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

Third party logistics providers must have written and verifiable processes for the screening and selection of business partners including foreign consolidators, customers, contractors, carriers, and vendors. Ensure that contracted service provider companies who provide transportation, cargo handling, and security services commit to C-TPAT Security Guidelines most closely associated with the particular enrollment sector. Periodically review the performance of the service providers to detect weakness or potential weaknesses in security. Third party logistics providers must refrain from the practice of subcontracting (to non CTPAT participants) beyond a second party or "double brokering" and ensure that other providers within their supply chain also do the same. Note: CBP believes double brokering weakens the supply chain as it lessens the accountability of those within the supply chain and puts the original stakeholder at a greater risk of supply chain incident.

Security Procedures, Point of Origin

C-TPAT Third party logistics providers must ensure business partners develop security processes and procedures consistent with the C-TPAT security guidelines to enhance the integrity of the shipment at point of origin.

Security Procedures, Participation/Certification in Foreign Customs Administrations Supply Chain Security Programs

Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the C-TPAT Third party logistics provider.

Security Procedures, Service Provider Screening and Selection Procedures

The C-TPAT Third party logistics provider must have documented service provider screening and selection procedures to screen the contracted service provider for validity, financial soundness, ability to meet contractual security requirements, and the ability to identify and correct security deficiencies as needed. Service Provider procedures should utilize a risk-based process as determined by an internal management team.

Security Procedures, Customer Screening Procedures

The C-TPAT Third party logistics provider must have documented procedures to screen prospective customers for validity, financial soundness, the ability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed. Customer screening procedures should utilize a risk-based process as determined by an internal management team.

Container Security (where applicable)

Third party logistics providers should ensure that all contracted service providers have procedures in place to maintain container integrity. Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded C-TPAT importer containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Container Security (where applicable), Container Inspection

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

- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/Outside doors
- Outside/Undercarriage

Container Security (where applicable), Container Seals

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers. Procedures must be in place for recognizing and reporting compromised seals and/or containers to U.S. Customs and Border Protection or the appropriate foreign authority. Only designated employees should distribute container seals for integrity purposes.

Container Security (where applicable), Container Storage

Containers 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 containers or container storage areas.

Conveyance Security (where applicable)

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

Conveyance Security (where applicable), Conveyance Inspection Procedures

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.

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

-Right side

-Floor

-Ceiling/Roof
-Inside/outside doors
-Outside/Undercarriage

Conveyance Security (where applicable), Trailer Security (where applicable)

All trailers in the third party logistics provider's custody, trailer integrity must be maintained, to protect against the introduction of unauthorized material and/or persons. Third party logistics providers must have procedures in place to maintain the integrity of their trailers at all times.

It is recognized that even though a third party logistics provider may not "exercise control" over the loading of trailers and the contents of the cargo, third party logistics provider 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 third party logistics provider must ensure that while in transit to the border, no loading of contraband has occurred, even in regards to unforeseen vehicle stops or trailer drops before final transit across the border. C-TPAT recognizes the unique situation of the cross-border cartage industry along the Southern Border corridors and encourages and endorses third party logistics providers to work within the supply chain to make a reasonable effort to ensure the integrity of trailers, especially during the cross-border segment.

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 third party logistics provider 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.

Conveyance Security (where applicable), Container Security

When transporting a container or trailer bound for the USA 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 (where applicable), Conveyance Tracking and Monitoring Procedures

Third party logistics providers 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. Third party logistics provider's 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.

Conveyance Security (where applicable), 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 third party logistics providers 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. Clearly defined written procedures must stipulate how seals in the third party logistics provider'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 all original and replacement 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 replacement 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 replacement second seal that is placed on the trailer.
- The third party logistics provider 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) (where applicable)

Shipments that are less-than-truckload must use a high security padlock or similarly appropriate locking device when picking up local freight in an international LTL environment. The third party logistics provider 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 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 third party logistics provider 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

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors and protect company assets. Access controls must include the positive identification of all employees, visitors and vendors at all points of entry.

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 Controls

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification.

Physical Access Controls, Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

Physical Access Controls, Challenging and Removing Unauthorized Persons

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

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, position held and submit such information to CBP upon written request, to the extent permitted by law.

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. 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

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.

Procedural Security, Documentation Processing

Procedures must be in place to ensure that all documentation used in the movement of merchandise/cargo is legible, complete, accurate and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

Procedural Security, Manifesting Procedures

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, Shipping & Receiving (where applicable)

Arriving cargo should be reconciled against information on the cargo manifest. Cargo weights, marks and labels, piece or carton count should be verified. Departing cargo should be checked against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

Procedural Security, Cargo Discrepancies

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

Security Training and Threat Awareness

As a liaison between CBP and the trade community, the third party logistics provider should create opportunities to educate those in the supply chain they do business with on C-TPAT policy, and those areas in which the third party logistics provider has relevant expertise, which might include security procedures, best practices, access controls, documentation fraud, information security, internal conspiracies, and technologies that further the goal of a secure global supply chain. These interactions should focus on employees working in shipping, information technology, receiving and mailroom processing. A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists at each point in the supply chain. Employees must be made aware of the employee response and reporting procedures the company has in place to address a security situations they may likely encounter. Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail. Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security (where applicable)

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. 3PL’s should incorporate the following C-TPAT physical security guidelines throughout their supply chains as applicable.

Physical Security (where applicable), 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 integrity and damage.

Physical Security (where applicable), Gates, Gate Houses

Gates through which 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 (where applicable), Parking

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

Physical Security (where applicable), 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 (where applicable), 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.

Physical Security (where applicable), Lighting

Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling, storage areas, fence lines and parking areas.

Physical Security (where applicable), Alarms Systems & Video Surveillance Cameras

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

Information Technology Security

Information Technology (IT) integrity must be maintained to protect data from unauthorized access or manipulation.

Information Technology Security, Password Protection

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.