Security Profile

For each of the sections below, you will be required to write a response and/or upload a document demonstrating how your company adheres to the stated requirement. There is no one right way to answer these questions- different solutions will be used successfully by different companies. It is important to provide detailed answers so that the Supply Chain Security Specialist who reviews your application has enough information to assess your company's application.

Business Partner Requirements, Security Procedures (Updated)

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.

- 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.
- 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.
- 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.

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. Click on the following link for guidance on conducting a risk assessment: http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/supply_chain/

Conveyance Security, Tractor and Trailer Integrity (Updated)

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

Conveyance Security, Conveyance Inspection Procedures

Using a checklist, drivers should be trained to inspect their conveyances 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, supervisory personnel or 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 conveyances. 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:

Tractors: Bumper/tires/rims, Doors/tool compartments, Battery box, Air breather, Fuel tanks, Interior cab, compartments/sleeper, Faring/roof

Trailers: Fifth wheel area - check natural compartment/skid plate, Exterior - front/sides, Rear - bumper/doors, Front wall, Left side, Right side, Floor, Ceiling/Roof, Inside/outside doors, Outside/Undercarriage

Conveyance Security, Trailer Security (Updated)

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 of any structural changes, such as a hidden compartment, discovered in trailers, tractors or other rolling-stock equipment that crosses the border. Notification should be made immediately to CBP, and in advance of the conveyance crossing the border. Notifications can be telephonically made to CBP's Anti-Terrorism Contraband Enforcement Team (A-TCET) at the port.

*C-TPAT recognizes the unique situation of the cross-border cartage industry in the Laredo, Texas corridor and encourages and endorses carriers to work within the supply chain to make a reasonable effort to ensure the integrity of trailers, especially during the cross-border segment.

Conveyance Security, Container Security

When transporting a container or trailer for a C-TPAT importer, a high security seal that meets or exceed the current PAS ISO 17712 standards for high security seals must be utilized.

Conveyance Security, 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. If driver logs are utilized, they must reflect that trailer integrity was verified.

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. Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting.

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.

During Department of Transportation Inspections (DOT) or other physical inspections on the conveyance as required by state, local or federal law, drivers must report and document any anomalies or unusual structural modifications found on the conveyance. In addition, Highway Carrier management should 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.

Conveyance Security, 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 may 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.

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/or the importer of the placement of the second seal.

Less-than Truck Load (LTL), Padlocks

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.

Less-than Truck Load (LTL), ISO 17712 seals

After the freight from the pickup and delivery run is sorted, consolidated and loaded onto a line haul carrier destined to the 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. These written procedures should be maintained at the terminal/local level.

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, 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.

Physical Access Controls, 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 visibly display temporary identification.

Physical Access Controls, Unauthorized Entry (Updated)

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.

Physical Access Controls, Challenging and Removing Unauthorized Persons

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Personnel Security (Updated)

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

Personnel Security, Pre-Employment Verification

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

Personnel Security, 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 Security, Personnel Termination Procedures

Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

Procedural Security (Updated)

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.

Procedural Security, 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, such as using a locked filing cabinet, should also be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation

Procedural Security, Document Review

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.

Procedural Security, 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.

Procedural Security, Supply Chain Security (Updated)

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to the conveyance including concealment in trailers.

Procedural Security, Cargo Discrepancies (Updated)

Procedures must be in place to record and immediately report all anomalies regarding truck drivers to U.S. Customs and Border Protection. If local, federal or state laws and union rules permit, conducting random screening of truck driver luggage and personal effects should occur.

Procedural Security, 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 (Updated)

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to conveyance, including concealment in trailers.

Physical Security, Unauthorized Access (Updated)

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.

Physical Security, 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.

Physical Security, 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.

Physical Security, 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.

Physical Security, Building Structure

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

Physical Security, 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.

Physical Security, 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.

Physical Security, 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, based on risk.

Security Training and Threat Awareness, Threat awareness program

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 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.

Information Technology Security, 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.

Information Technology Security, FAST Transponder Controls (Updated)

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.*

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.

*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.