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

Air carriers must have written and verifiable processes for the screening of business partners, including carrier's agents and service providers. Air carriers must also have screening procedures for new customers, beyond financial soundness issues to include indicators of whether the customer appears to be a legitimate business and/or posses a security risk. Air carriers must also have procedures to review their customer's requests that could affect the safety of the aircraft or the cargo or otherwise raise significant security questions, including unusual customer demands.

Air Carriers 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/

Business Partner Requirements, Security Procedures

Written or web-based procedures must exist for screening business partners which identify specific factors or practices, the presence of which would trigger additional scrutiny by the air carrier, up to and including a detailed physical inspection of the customer's cargo container/ULD prior to loading onto the aircraft. Particular attention should be given to house-to-house customer loaded containers/ULD.

Business Partner Requirements, C-TPAT Business Partners

For those business partners eligible for C-TPAT certification (importers, consolidators, etc.) the air 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 should be subject to additional scrutiny by the air carrier.

Business Partner Requirements, Contract Aircraft Service Providers

Air carriers should ensure that contract aircraft service providers commit to C-TPAT security recommendations through contractual agreements. Periodic reviews of the security commitments of the service providers should be conducted to detect weaknesses, or potential weaknesses, in security.

Business Partner Requirements, Participation/Certification in Foreign Customs Administrations Supply Chain Security Programs

Likewise, 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 air carrier.

Container or Unit Load Devices (ULD) Security

Air carriers must employ the use of high security seals (if and when applicable) and an accountable seal tracking process where cargo is transported via international cargo conveyance containers such as a ULD. In instances where cargo is not transported in a ULD, verifiable security methods must be put in to place to ensure, to the greatest extent possible, cargo is rendered tamper resistant and/or tamper evident. For all containers/ULDs in the air carrier's custody, container/ULD integrity must be maintained, to protect against the introduction of unauthorized material and/or persons. Air carriers must have documented procedures in place to maintain the integrity of the shipping containers/ULD and pallets in their custody. When an air carrier allows a ULD to leave their control, formal, verifiable procedures must be in place to track the ULD and it's return into the carrier's custody.

Special considerations and security procedures must be developed for passenger flights carrying cargo. These processes must be documented and verifiable. Security procedures for passenger aircraft transporting cargo must include more intrusive examination of the cargo prior to packaging and loading, such as x-ray inspections, based on written articulated risk indicators. Security procedures during transport from the cargo area to the aircraft should be identified and known by all employees involved in the transportation.

Container or Unit Load Devices (ULD) Security, Container/ULD Inspection

Air carriers must recognize the importance of a comprehensive inspection process prior to loading. The requirement to inspect all containers/ULDs, when used, prior to stuffing is placed upon the importers through the C-TPAT Minimum Security Criteria for Importers dated March 25, 2005, yet air carriers must visually inspect all aircraft cargo hold areas, the exterior of any

container/ULD, and the interior of the empty container/ULD, at the foreign port of lading. A seven-point inspection process is required for all empty containers/ULDs:

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

Container or Unit Load Devices (ULD) Security, Container/ULD Seals

When containers/ULDs are used, written procedures must stipulate how seals in the air carrier's possession are to be controlled, and only designated employees must distribute seals for integrity purposes. Procedures should also exist for recognizing and reporting compromised seals and/or containers/ULDs to U.S. Customs and Border Protection or the appropriate foreign authority.

Container or Unit Load Devices (ULD) Security, Container/ULD Storage

Containers/ULD 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 container/ULD or container/ULD storage areas.

Physical Access Controls (Updated)

Access controls prevent unauthorized entry to aircraft 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. Contracted employees and service providers should only have access to those areas of the aircraft or facilities where they have legitimate business. Companies who contract for day workers or employ contract workers within warehouses or other areas not requiring airport or federal regulated badges, should include in their contract with the personnel providers that supplied workers for international cargo areas have undergone a security background check.

Physical Access Controls, Boarding and Disembarking of Aircraft

Consistent with the air carrier's security plan, all crew, employees, vendors and visitors are subject to a search when boarding or disembarking flights departing to or arriving from foreign. All crewmembers, employees, vendors, and visitors must display proper identification.

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 be escorted and visibly display temporary identification. Procedures must be in place to examine containers/ULDs added to the aircraft by service providers (i.e. food carts). C-TPAT members contracting vendors and service providers not eligible for participation in C-TPAT must, by contract, require the providers to adhere to the minimum-security requirements for C-TPAT.

Physical Access Controls, Cargo Delivery Areas

Delivery of goods to the consignee or other persons accepting delivery of cargo at the carrier's facility should be limited to a specific monitored area.

Personnel Security (Updated)

In compliance with applicable laws and regulations for that location, written and verifiable processes must be in place to screen prospective employees and to periodically check current employees.

Physical Access Controls, Challenging and Removing Unauthorized Persons

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

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 immediately remove identification, facility, and system access for terminated employees.

Procedural Security/Manifesting Procedures (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. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to aircrafts, including concealment in cargo.

Procedural Security, Passenger and Crew

Air carriers must ensure compliance with the Advance Passenger Information System requirements so that accurate, timely and advanced transmission of data associated with international passengers and crew is provided to CBP. Procedures must be in place to record and report all anomalies regarding passenger and/or crew to U.S. Customs and Border Protection or other law enforcement agencies.

Procedural Security, Bill of Lading / Manifesting Procedures

Procedures must be in place to ensure that the information in the carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent, and is filed with CBP in a timely manner. Documentation control must include safeguarding computer access and information.

Bill of lading information filed with CBP should show the first foreign port (place) where the air carrier takes possession of the cargo destined for the United States.

Procedural Security, Cargo

Cargo must be properly marked and manifested to include accurate weight and piece count. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected - as appropriate. Procedures to separate domestic cargo from international cargo in warehouses or pre-staging areas should be in place.

Procedural Security, Aircraft

Upon arrival of an international flight, the air carrier will provide CBP with assistance, upon request, to conduct intensive aircraft searches when deemed appropriate by CBP. Aircraft searches will be conducted by CBP Officers who will maintain the integrity of the aircraft and control entrance and egress until the aircraft search is compete.

Procedures must be in place to conduct physical inspections of the aircraft prior to loading of cargo or passenger. This will include:

- Inspection of all baggage hold areas
- Inspection of all overheads
- Inspection of all lavatories
- Inspection of all galleys and food carts
- Inspection of the cockpit and electronics areas
- Exterior inspection of all wheel wells and landing gears
- Inspection of avionic compartments/bays as warranted

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 terrorists at each point in the supply chain. Employees must be made aware of the procedures the air carrier has in place to address a situation and how to report it.

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

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. Conduct periodic unannounced

security checks to ensure that all procedures are being performed in accordance with defined guidelines.

Physical Security (Updated)

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to the aircraft. Such measures are also covered by a facility's security plan. Cargo handling and storage facilities, container/ULD yards, and aircraft, in domestic and foreign locations, must have physical barriers and deterrents that guard against unauthorized access. Air carriers should incorporate the following C-TPAT physical security criteria throughout their supply chains as applicable.

Physical Security, Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities, container/ULD yards, and terminals. All fencing must be regularly inspected for integrity and damage.

Physical Security, Gates and 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, Parking

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

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.

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

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

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.