

## C-TPAT Security Criteria

### Highway Carriers

Highway carriers must conduct a comprehensive assessment of their international supply chain security practices based upon the following C-TPAT minimum-security criteria. Where a highway carrier does not control a specific element of their supply chain, such as a trucking yard, terminal, handling of trailers, or process subject to these criteria, the highway carrier must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain. The supply chain for highway carriers for C-TPAT purposes is defined from point of origin from the yard or where the tractors and trailers are stored, through pickup at the manufacturer/supplier/vendor, through to the point of distribution – and recognizes the diverse business models C-TPAT members employ.

These minimum security criteria are fundamentally designed to be the building blocks for highway carriers to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce dangerous elements into the global supply chain.

Highway carriers should routinely assess their degree of vulnerability to risk and should prescribe security measures to strengthen or adjust their security posture to prevent security breaches and internal conspiracies. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies, and in particular, highway carriers to elevate their security practices, especially if the highway carrier has the exclusive benefit of enrollment in the Free and Secure Trade (FAST) program.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk.<sup>1</sup> Therefore, the program allows for flexibility and the customization of security plans based on the member's business model. Appropriate security measures, as listed throughout this document, must be implemented and maintained.

#### **Business Partner Requirements**

Highway carriers must have written and verifiable processes for the screening of business partners, including carrier's agents, sub-contracted highway carriers, and service providers, as well as screening procedures for new customers, beyond financial soundness issues to include security indicators, such as business references and professional associations.

#### **Security procedures**

- Written procedures must exist for screening business partners which identify specific factors or practices, the presence of which would trigger additional scrutiny by the highway carrier, up to and including a detailed physical inspection of the customer's cargo trailer.
- For those business partners eligible for C-TPAT certification (importers, ports, terminals, brokers, consolidators, etc.) the highway carrier must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified. Non-C-TPAT business partners may be subject to additional scrutiny by the highway carrier.

---

<sup>1</sup> Truck Carriers shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, C-TPAT membership, potential terrorist threat via open source information, having inadequate security, past security incidents, etc.).

## DRAFT 1 – October 1, 2005

- Highway carriers should ensure that contract service providers commit to C-TPAT security recommendations through contractual agreements. For U.S. bound shipments, C-TPAT highway carriers that subcontract transportation services to other highway carriers, must use other C-TPAT approved highway carriers or carriers under direct control of the certified C-TPAT carrier through a written contract.
- Likewise, current or prospective business partners who have obtained a certification in a supply chain security program being administered by a foreign Customs Administration should be required to indicate their status of participation to the highway carrier.
- As highway carriers have the ultimate responsibility for all cargo loaded aboard their trailer or conveyance, they must communicate the importance of supply chain security and maintaining chain of custody as fundamental aspects to any company security policy.

### **Conveyance Security**

Conveyance integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material.

#### **Conveyance Inspection Procedures**

- Using a checklist, drivers should be trained to inspect their conveyances, i.e., trailer and tractor, for natural or hidden compartments. Training in conveyance searches should be adopted as part of the company's on-the-job training program.
- Conveyance inspections must be systematic and should be completed upon entering and departing from the truck yard and at the last point of loading prior to reaching the U.S. border.
- To counter internal conspiracies, a security manager, held accountable to senior management for security, should search the conveyance after the driver has conducted a search. These searches should be random, documented, based on risk, and should be conducted at the truck yard and after the truck has been loaded and en route to the U.S. border.
- Written procedures must exist which identify specific factors or practices, which may deem a shipment from a certain shipper of greater risk.
- The following systematic practices should be considered when conducting training on tractors and trailers. Highway carriers must visually inspect all empty trailers, to include the interior of the trailer, at the truck yard and at the point of loading, if possible. The following inspection process is recommended for all trailers and tractors:

1. Tractors:
  - Bumper/tires/rims
  - Doors/tool compartments
  - Battery box
  - Air breather
  - Fuel tanks
  - Interior cab compartments/sleeper
  - Faring/roof
2. Trailers:
  - Fifth wheel area - check natural compartment/skid plate
  - Exterior - front/sides
  - Rear - bumper/doors
  - Front wall
  - Left side

## DRAFT 1 – October 1, 2005

- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

### Trailer Security

- For all trailers in the highway carrier's custody, trailer integrity must be maintained, to protect against the introduction of unauthorized material and/or persons. Highway carriers must have procedures in place to maintain the integrity of their trailers at all times.
- It is recognized that even though a carrier may not “exercise control” over the loading of trailers and the contents of the cargo, highway carriers must be vigilant to help ensure that the merchandise is legitimate and that there is no loading of contraband at the loading dock/manufacturing facility. The highway carrier must ensure that while in transit to the border, no loading of contraband has occurred, even in regards to unforeseen vehicle stops.
- Trailers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into trailers, tractors or storage areas.
- The carrier must notify U.S. Customs and Border Protection immediately of any structural changes to trailers, tractors or other rolling-stock equipment that crosses the border.

### Container Security

- Highway carriers should only transport maritime containers of C-TPAT Importers that have a high security seal that meets or exceed the current PAS ISO 17712 standards for high security seals.

### Conveyance Tracking and Monitoring Procedures

- Highway Carriers must ensure that conveyance and trailer integrity is maintained while the conveyance is en route transporting cargo to the U.S. border by utilizing a tracking and monitoring activity log or equivalent technology. Predetermined routes should be identified, and procedures should consist of random route checks along with documenting and verifying the length of time between the loading point/trailer pickup, the U.S. border, and the delivery destinations, during peak and non-peak times.
- Highway Carrier management must perform a documented, periodic, and unannounced verification process to ensure the logs are maintained and conveyance tracking and monitoring procedures are being followed and enforced.

### Trailer Seals

- The sealing of trailers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of a carrier's commitment to C-TPAT. A high security seal must be affixed to all loaded trailers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.
- Based on risk, a high security barrier bolt seal must be applied to the door handle and/or a cable seal must be applied to the two vertical bars on the trailer doors.
- Clearly defined written procedures must stipulate how seals in the highway carrier's possession are to be controlled during transit. These written procedures should be briefed to all drivers and there should be a mechanism to ensure that these procedures are understood and are being followed. These procedures must include:
  - Verifying that the seal is intact, and if it exhibits evidence of tampering along the route.

## DRAFT 1 – October 1, 2005

- Properly documenting the original and second seal numbers.
- Verify that the seal number and location of the seal is the same as stated by the shipper on the shipping documents.
- If the seal is removed in-transit to the border, even by government officials, a second seal must be placed on the trailer, and the seal change must be documented.
- The driver must immediately notify the dispatcher that the seal was broken, by whom; and the number of the second seal that is placed on the trailer.
- The carrier must make immediate notification to the shipper, the customs broker and the importer of the placement of the second seal.

### **Less-than Truck Load (LTL)**

- LTL carriers must use a high security padlock or similarly appropriate locking device when picking up local freight in an international LTL environment. LTL carriers must ensure strict controls to limit the access to keys or combinations that can open these padlocks.
- After the freight from the pickup and delivery run is sorted, consolidated and loaded onto a line haul carrier destined to cross the border into the U.S., the trailer must be sealed with a high security seal which meets or exceeds the current PAS ISO 17712 standard for high security seals.
- In LTL or Pickup and Delivery (P&D) operations that do not use consolidation hubs to sort or consolidate freight prior to crossing the U.S. border, the importer and/or highway carrier must use ISO 17712 high security seals for the trailer at each stop, and to cross the border.
- Written procedures must be established to record the change in seals, as well as stipulate how the seals are controlled and distributed, and how discrepancies are noted and reported.
- In the LTL and non-LTL environment, procedures should also exist for recognizing and reporting compromised seals and/or trailers to U.S. Customs and Border Protection or the appropriate foreign authority.

### **Physical Access Controls**

Access controls prevent unauthorized entry to trucks, trailers and facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, and vendors at all points of entry. Employees and service providers should only have access to those areas of a facility where they have legitimate business.

- **Employees**  
An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.
- **Visitors / Vendors / Service Providers**  
Visitors, vendors, and service providers must present photo identification for documentation purposes upon arrival, and a log must be maintained. All visitors and service providers should be escorted and visibly display temporary identification.
- **Challenging and Removing Unauthorized Persons**  
Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

### **Personnel Security**

Written and verifiable processes must be in place to screen prospective employees and to periodically check current employees.

## DRAFT 1 – October 1, 2005

- **Pre-Employment Verification**  
Application information, such as employment history and references must be verified prior to employment.
- **Background checks / investigations**  
Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.
- **Personnel Termination Procedures**  
Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

### Procedural Security

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

Security procedures should be implemented that restricts access to the conveyance and prevents the lading of contraband while en-route from facilities in international locations to the United States.

Procedures must be in place to record and immediately report all anomalies regarding truck drivers to U.S. Customs and Border Protection. Random screening of truck driver luggage and personal effects should occur.

- **Documentation Processing**  
Procedures must be in place to ensure that all information used in the clearance of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Measures should also be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation
- **Document Review**  
Personnel should be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments that:
  - Originate from or are destined to unusual locations
  - Paid by cash or a certified check
  - Have unusual routing methods
  - Exhibit unusual shipping / receiving practices
  - Provide vague, generalized or poor information
  - All instances of a suspicious cargo shipment should be reported immediately to the nearest U.S. Customs and Border Protection port-of-entry.
- **Bill of Lading / Manifesting Procedures**  
Bill of lading information filed with CBP should show the first foreign location/facility where the highway carrier takes possession of the cargo destined for the United States. Additionally, to help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and timely.
- **Cargo**  
Cargo must be properly marked and manifested to include accurate weight and piece count. Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected - as appropriate.

**Physical Security**

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to conveyance, including concealment in trailers. Cargo handling and storage facilities, trailer yards, etc., must have physical barriers and deterrents that guard against unauthorized access. Highway carriers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

- **Fencing**  
Perimeter fencing should enclose the entire truck yard or terminal, especially areas where tractors, trailers and other rolling stock are parked or stored. All fencing must be regularly inspected for integrity and damage.
- **Gates and Gate Houses**  
Gates through which all vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.
- **Parking**  
Private passenger vehicles must be prohibited from parking in close proximity to parking and storage areas for tractors, trailers and other rolling stock that crosses the international border.
- **Building Structure**  
Buildings must be constructed of materials that resist unlawful entry. The integrity of 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 issuance of all locks and keys, to include the locks and keys for tractors. When parked in the yard, doors to tractors should be locked and the windows should be closed to prevent unauthorized access.
- **Lighting**  
Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, parking or storage areas for tractors, trailers, rolling stock, and fences.
- **Alarms Systems & Video Surveillance Cameras**  
Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to vessels, cargo handling and storage areas.

**Security Training and Threat Awareness**

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists at each point in the supply chain. Employees must be made aware of the procedures the highway carrier has in place to address a situation and how to report it.

Additionally, specific training should be offered to assist employees in maintaining trailer and tractor integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

**Information & Technology Security**

- **Password Protection**  
Measures should be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access. Automated systems must use individually assigned

## DRAFT 1 – October 1, 2005

accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

- **Accountability**

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

- **FAST Transponder Controls**

Transponders or any technology provided to the highway carrier by U.S. Customs and Border Protection to utilize the Free and Secure Trade (FAST) program must be protected against misuse, compromise, theft, tampering, altering or duplication.<sup>2</sup>

C-TPAT highway carriers must have documented procedures in place to manage the ordering, issuance, activation, and deactivation of FAST transponders. C-TPAT highway carriers are prohibited from requesting FAST transponders for any highway carrier company that is not owned and controlled by the C-TPAT approved highway carrier.

C-TPAT highway carriers are also prohibited from requesting FAST transponders for any owner-operator not under written contract to provide exclusive transportation services for the C-TPAT highway carrier.

---

<sup>2</sup> Any misuse of FAST technology, to include loaning FAST transponders to external carriers will result in suspension or removal from the FAST Program. FAST is a benefit based on trust and confidence.