

Final – March 1, 2006

C-TPAT Security Criteria Sea Carriers

Sea carriers must conduct a comprehensive assessment of their security practices based upon the following C-TPAT minimum-security criteria. Where a sea carrier does not control a specific element of the cargo transportation service it has contracted to provide, such as marine terminal operator or a time chartered vessel with whom it has contracted, the sea carrier must work with these business partners to seek to ensure that pertinent security measures are in place and adhered to. The sea carrier is responsible for exercising prudent oversight for all cargo loaded on board its vessel, pursuant to applicable law and regulations and the terms of this program.

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. Security measures, as listed throughout this document, must be implemented and maintained as appropriate to the carrier's business model and risk understanding. CBP's C-TPAT validation process shall include a review of the carrier's assessment and program.

C-TPAT recognizes 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. The Physical Access Controls and Physical Security provisions of these criteria are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and Coast Guard regulations.

Business Partner Requirements

Sea carriers must have written and verifiable procedures for the screening of carrier's agents and service providers contracted to provide transportation services for the carrier. Sea 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 poses a security risk. Sea carriers shall also have procedures to review their customer's requests that could affect the safety of the vessel or the cargo or otherwise raise significant security questions, including unusual customer demands, such as specific stowage placement aboard the vessel (beyond a request for below deck or on deck stowage).

- **Security procedures**

Sea carriers must have written or web-based procedures for screening new customers to whom they issue bills of lading, 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 exterior of the suspect customer's container prior to loading onto the vessel. These procedures may also include a referral to CBP or other competent authorities for further review. CBP will work in partnership with the sea carriers to identify specific information regarding what factors, practices or risks are relevant.

¹ Sea carriers shall have a documented and verifiable process for assessing security vulnerabilities within their operations based on their business model (i.e., volume, country of origin, routing, security alerts via open source information, ports identified by U.S. Coast Guard as having inadequate security, past security incidents, etc.).

Final – March 1, 2006

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.²

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 while in their custody. A high security seal must be affixed to all loaded containers bound for the U.S. All seals used or distributed by the sea carrier must meet or exceed the current PAS ISO 17712 standards for high security seals³.

Sea carriers and/or their marine terminal operators must have processes in place to comply with seal verification rules and seal anomaly reporting requirements once promulgated and mandated by the U.S. government.

- **Container Inspection**

The requirement to inspect all containers prior to stuffing (to include the reliability of the locking mechanisms of the doors) is placed upon the importers through the C-TPAT Minimum Security Criteria for Importers dated March 25, 2005. Sea carriers must visually inspect all U.S.-bound empty containers, to include the interior of the container, at the foreign port of lading

- **Container Seals**

Written procedures must stipulate how seals in the sea carrier's possession are to be controlled. 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**

The sea carrier must store containers in their custody in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting detected, unauthorized entry into containers or container storage areas to appropriate local law enforcement officials.

Physical Access Controls

The sea carrier shall establish access controls to prevent unauthorized entry to its vessels and cargo facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, government officials and vendors at all restricted access 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 governed by the International Ship and Port Security Code and MTSA. The Physical Access Control provisions of these criteria are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and MTSA regulations.

- **Boarding and Disembarking of Vessels**

Consistent with the vessel's ISPS security plan, all crew, employees, vendors and visitors may be subject to a search when boarding or disembarking vessels. A vessel visitor log must be maintained and a temporary visitor pass must be issued as required by the vessel's security plan. All

² An ISPS regulated vessel operator or port facility is not expected under these criteria to show a carrier or other third party its ship or port security plan. It is recognized that under the ISPS Code relevant portions of an ISPS security plan are not subject to inspection without the contracting government's agreement.

³ When a container has been affixed with a high security seal that meets or exceeds the current PAS ISO 17712 standards and the shipper or carrier wishes to apply a supplementary, additional seal to the container to provide enhanced level of security, such supplementary seals do not have to meet the PAS ISO 17712 standards.

Final – March 1, 2006

crewmembers, employees, vendors and visitors, including government officials, must display proper identification, as required by the applicable ISPS/MTSA security plan.

- **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, government officials, and service providers must present photo identification for documentation purposes upon arrival at carrier's vessels or cargo facilities, and a visitor log must be maintained. Measures described by the approved ISPS/MTSA security plan addressing the escort of visitors and service providers, including, when appropriate, the use of temporary identification will be followed.

- **Challenging and Removing Unauthorized Persons**

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

Personnel Security

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.

- **Pre-Employment Verification**

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

- **Background checks / investigations**

Depending on the sensitivity of the position, background checks and investigations shall be conducted for prospective employees as appropriate and as required by foreign, federal, state and local regulations. 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.

- **Crewmen Control – Deserter/Absconder Risk**

CBP will work with the U.S. Coast Guard and sea carriers to identify specific factors which may indicate when a crewman poses a potential risk of desertion/absconding. When such factors are identified and provided to the carriers, the carrier shall provide this information to its vessel masters and to the vessels under charter to the carrier, and such vessels shall establish procedures to address the 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 from a U.S. port. 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.

Final – March 1, 2006

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. Consistent with the carrier's ISPS Code security plan, procedures must be in place to prevent unauthorized personnel from gaining access to the vessel. In those geographic areas where risk assessments warrant checking containers for human concealment in containers, such procedures should be designed to address the particular, identified risk at the load port or the particular port facility. CBP will inform the sea carriers when it is aware of a high risk of human concealment or stowaways at particular ports or geographic regions. Documented procedures must also include pre-departure vessel security sweeps for stowaways at the foreign load port, and during normal watch activity while en route to the United States as warranted by risk conditions at the foreign load port.

- **Passenger and Crew**

Sea carriers must ensure compliance with the U.S. Coast Guard Notice of Arrival and Departure 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.

- **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 sea carrier takes possession of the cargo destined for the United States.

- **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 made on a voyage specific basis when CBP requires additional voyage information and will be honored by the sea carrier in a timely manner. CBP recognizes that these are not regulated documents and that the data included may not always match the manifest filing.

- **Cargo**

Customs and/or other appropriate law enforcement agencies must be notified if illegal or highly suspicious activities are detected - as appropriate.

Security Training and Awareness

A security awareness program should be established and maintained by the carrier to recognize and foster awareness of security vulnerabilities to vessels and maritime cargo. Employees must be made aware of the procedures the sea carrier has in place to report a security concern or incident.

Additionally, specific training should be offered to assist employees in maintaining vessel and cargo integrity, recognizing internal conspiracies, and protecting access controls.

Physical Security

Carriers shall establish written and verifiable procedures to prevent unauthorized personnel from gaining access to its vessels, including concealment in containers, and to prevent tampering with cargo conveyances while they are in the carrier's custody. Such measures are covered by a vessel's and a port facility's ISPS security plan. Physical Security provisions of these criteria are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and MTSA regulations. Non-ISPS Code regulated cargo handling and storage facilities and container yards operated by the carrier, 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 as applicable.

Final – March 1, 2006

- **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 and secured when not in use.
- **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**
At those locations determined appropriate by the carrier's risk assessment, 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.

Security Assessment, Response and Improvement

Carriers and CBP have a mutual interest in security assessments and improvements, and recognize that specific, implemented security procedures may be found in the future to have weaknesses or be subject to circumvention. When a security shortcoming or security incident is identified, the Carrier and CBP officials will meet in an effort to ascertain what led to the breakdown and to formulate mutually agreed remedial measures. If CBP determines that the security incident raises substantial concerns or a security weakness requires substantial remediation, CBP headquarters officials will meet with the carrier's senior management to discuss such concerns and to identify appropriate remedial measures to be taken.

Final – March 1, 2006

While CBP has the authority to suspend or remove a sea carrier from the C-TPAT program for substantial non-compliance with the security criteria of the program, such authority is exercised only in the most serious circumstances.