C-TPAT

Customs-Trade Partnership Against Terrorism

# SUPPLY CHAIN SECURITY

## Training Guide


★ NOW FOR IMPORTERS AND EXPORTERS ★

# C-TPAT

Customs and Border Protection (CBP) recognizes that a safe and secure supply chain is the most critical part of their work in keeping our country safe. For this reason, CBP is seeking a strong antiterrorism partnership with the trade community through the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary Government-business initiative to build cooperative relationships that strengthen and improve the overall international supply chain and the security of the U.S. border.

Through this initiative, CBP is asking businesses within the supply chain, such as importers, exporters, carriers, consolidators, licensed customs brokers and manufacturers, to ensure the integrity of their security practices and to communicate and verify the security guidelines of their business partners.

Even without official participation in C-TPAT, companies should consider following C-TPAT guidelines in their security practices.

For more information, visit: **www.cbp.gov/ctpat**

## CBP Mission Statement

- We are the guardians of our Nation's borders.
- We safeguard the American homeland at and beyond our borders.
- We protect the American public against terrorists and the instruments of terror.
- We steadfastly enforce the laws of the United States while fostering our Nation's economic security through lawful international trade and travel.

C-TPAT

## Training Program

Education and training are the best weapons to use in the fight against terrorism. C-TPAT partner members must understand the value in educating their employees and preparing them to perform their jobs effectively.

The following describes a good training program:

- Training is mandatory.
- Training is recurring.
- The program comprises every procedure the company has in place to address and report a situation.
- The C-TPAT Minimum Security Criteria are addressed.
- Employees in sensitive positions receive additional training.
- The program encourages accountability.
- The program is incentive-based.
- The program is Web-based.
- The program embraces employee input and feedback.

## Disclaimer

The C-TPAT program has members ranging from importers to U.S. Customs brokers. Each business entity has its own set of guidelines or Minimum Security Criteria. This guide is intended for importers and exporters who are C-TPAT members. However, the Minimum Security Criteria cited within may have been merged, condensed or otherwise modified to satisfy printing requirements.

**For a complete listing of the security criteria for all types of businesses, go to www.cbp.gov/ctpat and click on the "Minimum Security Criteria" link.**

# C-TPAT SECURITY CRITERIA FOR IMPORTERS

## Importer Eligibility Requirements

To qualify for the C-TPAT program, your company must be an active importer, meaning that you have imported goods within the past year. Very low-volume importers (less than 24 importations) will be considered on a case-by-case basis.

Specific eligibility requirements are as follows. Your company must:

1. Be an active U.S. importer or nonresident Canadian importer into the U.S.
2. Have a business office staffed in the U.S. or Canada.
3. Have an active U.S. Importer of Record (IOR) ID in one of the following formats:
   - U.S. Social Security number
   - U.S. Internal Revenue Service assigned ID(s)
   - CBP assigned importer ID
4. Possess a valid continuous import bond registered with CBP.
5. Have a designated company officer who will be the primary cargo security officer responsible for C-TPAT.
6. Commit to maintaining the C-TPAT supply chain security criteria as outlined in the C-TPAT importer agreement.
7. Create and provide CBP with a C-TPAT supply chain security profile, which identifies how your company will meet, maintain and enhance internal policy to meet the C-TPAT Importer security criteria.

## Importer Minimum Security Criteria

Importers must conduct a comprehensive assessment of their international supply chains based on the C-TPAT Minimum Security Criteria listed in this guide.

When an importer outsources or contracts elements of its supply chain, such as to a foreign facility, conveyance or domestic warehouse, the importer must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout the supply chain.

For C-TPAT purposes, the supply chain is defined as starting from the point of origin (manufacturer, supplier, vendor) and ending at the point of distribution.

C-TPAT recognizes the diverse business models its members employ and the complexity of international supply chains. It endorses the application and implementation of security measures based on risk analysis. Therefore, the program allows for flexibility and the customization of security plans based on each member's business model.

Appropriate security measures must be implemented and maintained throughout the importers' supply chains, based on risk.

## Business Partner Requirements

Importers must have verifiable written processes for the selection of business partners, including manufacturers, product suppliers and vendors.

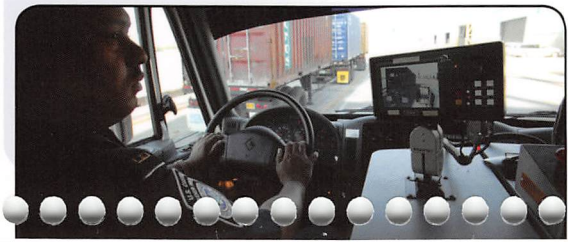
### Security Procedures

If their business partners (carriers, ports, terminals, brokers, consolidators, etc.) are eligible for C-TPAT certification, importers must have documentation indicating whether the partners are certified: C-TPAT certificate, Status Verification Interface (SVI) number, etc.

If their business partners are not eligible for C-TPAT certification, importers must require them to demonstrate that they meet C-TPAT security criteria via written or electronic confirmation:

- Contractual obligations
- Letter from a senior business partner officer attesting to compliance
- Written statement from the business partner demonstrating compliance with C-TPAT security criteria or an equivalent security program accredited by the World Customs Organization (WCO) and administered by a foreign customs authority
- Completed importer security questionnaire

Importers must conduct a documented risk assessment to verify the compliance with C-TPAT security criteria of business partners who are not eligible for C-TPAT certification.



## Point of Origin

Importers must make sure business partners develop security processes and procedures consistent with C-TPAT security criteria to ensure the integrity of the shipment at the point of origin.

Based on risk, they should conduct periodic reviews of the business partners' processes and facilities to ensure that required security standards are maintained.

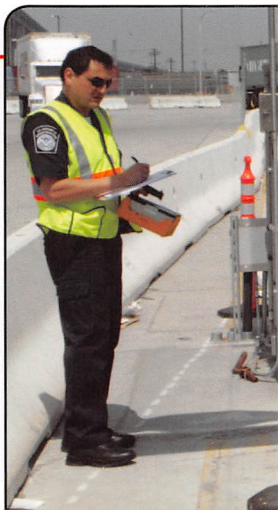
## Participation and Certification in Foreign Customs Administrations' Supply Chain Security Programs

Importers must require current and prospective business partners to indicate their status of participation if they are certified by a supply chain security program administered by a foreign customs administration.

## Other Internal Criteria for Selection

Importers should address internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies, as needed.

Internal requirements should be assessed against a risk-based process determined by an internal management team.



# C-TPAT SECURITY CRITERIA FOR EXPORTERS

The original goal of the C-TPAT program was to enhance security throughout the international importing supply chain, from point of stuffing through to the first U.S. port of arrival. However, exporting also has an important role in international supply chains. C-TPAT opened the program to U.S. exporters to support the Administration's Export Initiative, support export growth and increase the competitiveness of the U.S. business community.

## Definition of an Exporter

For C-TPAT purposes, an exporter is defined as a person or company who, as the principal party in interest in the export transaction, has the power and responsibility for determining and controlling the sending of the items out of the U.S.

## Exporter Entity Eligibility Requirements

Entities that wish to participate in the C-TPAT exporter program must meet the following eligibility requirements:

1. Be an active U.S. exporter out of the U.S.
2. Have a business office staffed in the U.S.
3. Be an active U.S. exporter with a documentable Employer Identification Number (EIN) or a Dun & Bradstreet (DUNS) number.
4. Have a documented export security program and a designated officer or manager who will act as the C-TPAT program main point of contact (POC). Also have an alternate POC should the designated POC be unavailable.

5 Commit to maintaining the C-TPAT supply chain security criteria as outlined in the C-TPAT exporter agreement.

6 Create and provide CBP with a C-TPAT supply chain security profile that identifies how the exporter will meet, maintain and enhance internal policy to meet the C-TPAT exporter security criteria.

7 Have an acceptable level of compliance for export reporting for the latest 12-month period and be in good standing with U.S. regulatory bodies such as:

- Departments of Commerce, State, Treasury, Energy, Justice and Defense
- Nuclear Regulatory Commission (NRC)
- Drug Enforcement Agency (DEA)
- Environmental Protection Agency (EPA)

## Exporter Minimum Security Criteria

Exporters must conduct a comprehensive risk assessment of their international supply chains based on the C-TPAT Minimum Security Criteria listed in this guide.

When an exporter outsources or contracts elements of its supply chain, such as to a warehouse, logistics provider, carrier or other export supply chain element, the exporter must work with these business partners to ensure that effective security measures are in place and adhered to throughout the entire supply chain.

C-TPAT recognizes the complexity of international supply chains and endorses the application and implementation of security measures based upon risk analysis by exporters. Therefore, the program allows for flexibility and the customization of security plans based on each member's business model.

Appropriate security measures must be implemented and maintained throughout the exporters' supply chains, based on risk.

## Business Partner Requirements

Exporters must have verifiable written processes for the screening and selection of business partners, including service providers, manufacturers, product suppliers and vendors. They must be checked against screening lists where applicable – flip to the "Screening for Prohibited or Restricted Parties" section in the "Procedural Security" tab.

Entities on prohibited lists must be reported to the Supply Chain Security Specialist (SCSS) and the relevant authority within 24 hours prior to departure.

### Security Procedures

There must be written procedures for screening business partners to identify specific factors or practices, which, if present, would trigger additional scrutiny by the exporter.

If their business partners (importers, carriers, ports, terminals, brokers, consolidators, etc.) are eligible for C-TPAT certification, exporters must have documentation, such as a Status Verification Interface (SVI) number, indicating whether these business partners are C-TPAT certified and/or participating in a reciprocal Authorized Economic Operator (AEO) program (e.g., AEO certificate).

If their business partners are not eligible for C-TPAT certification or participation in an AEO program, exporters must require them to demonstrate that they meet C-TPAT security criteria via written or electronic confirmation (e.g., contractual obligations; a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating compliance with C-TPAT security criteria or an equivalent AEO security program administered by a foreign customs authority; or a completed exporter security questionnaire).

Exporters must conduct a documented risk assessment to verify the compliance with C-TPAT security criteria of business partners who are not eligible for C-TPAT certification. Risk assessments of the company's export program must be completed on an annual basis.

## Point of Origin

Exporters must inform business partners of security processes and procedures consistent with the C-TPAT security criteria to ensure the integrity of the shipment at point of export.

Based on risk, they should conduct periodic reviews of the business partners' processes and facilities to ensure that required security standards are maintained.

## Participation and Certification in Foreign Customs Administrations' Supply Chain Security Programs

Exporters must require current and prospective business partners to indicate their status of participation if they are certified by a supply chain security program administered by a foreign customs administration.

## Other Internal Criteria for Selection


Exporters should address internal requirements, such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies, as needed.

Internal requirements should be assessed by management, using a risk-based document.

# SECURITY RISK RATING

All C-TPAT partners are responsible for establishing their own overall security risk rating system based on their business model.

Businesses use various methods to rate risk within their international supply chains. However, the following risk ratings are recommended when examining security threats and vulnerabilities within the international supply chain.

## Threat Assessment

There are many open sources providing information on threats within the international supply chain. After conducting research, assign a rating to each threat:

| | | |
|---|---|---|
| 1 | Low Risk | ↘ No recent incident<br>↘ No intelligence<br>↘ No information |
| 2 | Medium Risk | ↘ No recent incident<br>↘ Some intelligence<br>↘ Information on possible activity |
| 3 | High Risk | ↘ Recent incident<br>↘ Intelligence<br>↘ Information |

A score of 3 in any of the following areas indicates a high-risk supply chain:

- ↘ Terrorism
- ↘ Contraband smuggling
- ↘ Human smuggling
- ↘ Organized crime

## Vulnerability Assessment

One method of assessing vulnerability is to send security questionnaires to business partners who are not eligible for or do not participate in the C-TPAT program.

The security questionnaire should ask business partners to describe the security measures for their various processes in the international supply chain. It should not include only yes/no questions.

The questionnaire should address whether systems of checks, balances and accountability are in place, particularly in the following areas:

- Security for instruments of international traffic
- Cargo tracking and monitoring
- Seal security
- Business partner screening (subcontracts)

The chart below lists the vulnerability ratings for all C-TPAT Minimum Security Criteria categories:

| | | |
|---|---|---|
| 1 | Low Risk | Meets all applicable minimum security "musts" and "shoulds" |
| 2 | Medium Risk | Meets all applicable minimum security "musts" but not all "shoulds" |
| 3 | High Risk | Does not meet all minimum security "musts" |

# FIVE STEP RISK ASSESSMENT PROCESS

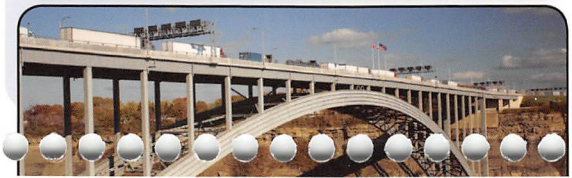
The Five Step Risk Assessment Process is recommended to assist C-TPAT partners with conducting a risk assessment of their international supply chains. The following information is intended to serve as a guide. It does not address everything that should be included in an international supply chain security risk assessment.

C-TPAT members may have numerous supply chains, which may present a monumental task when conducting a comprehensive security risk assessment. Therefore, it is recommended that importers identify their high-risk supply chains by conducting a threat assessment at the point of origin and at the place where the cargo is routed or transshipped. Then they should conduct a comprehensive security vulnerability assessment of those supply chains.

Exporters should conduct a risk assessment of their partners in the export chain, including any carriers they select for freight destined to the port of export and across the border to the destination, as well as freight forwarders, brokers, consolidators, etc.

Conversely, if supply chains involve a limited number of business partners or related business partners, the security risk assessment may not require such extensive efforts.

For more details, go to **www.cbp.gov/ctpat** and, under "Resources for Partners," click on the link for "Five Step Risk Assessment Guide."



## **Step 1:** Map Cargo Flow and Business Partners

Identify all parties involved in the following processes:

- Procurement
- Production
- Packing
- Storage
- Loading and unloading
- Transportation
- Document preparation

Methods:

- Request information from supply chain partners.
- Review documentation (bills of lading, manifests, invoices, etc.) to determine routing.
- Perform onsite visits or audits of the supply chain.

## **Step 2:** Conduct Threat Assessment

Identify and rate the country and region's threat risk for each international supply chain in at least the following areas:

- Terrorism (political, bio, agro, cyber)
- Contraband or human smuggling
- Organized crime
- Conditions fostering any of the above threats

Methods:

- Search for open-source Internet information (Government and private organizations) – flip to the "Resources" tab.
- Consult onsite representatives or contacts at the origin.
- Contact law enforcement (foreign or domestic), and the local, state, Federal or national authorities.
- Consult trade and security organizations.
- Check for restricted or prohibited parties on the Consolidated Screening List – flip to the "Procedural Security" tab.
- Refer to assigned C-TPAT Supply Chain Security Specialist (SCSS). The SCSS is available to discuss security issues and review problems.

## **Step 3:** Conduct Vulnerability Assessment

Assess the vulnerability of all business partners in the international supply chain (contracted or subcontracted):

- Identify their processes.
- Ensure they meet all applicable Minimum Security Criteria.
- Rate their compliance in each applicable Minimum Security Criteria category.

Methods:

- Request a Status Verification Interface (SVI) number or C-TPAT membership.
- Participate in a mutual recognition program.
- Send a security questionnaire.
- Have a company representative visit the site.
- Have overseas personnel or agents visit the site.
- Consult business reports.
- Request security certifications covering the C-TPAT Minimum Security Criteria.
- Have a third party conduct supply chain security assessments.

## **Step 4:** Prepare Action Plan

Establish a corrective action plan to address vulnerabilities found in a business partner's security programs.

Methods:

- Create a Word document.
- Create an Excel spreadsheet.
- Use project management software.

## **Step 5:** Document How Risk Assessments Are Conducted

Produce a description of the company's approach, policies and procedures for conducting an international supply chain security risk assessment.

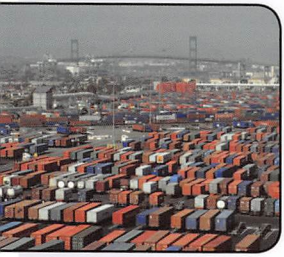
Methods:

- Document the company's policy for conducting an international supply chain security risk assessment.
- Document the procedures used to conduct an international supply chain security risk assessment.

A company's documented risk assessment process should contain at least the following information:

- Date at which the risk assessment process was established
- Parties responsible for keeping the process up to date, including backup people
- When risk assessments must be conducted (for new suppliers or service providers overseas)
- How often risk assessments must be conducted (as circumstances dictate, at least once a year for most C-TPAT partners or every quarter for highway carriers)
- Required frequency of reviews and updates to processes, policies and procedures (annually, biannually, as needed)
- How threat assessments of the international supply chain are to be conducted (sources used to determine threats)
- How vulnerability assessments on the international supply chain are to be conducted (questionnaires, site visits, C-TPAT status, participation in an international import and export supply chain security program)
- How follow-ups are conducted on action items (site visits, submission of documents or photographs)
- Process for training key individuals responsible for the processes
- Management oversight and accountability to ensure the processes are carried out consistently and effectively

# CONVEYANCE SECURITY

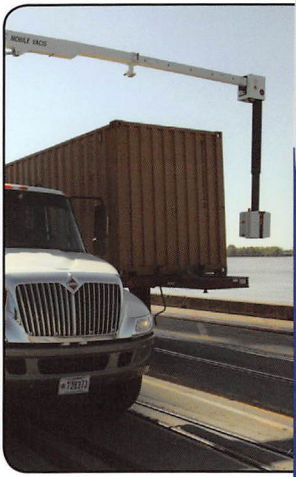


Container and trailer integrity must be maintained to protect against the introduction of unauthorized materials or people. Procedures must be in place at the point of stuffing to properly seal and maintain the integrity of the shipping containers and trailers.

## Inspection

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing and the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

1. Outside and undercarriage
2. Inside and outside doors, including door hardware and fasteners
3. Right side
4. Left side
5. Front wall
6. Ceiling and roof
7. Floor (inside)



Flip to the "Inspection" tab.

## Self-Reporting

According to C-TPAT Conveyance Security criteria, carriers, importers and exporters must report any anomalies or structural changes, such as a hidden compartment discovered in a container, trailer, tractor or other rolling-stock equipment crossing the border or destined for export.

CBP should be immediately notified, before the conveyance crosses the border. The assigned Supply Chain Security Specialist (SCSS) should be notified within 24 hours of discovery.

**For Port of Entry contact numbers, visit:**
**www.cbp.gov/contact/ports**

## Storage

Containers and trailers must be stored in a secure area to prevent unauthorized access or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

## Seals

Properly sealing trailers and containers, and ensuring continuous seal integrity, are crucial steps in a secure supply chain and a critical part of the commitment to C-TPAT.

A high-security seal must be affixed to every loaded trailer and container bound for the U.S. or destined for export from the U.S. The seal must be checked at each stage of the supply chain to ensure seal integrity, and it must be intact until the trailer or container reaches its final destination.

All seals must meet or exceed the current ISO 17712 standards for high-security seals. For integrity purposes, only designated employees should distribute these seals. Written procedures must stipulate how importers, exporters and carriers are to control seals during transit. These procedures must be clearly defined and include the following steps:

- Ensuring that seals are affixed to loaded trailers and containers during transit
- Verifying whether seals are intact or exhibit evidence of tampering during transit
- Reporting any compromised seals, trailers or containers to CBP or the appropriate foreign authority
- Properly documenting the original and second seal numbers
- Verifying that the seal numbers and locations are the same as stated in the shipping documents
- Placing a second seal on a trailer and documenting the change if the first seal was removed (even if by a Government official) while en route to the border

## Highway Carriers

Importers and exporters should ensure that their transportation providers adhere to the following procedures. Highway carriers must use a tracking and monitoring activity log or equivalent technology to ensure conveyance and trailer integrity while transporting cargo to the U.S. border or to the point of export.

Predetermined routes should be identified by the carrier. There should be random route checks by the carrier along with documentation and verification of the length of time between the loading point/trailer pickup, the export point and/or the delivery destinations, during peak and off-peak times. Drivers should notify the dispatcher of any delay due to weather, traffic or rerouting.

Highway carrier management must perform and document periodic, unannounced verifications to ensure the following:

- Logs are maintained.
- Conveyance tracking and monitoring procedures are followed and enforced.

If a seal gets broken, the driver must immediately notify the dispatcher and give the following information:

- Who broke the seal
- The number of the second seal placed on the trailer

Also, the carrier must immediately notify the shipper, customs broker and importer or exporter about the placement of the second seal.

# VVTT SEAL INSPECTION

The main elements of a strong security training and awareness program include the following:

- Container/trailer tracking
- Seal inspection and controls

Seals are much more vulnerable to tampering when they can be manipulated prior to application and closing. Seals should never be handled by unauthorized or untrained individuals.

Minimize the possibility of seal tampering by establishing a seal integrity process. Before seals are put in place and closed, use the following **VVTT** seal verification and inspection process.

**V**iew the seal and container locking mechanisms.

**V**erify the seal number for accuracy.

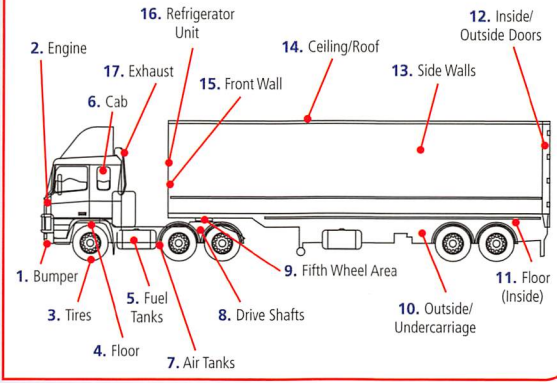
**T**ug on the seal to make sure it is affixed properly.

**T**wist and turn the seal to make sure it does not unscrew.

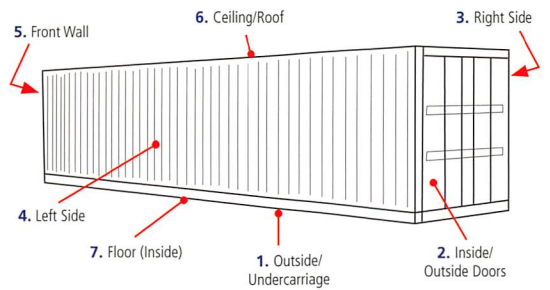
VVTT SEAL INSPECTION

# VEHICLE INSPECTION

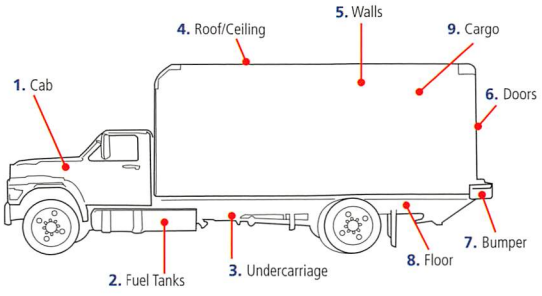
## 17-Point Tractor and Trailer Inspection



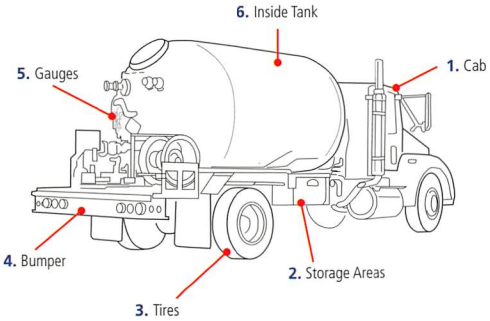

## Seven-Point Container Inspection



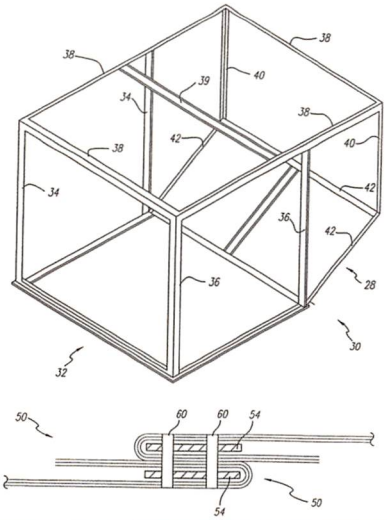
## Nine-Point Box Truck, Semi-Van or Step Van Inspection



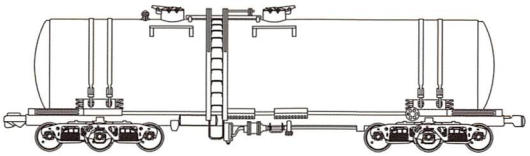

## Six-Point Propane Tanker Inspection



## Air Cargo Container




## Rail Tank Car



# HIJACKING PREVENTION & TRACKING

Hijackers may target trucks, buses and other commercial vehicles not for their cargo but to use the vehicle for other illegal purposes:

- Committing robberies
- Transporting explosives or other materials for destruction
- Perpetrating various types of terrorist activities

Employers should practice safety procedures to prevent hijacking:

- Increased use of high-quality seals and padlocks
- No-stop policy for drivers when possible, especially within two to three hours of the trip's origin
- En route tracking and communication protocols

Drivers should be trained to adhere to strict security measures to prevent hijacking:

- Know or learn the route, especially if it is a new one or it has a pick-up or drop-off location that has never been visited before. Keep fixed driving routes and know alternatives. Designate predetermined checkpoints.
- Make a backup plan in case equipment such as a global positioning system (GPS) fails.
- Be aware of safe areas in case you are targeted, and park in secure areas with ample lighting.
- Carry a 24-hour emergency telephone number at all times.
- Know the cargo, especially when carrying a potentially hazardous or high-value load.

- Check the load when possible to make sure the vehicle is carrying the right cargo.
- Inform the dispatcher of your route and then follow it. If the route changes, inform someone.
- Remember, there is safety in motion. You are most vulnerable to hijacking when the vehicle is stopped.
- Lock the vehicle every time you make a stop. Keep the trailer unit locked securely from the moment the vehicle is loaded. Lock the cab and roll up the windows when parked or in slow-moving traffic.
- Unlock the truck for as short a time as possible when you stop to rest, eat or make a delivery.
- Stop only in designated rest areas where other trucks are parked.
- Avoid stopping at the same places every trip.
- Do not stop to help motorists in trouble, but do call for assistance.
- Be aware of your surroundings. Watch for suspicious vehicles at the pick-up point, cars or vans that follow the vehicle on the highway or anything that seems unusual.
- Never pick up hitchhikers.
- Do not leave a vehicle at the customer's dock.
- When making a delivery, do not leave the cargo unattended on the street, not even for a minute or two.
- For both tractors and trailers, keep the vehicle number, license plate number and vehicle identification number (VIN) with you at all times. This is critical information for law enforcement if the vehicle is stolen or hijacked.

# PROCEDURAL SECURITY

For importers and exporters, security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain.

Exporters should implement security procedures that restrict access to the export shipment to prevent the lading of contraband while en route from facilities in domestic locations prior to export from the U.S.

## Screening for Prohibited or Restricted Parties

Certain individuals and organizations are prohibited from receiving U.S. exports. Exporters must check any party involved in an export transaction against the Government's Consolidated Screening List, which includes the following:

- Denied Persons List
- Entity List
- Unverified List
- Nonproliferation Sanctions List
- Arms Export Control Act (AECA) Debarred List
- Specially Designated Nationals List

**To download the Consolidated Screening List, go to: www.export.gov/ecr or www.bis.doc.gov**

Entities on prohibited lists must be reported to the Supply Chain Security Specialist (SCSS) and the relevant authority within 24 hours prior to departure.

## Documentation Processing

When clearing merchandise and cargo, or preparing it for export, procedures must be in place to ensure that all information is legible, complete and accurate.

For exporters, as well as required export forms, the Electronic Export Information (EEI) may need to be prepared.

There also must be protection against the exchange or loss of information and the introduction of erroneous information. Documentation control must include safeguarding computer access and information.

## Bill of Lading/Air Waybill/Manifesting Procedures

To help protect the integrity of cargo received from abroad or being exported, procedures must be in place to ensure that information received from or transmitted to business partners is reported accurately and in a timely manner.

## Shipping and Receiving

Arriving cargo should be verified against information on the cargo manifest. Arriving or departing cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified.

Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be identified before the cargo is released or received.

## Cargo Discrepancies

All shortages, overages and other significant discrepancies or anomalies must be resolved or investigated appropriately. CBP, the assigned SCSS and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

# SMUGGLING TECHNIQUES

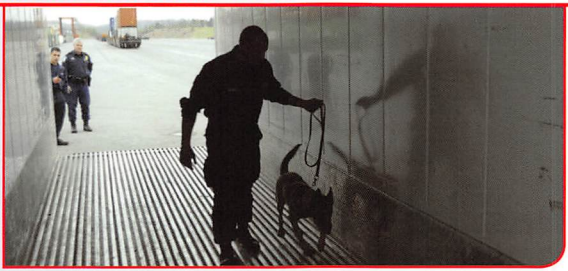
## Trailer Compartment


## Inspections

### Radioactive Inspection Prep at Port


### X-Ray Truck Search for Contraband

### Random Truck Search with K9



# PHYSICAL ACCESS CONTROLS

Access controls prevent any unauthorized entry into a facility, maintain control of employees and visitors, and protect company assets.

Access controls must include the identification of all employees, visitors, vendors, service providers, etc., at all points of entry. Company management or security personnel must control the issuance and recovery of all ID badges.

## Employees

An employee identification system must be in place. Employees should be given access only to those secure areas needed to perform their duties.

Procedures for issuing, recovering and altering access devices (keys, key cards, etc.) must be documented.

## Visitors

Visitors must present photo ID on arrival. They should be escorted and must visibly display temporary identification.

## Deliveries (Including Mail)

All vendors, service providers, etc., must present proper photo or vendor ID on arrival. Arriving mail and packages should be screened periodically before being disseminated.

## Unauthorized People

People should have access only to those areas of a facility where they have legitimate business. Procedures must be in place to identify, challenge and address unauthorized or unidentified people.

Always be aware of your surroundings. Report anything suspicious to your supervisor or to local law enforcement.

# SUSPICIOUS MAIL OR PACKAGES

## Protect yourself, your business and your mailroom.

**If you receive a suspicious letter or package:**

- Stop. Don't handle.
- Isolate it immediately.
- Don't open, smell or taste.
- Activate your emergency plan. Notify a supervisor.


**If you suspect the mail or package contains a bomb (explosive), or a radiological, biological or chemical threat:**

- Isolate area immediately
- **Call 911**
- Wash your hands with soap and water

UNITED STATES POSTAL SERVICE.

To order this poster, call 1-800-332-0317.

Postal 84
September 2004
PSN 7690-07-000-7097

# PHYSICAL SECURITY

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

**Importers** should incorporate the following C-TPAT physical security criteria throughout their supply chains, as applicable.

**Exporters** must have procedures in place to prevent, detect or deter undocumented material and unauthorized personnel from gaining access to conveyances, including concealment in containers. Exporters should, according to their business models, incorporate the following C-TPAT physical security criteria throughout their supply chains, as practical and appropriate.

## Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high-value and hazardous cargo. All fencing must be regularly inspected for damage or tampering.

## Gates and Gatehouses

Gates for vehicles and personnel must be manned or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

## Parking

Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

## Building Structure

Buildings must be constructed with materials that can resist unlawful entry. The integrity of the structures must be maintained by periodic inspection and repair.

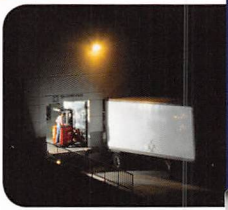
## Locking Devices and Key Controls

All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuing of all locks and keys.

## Lighting

Adequate lighting must be provided inside and outside the facility, including in the following areas:

- Entrances and exits
- Cargo handling and storage areas
- Fence lines
- Parking areas



## Alarm Systems and Video Surveillance

Alarm systems and video surveillance cameras should be used to monitor the premises and prevent unauthorized access to cargo handling and storage areas.

# PERSONNEL SECURITY

Processes must be in place to screen prospective employees and periodically check current employees.

## Pre-Employment Verification

Application information, such as employment history and references, must be verified prior to employment.

## Background Checks and Investigations

As per foreign, Federal, state and local regulations, background checks and investigations should be conducted for prospective employees. For current employees, there should be periodic checks and reinvestigations based on cause or the sensitivity of their positions.

## Personnel Termination Procedures

Companies must have procedures to remove identification, facility access and system access from terminated employees.

# TERMINATION & PROPERTY RETURN FORM

**Employee Name:**

**Department:**

**Date of Release:**

| Action | Completion Date | Initials | Department Responsible |
|---|---|---|---|
| Collect badge/ID | | | |
| Collect keys/pass | | | |
| Collect company cell phone | | | |
| Collect company laptop | | | |
| Collect company credit cards | | | |
| Collect uniform | | | |
| Terminate login access | | | |
| Terminate alarm code/ access | | | |
| Notify cell phone carrier | | | |
| Notify payroll provider | | | |
| Notify insurance provider | | | |

**Verified By (Printed):**

**Signature:**

**Date:**

# INFORMATION TECHNOLOGY SECURITY

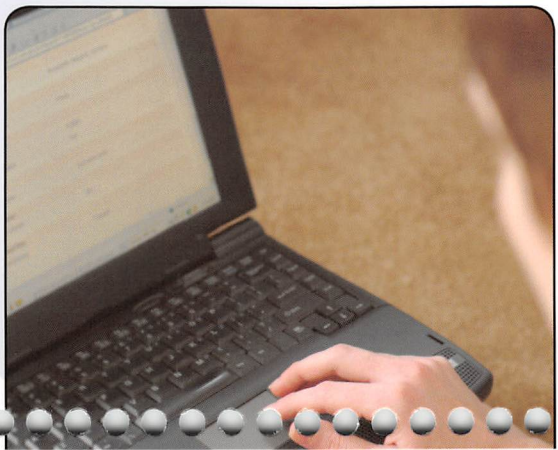
Importers and exporters must ensure that all confidential business data is protected from the abuse of available information technology (IT).

## Password Protection

Automated systems must use individually assigned accounts that require a periodic change of password. Employees must receive training on IT security policies, procedures and standards.

## Accountability

A system must be in place to identify IT abuses, including improper access and tampering with or altering of business data. All violators must be subject to appropriate disciplinary actions.



# SECURITY TRAINING & THREAT AWARENESS

Security personnel should establish a program to foster awareness of the threat posed by terrorists at every point in the supply chain. Employees must be made aware of the procedures in place to address and report a threatening situation or a security incident (including suspicion of a security incident).

Employees receiving and opening mail or working in the shipping and receiving areas should have additional training. Specific training should also be offered to assist employees in the following:

- Maintaining cargo integrity
- Recognizing internal conspiracies
- Protecting access controls
- Enhancing physical security

These programs should offer incentives for active employee participation.

## Additional Information for Exporters

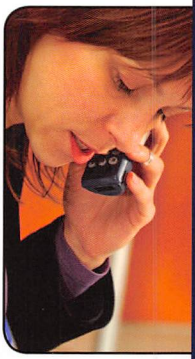
A C-TPAT exporter must have a documented export security program as well as a designated officer or manager who will act as the C-TPAT program point of contact. The corporate structure of the company should support the program and display this support in correspondence to personnel.

An exporter's threat awareness program should promote awareness of the threat posed by illegal activities at each point in the supply chain, to include the final point of export. There should also be a documented procedure for how the export security officer or manager receives information about changes in regulations or procedures.

# TRAINING BEST PRACTICES

- Conduct an annual security awareness seminar modeled after the C-TPAT seminar for the following people:
  - Suppliers based in the U.S.
  - Customers
  - Other business partners
- Offer multiple levels of C-TPAT training for the following staff members:
  - Managers and supervisors
  - Shipping and receiving personnel
  - Internal personnel dealing with contractors
  - Hourly staff
- For exporters, keep a dedicated person or team up to date on the latest export regulations. Training should be frequent and verifiable.
- Provide all employees with formal, documented training on security and threat awareness via an online portal. The following topics should be covered:
  - Improving the physical security of the facility
  - Challenging unidentified people on the premises
  - Maintaining a safe work environment
  - Procedures regarding conveyance security and incident reporting
  - Practice drills for emergency response
- Send an e-mail notification to managers if employees in their department have not completed the mandatory online training.
- Send monthly security reminders to all personnel by e-mail.
- Have management representatives of C-TPAT partner companies provide security guards with site-specific training. Guards should also receive C-TPAT training and orientation.

- Have managers assess the security awareness of a random sample of employees every year to gauge the company's overall awareness and identify any security issues that may need greater attention.
- Conduct tabletop exercises regularly to address possible security breaches in the supply chain.
- Use the following measures to ensure employees are notified of an alert issued by the Department of Homeland Security (DHS) warning of a potential or actual terrorist threat:
  - Digital message boards at all building entrances
  - Closed-circuit television (CCTV) monitors
  - E-mail notifications
  - Company website
  - Toll-free phone number



- Allow all personnel to express safety concerns or present security issues through the following channels:
  - Free hotline administered by a neutral third party
  - Private Internet forum
- Conduct the following at every U.S. facility:
  - Security drills
  - Exercises to test the workforce's effectiveness when reacting to a security incident
- Display C-TPAT awareness posters in several languages throughout every facility.
- Have managers offer a monetary reward for exhibiting good work practices, which include the following:
  - Making recommendations regarding security
  - Informing management of any security issues

# POINTS OF CONTACT

## C-TPAT Portal System

Use the portal to register, to access your account or to communicate with your assigned Supply Chain Security Specialist (SCSS). The portal also provides various multi-media security materials.

**https://ctpat.cbp.dhs.gov**

For more information, phone 202-344-1180 or e-mail: **industry.partnership@dhs.gov**

## Customs and Border Protection (CBP)

Report suspicious activity to **1-800-BE-ALERT (1-800-232-5378)**.

For general inquiries, contact the CBP Information Center at **1-877-CBP-5511 (1-877-227-5511)**. If you are outside the U.S., call **202-325-8000**.

For more CBP contact information, visit: **www.cbp.gov/contact**

## State and Local Points of Contact

| Agency | Phone Number |
|---|---|
| Local Port of Entry | |
| SCSS | |
| Local FBI-JTTFs | |

| | |
|---|---|
| State/Local Hazmat Response Team | |
| State Police | |
| Local Police Department | |
| Local Fire Department | |
| State/Local Fusion Center | |
| State/Local Environmental Agency | |
| Other Point of Contact: _____ | |
| Other Point of Contact: _____ | |

## RESOURCES

| | |
|---|---|
| Cargo Security Alliance | www.securecargo.org |
| C-TPAT | www.cbp.gov/ctpat |
| Customs and Border Protection (CBP) | www.cbp.gov |
| FBI Infrastructure Security | www.infragard.org |
| International Chamber of Commerce | www.icc-ccs.org |
| International Maritime Organization | www.imo.org |
| State Department Overseas Security Advisory Council | www.osac.gov |
| U.S. Department of Commerce | www.commerce.gov |

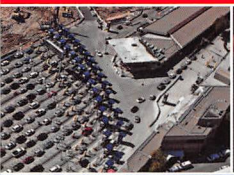
# SUPPLY CHAIN SECURITY TRAINING GUIDE

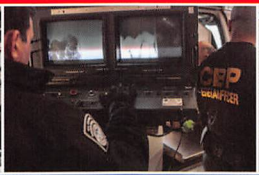
C-TPAT
Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary Government-business initiative started by Customs and Border Protection to build cooperative relationships that strengthen and improve the overall international supply chain and the security of the U.S. border.

This guide covers what importers and exporters need to know:

- C-TPAT Minimum Security Criteria
- Risk assessment process
- Conveyance and procedural security
- Physical access controls
- Physical, personnel and IT security
- Security training and threat awareness






QUICK SERIES


1-800-361-4653 | www.quickseries.com

01-0459-036-01 | 0459-007
ISBN 978-1-935665-70-0 | Printed in Canada