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, General (Updated)

Unless otherwise expressly indicated, for purposes of implementing the minimum standards prescribed in this section, the term "business partner" will include all third parties within the supply chain with whom the Customs Broker voluntarily, and on its own initiative engages in the performance of its agency obligations for importer clients (but does not include those clients). Brokers must have written and verifiable processes for the screening of new business partners, beyond financial soundness issues, to include security indicators.

Written procedures must exist to address the specific factors or practices as determined by CBP as sufficient to trigger additional scrutiny of the import transaction as informed by U.S. Customs and Border Protection (CBP). CBP will work in partnership with the brokers to identify specific information regarding what factors, practices or risks are relevant.

For business partners eligible for C-TPAT certification, the Customs Broker must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are, or are not C-TPAT certified. 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 broker. To the extent such information can be obtained, brokers will maintain secure provider lists of C-TPAT certified (or equivalent) service providers in all relevant categories.

For client-importers, brokers must ensure that C-TPAT security criteria is provided by making educational opportunities available through seminars, through consultative services, dissemination of text materials, and/or through providing assistance to clients in obtaining such materials on the CBP website or elsewhere, when requested. The brokers must develop and document a process for handling security related client-importer inquiries. Brokers should encourage client-importers to join the C-TPAT program.

U.S. Customs Brokers must conduct a comprehensive assessment of their security practices based upon the following C-TPAT minimum-security criteria. Click on the following link for

guidance on conducting a risk assessment:
http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/supply_chain/

Container and Trailer, Security

Customs Brokers must convey to their business partner importers, whether a C-TPAT member or not, concerning the criticality of having security procedures in place at the point of stuffing, procedures to inspect, properly seal and maintain the integrity of the shipping containers and trailers. Customs Brokers should also convey to their business partners, that the seven-point inspection process for empty containers prior to the loading the cargo, as well as the seventeen-point inspection process for all trailers/tractors, should be followed and can be found on the C-TPAT Secure Communications Portal, under 'Document Exchange'.

Container and Trailer, Seals

The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and the broker should convey to their business partners that seals used to secure loaded containers and trailers bound for the U.S. must meet or exceed the current PAS ISO 17712 standards for high security seals.

Remind all client-importers that all loaded U.S.-bound containers and trailers must have a PAS ISO 17712 high-security seal affixed.

When necessary, the broker should also inform their business partners that they must institute procedures for recognizing and reporting compromised seals to CBP or the appropriate foreign authority.

Physical Access Controls, Employees

For all brokers, procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented. In addition, for broker facilities at which there is in excess of 50 employees, a security identification system must be in place for positive identification and access control purposes, under which company management or security personnel will maintain and adequately control the issuance and return of employee photo identification badges, or equivalent control.

Physical Access Controls, Visitors

For documentation purposes, unknown visiting persons should be required to present photo identification upon arrival and should be escorted while on the broker's premises. The broker should maintain a logbook or electronic diary of all unknown visiting persons, recording such data as visitor name, purpose of visit and confirmation of identity. In addition, for the broker category of facilities in excess of 50 employees, all visitors/vendors should be provided temporary identification badges upon arrival, to be visibly displayed at all times while on the brokers premises.

Physical Access Controls, Building Security (Updated)

Access controls to 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 and visitors at all points of entry.

Physical Access Controls, Challenging and Removing Unauthorized Persons

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

Physical Access Controls, Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival of all first time/unknown vendors or vendor representatives. At times of heightened alert involving package and mail delivery, these items should be screened before being disseminated.

Physical Access Controls, Personnel Security

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

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

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

Procedural Security, General

Security measures must be in place to ensure the integrity of any data or documents relevant to security of processes, transportation, handling, and storage of cargo in the supply chain.

Customs Brokers should notify CBP and/or other law enforcement agencies, as specified by CBP for these purposes, whenever anomalies or illegal activities related to security issues are detected or suspected.

Documentation Processing, General

Measures should be in place to ensure that data transmitted by the Customs Broker is of optimal quality in order for CBP to maximize the use of automated targeting and other screening tools for cargo release or designation for a physical examination. Procedures must be in place to ensure that all information provided by the importer/exporter, freight forwarder, etc., and used in the clearing of merchandise/cargo, is legible and protected against the exchange, loss or introduction of erroneous information.

Documentation controls for the broker, should include procedures for:

Ensuring the consistency of information transmitted to CBP through the entry summary process with the information that appears on the transaction documents provided to the broker, with regard to such data as the supplier and consignee name and address, commodity description, weight, quantity, and unit of measure (i.e. boxes, cartons, etc.) of the cargo being cleared.

Review of documentation for completeness and clarity and contacting the business partner or importer/exporter, as necessary, to obtain corrected documentation or information.

To the extent such information comes to the broker’s attention, alerting the importer/exporter of its obligation to notify CBP and/or any other appropriate law enforcement agency of any errors and/or shortages and overages of merchandise that create a security risk in the supply chain, and providing assistance that is consistent with its for hire services in making such notification and correction of data as may be required or requested by the importer/exporter.

Documentation Processing, Advanced Submission of Data

C-TPAT importers who are currently NOT filing entry prior to the arrival of their cargo in the port of arrival are not receiving their full C-TPAT benefits, especially reduced examinations.

To fully realize the reduced cargo examinations afforded to certified and validated C-TPAT importers, entry must be made to CBP as early in the importation process as possible, and at a minimum, of 24 hours prior to the cargo arriving to the first port of entry within the United States. The reason this is necessary is that C-TPAT benefits are aligned with a C-TPAT members' importer of record number. The importer of record number only becomes known when entry is filed; importer of record numbers are not identified on manifest information. To receive full benefits, the entry should be filed prior to arrival of the cargo.

This applies only to cargo imported via ocean transport (sea containers), and not to cargo arriving via other modes of transport.

Documentation Processing, Cargo Discrepancies

All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities anomalies are detected or suspected- as appropriate. The broker will insure that the client-importer is aware of the following:

The discrepancy or anomaly must be fully investigated.

CBP and/or other appropriate law enforcement agencies, as appropriate, should be notified of such discrepancy or anomaly.

Consistent with its for hire services, the broker can assist in the reporting of the anomaly, and will make appropriate modifications in the transmission of entry data.

Documentation Processing, Shipping & Receiving

Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before the cargo is received or released. Procedures should also be established to track the timely movement of incoming goods.

Physical Security, Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities. When required by CBP, 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, Gates and Gate Houses

Security 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, Parking

Where substantially comparable alternative parking is available, private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

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, Building Security (Updated)

Cargo handling and storage facilities, as well as those facilities used to make entry of international cargo, must have physical barriers and deterrents that guard against unauthorized access. Brokers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable. (Note: C-TPAT is cognizant of the diverse business models that Brokers employ and takes into consideration that the physical security measures outlined in this document may not correspond to the business model of some C-TPAT brokers.

Physical Security, Lighting

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

Physical Security, Alarms Systems & Video Surveillance Cameras

When reasonably and specifically required by CBP, alarm systems and video surveillance cameras must be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Physical Security, Physical Security

Cargo handling and storage facilities, as well as those facilities used to make entry of the international cargo, must have physical barriers and deterrents that guard against unauthorized access.

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. Office buildings must have after hour access limited.

Information Technology Security, General

Measures must be in place to safeguard computer access and information. 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, 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, System and Data Protection

Anti-virus and anti-spy ware should be installed and kept current in Customs Broker computer systems susceptible to infiltration.

Security Training and Threat Awareness

As a liaison between CBP and trade community, the broker should create opportunities to educate the importing community on C-TPAT policy, and those areas in which the broker 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 security awareness program should also include notification being provided to CBP and other law enforcement agencies whenever anomalies or illegal activities related to security are detected or suspected.