

C-TPAT Security Criteria

Sea Carriers

Sea carriers must conduct a comprehensive assessment of their international supply chain security practices based upon the following C-TPAT minimum security criteria. Where a sea carrier does not control a specific element of their supply chain, such as a port, terminal, direct handling of cargo containers, or process subject to these criteria, the sea carrier must work with these business partners to ensure that pertinent security measures are in place and adhered to throughout their supply chain. The sea carrier has ultimate responsibility for all cargo loaded on board their vessel. The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution – and recognizes the diverse business models C-TPAT members employ.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk.¹ 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.

C-TPAT also acknowledges that sea carriers are already subject to defined security mandates created under the International Ship and Port Security code (ISPS) and the Maritime Transportation Security Act (MTSA). It is not the intention of C-TPAT to duplicate these vessel and facility security requirements, rather, C-TPAT seeks to build upon the ISPS and MTSA foundation and require additional security measures and practices which enhance the overall security throughout the international supply chain.

ISPS and MTSA compliance are a prerequisite for C-TPAT sea carrier membership, and only vessels in compliance with the applicable ISPS code requirements may be utilized by C-TPAT members. Marine terminals operated by C-TPAT members must also comply with ISPS code requirements.

Business Partner Requirements

Sea carriers must have written and verifiable processes for the screening of business partners, including carrier's agents and service providers, as well as screening procedures for new customers, beyond financial soundness issues to include security indicators.

- **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 sea carrier, up to and including a detailed physical inspection of the suspect customer's container prior to loading onto the vessel.

For those business partners eligible for C-TPAT certification (importers, ports, terminals, brokers, consolidators, etc.) the sea 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 sea carrier.

Sea carriers should ensure that contract vessel services providers commit to C-TPAT security recommendations. Periodic reviews of the security commitments of the service providers should be conducted to detect weaknesses, or potential weaknesses, in security.

¹ Sea 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, ports identified by U.S. Coast Guard as having inadequate security, past security incidents, etc.).

DRAFT 1 – November 1, 2005

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 sea carrier.

- **Non-Vessel Operating Common Carriers**

Written procedures must exist which identify specific factors or practices which may deem a shipment from an NVOCC of greater risk, and appropriate measures must then be undertaken by the sea carrier, up to and including examination of the container prior to loading, or refusal to load the container.

Container Security

For all containers in the sea carrier's custody, container integrity must be maintained, to protect against the introduction of unauthorized material and/or persons. Sea carriers must have procedures in place to maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

Sea carriers must also fully comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

- **Container Inspection**

Sea carriers must recognize the importance of a comprehensive container inspection process prior to loading, to include the reliability of the locking mechanisms of the doors. The requirement to inspect all containers prior to stuffing is placed upon the importers through the C-TPAT Minimum Security Criteria for Importers dated March 25, 2005, yet sea carriers must visually inspect all empty containers, to include the interior of the container, at the foreign port of lading. A seven-point inspection process is recommended for all empty containers:

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

- **Container Seals**

Written procedures must stipulate how seals in the sea carrier's possession are to be controlled, and only designated employees should distribute container seals for integrity purposes. Procedures should also exist for recognizing and reporting compromised seals and/or containers to US Customs and Border Protection or the appropriate foreign authority consistent with the seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

- **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.

Physical Access Controls

Access controls prevent unauthorized entry to vessels 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. Shore employees and service providers should only have access to those areas of the vessel where they have legitimate business. Vessel and facility access controls are also governed by the International Ship and Port Security code

DRAFT 1 – November 1, 2005

- **Boarding and Disembarking of Vessels**
Consistent with the vessel's ISPS security plan, all crew, employees, vendors and visitors are subject to a search when boarding or disembarking vessels. A vessel visitor log must be maintained and a temporary visitor pass must be issued. All crewmembers, employees, vendors and visitors must display proper identification.
- **Crewmen Control – Deserter/Absconder Risk**
Written procedures must exist which identify specific factors which may indicate that a crewman poses a potential risk of desertion/absconding. Added security measures appropriate to the risk present should be employed upon arrival into the U.S. port/territories.
- **Deserter/Absconder Notifications**
Vessel masters must account for all crewmen prior to the vessel's departure. If the vessel master discovers that a crewman has deserted or absconded, the vessel master must report this finding by the most practical means to CBP immediately upon discovery and prior to the vessel's departure.
- **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.

- **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. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to vessel, including human concealment in containers. Procedures must include pre-departure vessel security sweeps for stowaways.

DRAFT 1 – November 1, 2005

- **Passenger and Crew**

Sea carriers must ensure compliance with the U.S. Coast Guard Notice of Arrival requirements so that accurate, timely and advanced transmission of data associated with international passengers and crew is provided to the U.S. government and 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. In accordance with ISPS vessel security plans, identification protocols and entry/exit logs must be maintained, and random screening of baggage and personal effects should occur.

- **Documentation Processing**

Procedures must be in place to ensure that all information used in the clearing 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.

- **Bill of Lading / Manifesting Procedures**

Bill of lading information filed with CBP should show the first foreign port (place) where the sea 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.

- **BAPLIEs**

At the request of CBP, sea carriers will provide a requested BAPLIE and/or stowage plan, in a format readily available. Such requests will be honored 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.

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 sea carrier has in place to address a situation and how to report it.

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

Physical Security

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

- **Fencing**

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

- **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.

DRAFT 1 – November 1, 2005

- **Parking**
Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and vessels.
- **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.
- **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. While at port, the pier and waterside of the vessel must be adequately illuminated.
- **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.

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.
- **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.