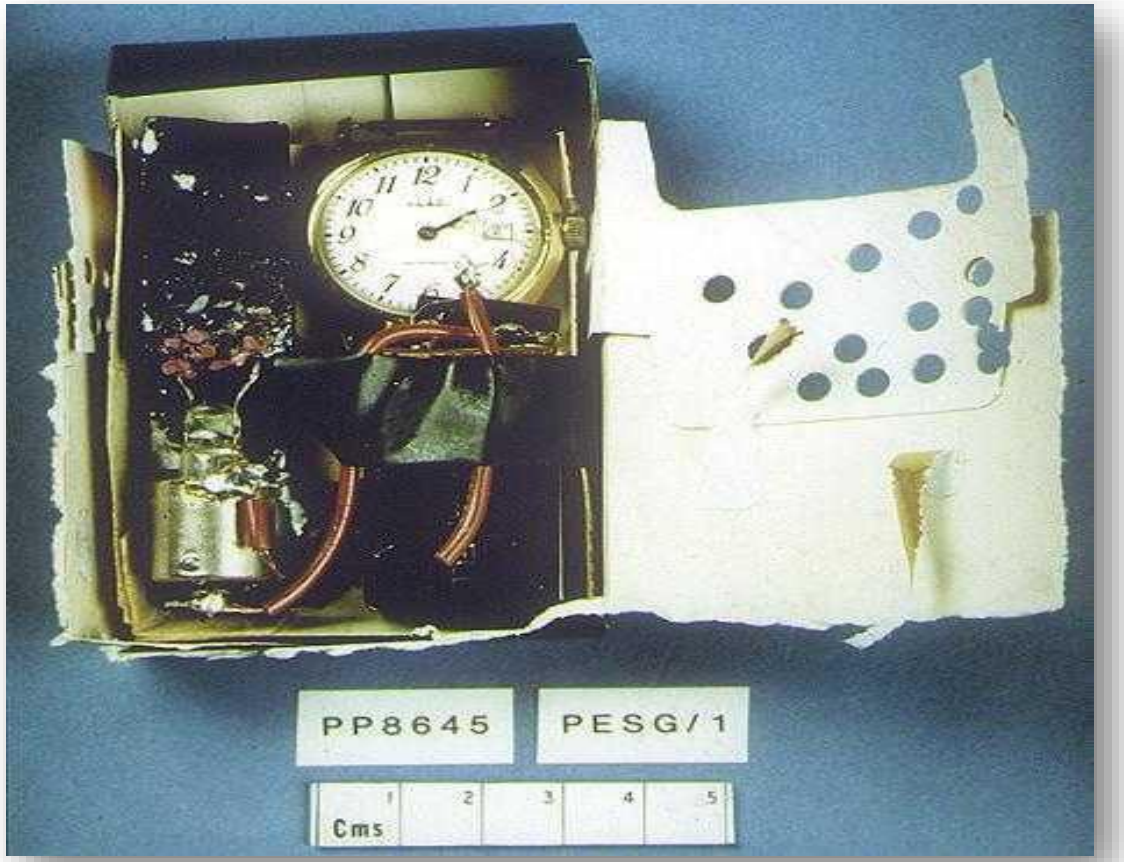
Explosives





Complete Explosive Devices





IID Components

(Improvised Incendiary Device)

- Flammable material (Incendiary Material)
- Means of Ignition
- (FICE) friction, electrical.
- Timer or delay mechanism.

Complete Incendiary Devices

Reacting to Threat Warnings

- Remain calm
- If in the x-ray machine keep item in tunnel and preserve the image
- Get a second opinion
- Follow company procedures
- If suspect IED / IID DO NOT TOUCH

It is a telephone bomb threat, what shall I do?

- Stay calm
- Listen carefully and write everything down
- Note exact time of call
- If possible, record the call
- Do not hang up as you may lose the ability to trace the call
- Complete the Bomb Threat Form Notify immediate supervisor/manager and evacuate premises.
- Call/Fax Bomb Threat Form to Corporate Security

The common motives for making a “Telephone Bomb Warning”

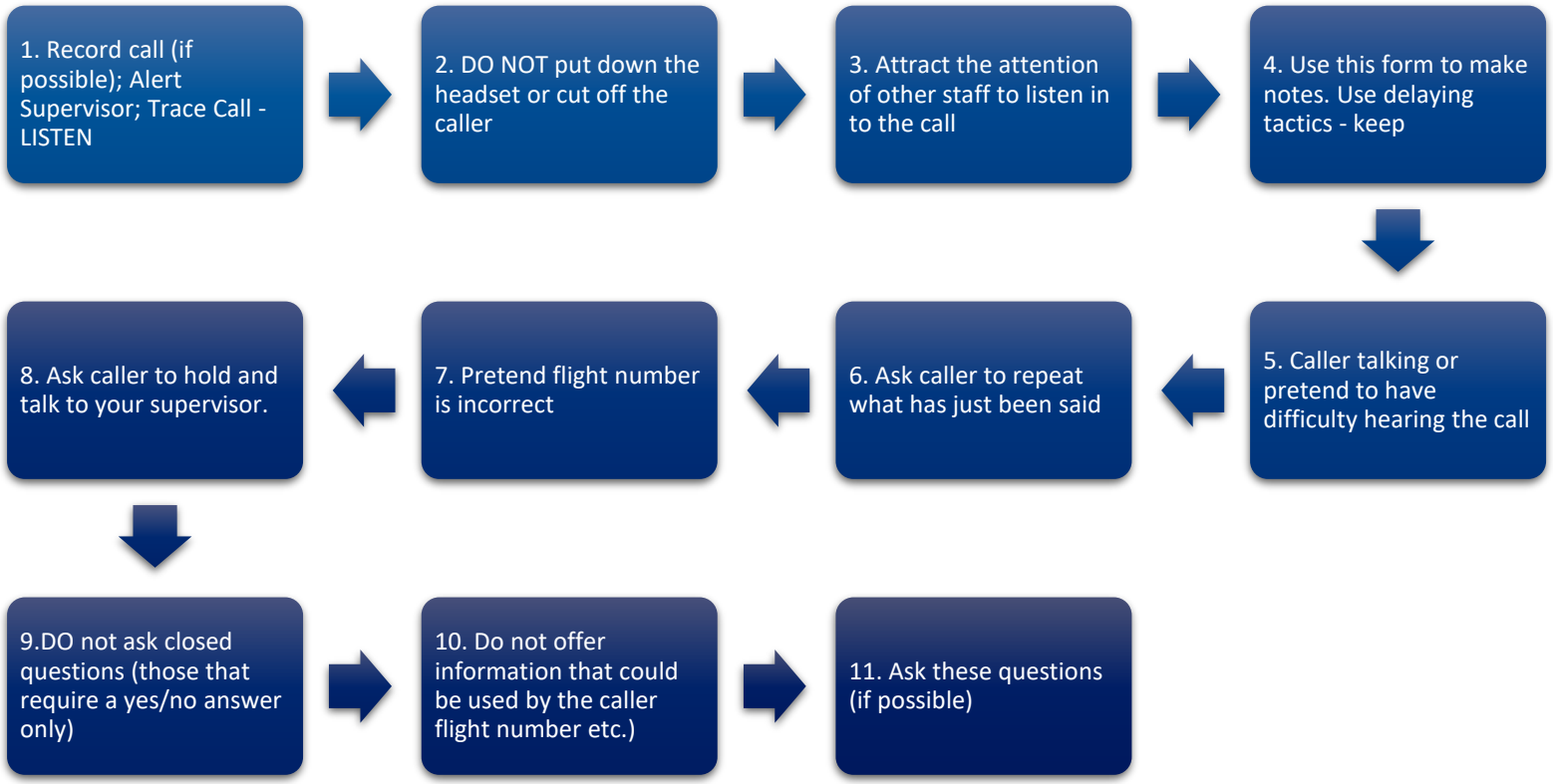
- Serious or genuine warnings of a real (or believed to be real) attack
- Cause disruption
- Malicious or hoax calls, for example a drunken party goer or some one encouraged by articles in the press
- Recent examples:
  - Asylum seeking partners phoning to extend stay in the country, tweets against Airports, late passengers for flights

The Five “W” questions Bomb Threat

WHERE	WHEN	WHAT	WHO	WHY
is the bomb ?	will it go off ?	does it look like ?	are you ?	are you doing this ?

Bomb / Threat Reporting Form

Guidance - handling telephoned threat call



12. Supplementary questions (if possible)
Where are you calling from?
. What is your name and telephone number?
. Why do you expect me to believe you?
. What do you hope to accomplish by doing this?
. How would your family feel if they know what you have done?
. Are you aware that there are many innocent people involved?
. If they have done you no harm why are you doing this?
. Why pick on this flight or building?

What shall I do when the call ends

- Leave the phone off the hook - this may help in tracing the call
- Evacuate the premises
- Notify your manager and complete the Bomb Threat Report Form

Notification Who to contact if support is needed and other pertinent information!

Objective:

To ensure all staff members understand the Notification Process and are fully aware of which organizations are to be contacted immediately upon discovery of a prohibited/suspicious article or receiving a bomb treat.

NOTIFICATION

- Upon discovery of: Rejecting cargo because individual/entity has provided: - False Information, IED,IID Prohibited Weapons
    - TSA
    - Local Authorities
    - Screening Supervisor
    - Duty Manager
    - Station Manager or Security Manager

NOTIFICATION

Immediately notify :

- the Air Carrier Management Representative (ACMR)
- a Law Enforcement Officer (LEO)
- the Transportation Security Operations Center (TSOC) at +1-866-655-7023 / +1-703-563-3240

Security

- **Secured Area** : A portion of an airport, specified in the airport security program, in which certain security measures are carried out. This area is where aircraft operators and foreign air carriers that have a security program enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security measures.

- **Direct Air Carrier**: A person who provides or offers to provide air transportation and who has control over the operational functions performed in providing that transportation; one holding an Federal Aviation Administration (FAA)- issued operating certificate authorizing the transportation of person or property for hire.

- **Indirect Air Carrier (IAC):** Any person or entity within the United States not in possession of an FAA air carrier operating certificate that undertakes to engage indirectly in air transportation of property and uses for all or any part of such transportation the services of an air carrier. This does not include the United States Postal Services (USPS) or its representative while acting on behalf of USPS.

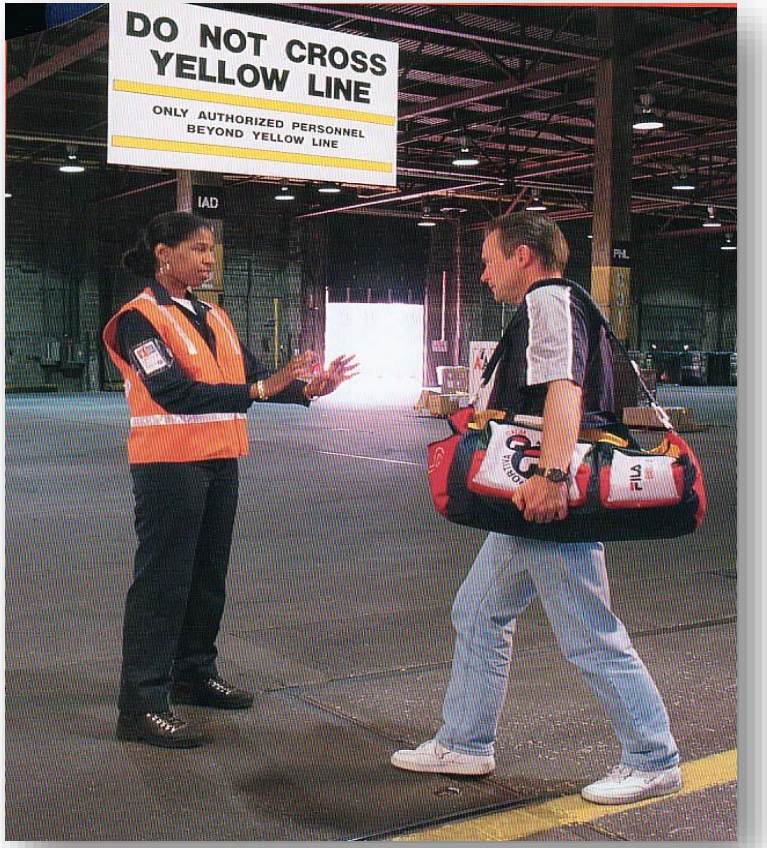
Escorted Personnel

Escorted personnel must be documented at point of entry by authorized employee who has escort privileges.

The escorted individual must show a valid government issued ID to the authorized employee.

A record showing date ,time ,visitors name and signature and reason for visit must be kept at station.

All escorting procedure must comply with local airport authority requirements.



Proper Identification

- What do you think some of your obligations are?
  - Proper use of the Airport ID Card.
  - Prevent unauthorized personnel from gaining access into restricted areas at Airport.

- Why do you think the ID card is important?
  - It is important because it distinguishes who is authorized to be in the SIDA and who is not.

- What does it mean to display?
  - Display should not be confused with “Wearing”. Display means that:
  - The face of the card is visible at all times
  - Worn on your outermost garment.
  - Worn above the waist
  - Outer Most Garment

PIGGYBACKING

- Piggybacking is the act of following one or more individuals or vehicles through a controlled access point to the SIDA without allowing the access point to reset (door closing or gate arm completely closing).

- If an individual swipes his/her ID card and gains access through a door, do you think it is permitted for this person to hold the door open for another person?
  - No. Federal regulation requires that “each individual” swipe his/her ID card when entering the SIDA. This is one time when you are required to not be courteous and hold the door open for the next person.

Proper Identification

Challenge:

This is our most effective tool for maintaining airport security. Not only do you have an obligation to ensure that you are displaying a valid airport authorized id badge card, you also have an obligation to make sure that ALL INDIVIDUALS IN THE SIDA ARE DISPLAYING THEIR AIRPORT AUTHORIZED ID BADGE CARDS. This means approaching individuals not displaying an ID card and asking them if they have one and to see it.

How to challenge

- Stop the person and advise them that they will not be allowed access unless they display a valid airport ID card.
- Make sure you have your ID properly displayed
- Approach the person in a non threatening manner
- Ask them to show you their Port ID
- Advise them that they are in a restricted area
- If they cannot produce an ID, escort them to Security or your supervisor

How to challenge

If an individual becomes irate, uncooperative or threatening when challenging them:

- You SHOULD NOT attempt to physically remove the person.
- You should remove yourself from any immediate danger and contact your supervisor and your local police.
- The police treat these calls with the highest urgency and will send officers to the scene immediately.
- While waiting you should try to get a description of the person and what direction they are going.

Thank You
Questions!!!

CHOICE
AVIATION SERVICES