

August 2007

**Customs-Trade Partnership Against Terrorism (C-TPAT)
Minimum-Security Criteria
U.S and Foreign-Based Marine Port Authority and Terminal Operator (MPTO)**

Eligibility for C-TPAT

Eligibility for U.S. based MPTO

- An active U.S. Marine or Port Terminal Operator (MPTO) in the U.S.
- Must handle cargo vessels arriving from international locations.
- Have a business office staffed in the U.S.
- Have an active Federal Maritime Commission (FMC) Marine Terminal Operator (MTO) 6-digit FMC MTO number
- Have a designated company officer that will be the primary cargo security officer responsible for C-TPAT

Eligibility for foreign-based MPTO

- An active MPTO in an international location that received an invitation from U.S. Customs and Border Protection (CBP) to join C-TPAT.
- Must handle cargo vessels departing to the U.S.
- Have a designated company officer that will be the primary cargo security officer responsible for C-TPAT

Introduction

U.S. and Foreign-based Marine Port Authority and Terminal Operators (MPTO) must conduct a comprehensive assessment of their security practices based upon the following C-TPAT minimum-security criteria. C-TPAT recognizes the complexity of marine port and terminal operations 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 C-TPAT member's business model, the port's geography, the commodities handled at the port and the terms and conditions of the lease agreement between the Marine Port Authority and the Terminal Operator.

C-TPAT is also cognizant of the unique role and relationship between Marine Port Authority and Terminal Operators situation regarding terminal operators who operate as tenants within a marine port. For C-TPAT purposes, each terminal operator must implement the C-TPAT security criteria within the physical area and processes within the terminal operator's area of control and responsibility. Where a marine port authority does not control a specific process or element of the supply chain, such as a sea carrier, terminal operator or independent contractor, the MPTO should work with these business partners to seek to ensure that pertinent security measures are in place and adhered to within the overall port.

C-TPAT recognizes that MPTOs 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

¹ Marine Port & Terminal Operators 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 of incoming vessels and cargo, foreign ports identified by U.S. Coast Guard as having inadequate security routing of incoming vessels/cargo, security alerts via open source information, past security incidents, etc.).

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 MPTO membership, and only terminals in compliance with the applicable ISPS code requirements may be utilized by C-TPAT members. 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.

CBP and Foreign Customs Initiatives

As a C-TPAT member you are playing an important role as part of CBP's comprehensive strategy to enhance cargo and container security. Other initiatives under this strategy include the Trade Act 24-Hour Rule, the utilization of Non-Intrusive Inspection Technology and the Container Security Initiative (CSI), and the Secure Freight Initiative (SFI).

- While much of the burden of these initiatives fall upon the Carrier and the Importer, your role as a C-TPAT MPTO requires your full cooperation with these entities, as appropriate, in areas consisting of inspection, timely submission of trade data, cargo/container movement and high risk targeting. If you are an MPTO operating in an international port with a CSI contingent, you should make every effort to maintain regular liaison with the Team Leader of the CSI contingent, as a forum to discuss supply chain security issues and to gauge and evaluate current approaches to security and targeting.
- **Participation/Certification in a Foreign Customs Administration Supply Chain Security Program**
Foreign-based MPTOs who have obtained a certification in a supply chain security program being administered by Foreign Customs Administration should indicate their status of participation to their business partners.

Business Partner Requirements

MPTOs must have written and verifiable procedures for the screening of service providers contracted to provide services within the confines of the port or terminal. MPTO 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.

- **Security Procedures**
MPTO must have written, or web-based procedures for screening new customers, which identify specific factors or practices, the presence of which would trigger additional scrutiny by the MPTO, 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. If you are an MPTO operating in an international port with a CSI contingent, the referral should be made to the CSI Team Leader, as well as to local authorities. CBP will work in partnership with the MPTO to identify specific information regarding what factors, practices or risks are relevant.

MPTO should ensure that contract service providers commit to C-TPAT security recommendations. Periodic reviews of the security commitments of the service providers should be conducted.

Container Security

For all containers in the MPTO's custody, container integrity and breach detection measures should be maintained to protect against intrusion by unauthorized persons attempting to commit an internal conspiracy, or modifications (false compartments). During operational procedures consisting of cargo loading, handling and processing MPTOs should make every attempt to visually inspect containers to detect any breaches.

- **Container Storage**

The MPTO 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. If you are an MPTO operating in an international port with a CSI contingent the report should also be made to the CSI Team Leader. Cargo that is allowed for storage for an extended period of time should have documentation readily available that describes the contents. Containers should be segregated according to HAZMAT and temporary storage designations. MPTOs should institute practices to routinely check storage areas for cargo/containers. Empty containers should be checked to ensure that they are empty, and devoid of false compartments.

- **Container Seals**

Procedures should exist for recognizing and reporting compromised seals to U.S. Customs and Border Protection, appropriate foreign authorities or to the CSI Team Leader if you are an MPTO operating in an international port with a CSI contingent. MPTOs should make every attempt to visually inspect containers to ensure that an PAS ISO 17712 high security seal is affixed to the container and to detect any tampering or container breaches.

Physical Access Controls

The MPTO shall establish access controls to prevent unauthorized entry to cargo facilities and maintain control of employees, service providers and visitors. Access controls must include the positive identification of all employees, service provider (especially truck drivers), government officials and vendors at all restricted access points of entry. Port and terminal employees and service providers should only have access to those areas of the port where they have legitimate business. 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.

- **Security Personnel**

The MPTO should ensure that security guards are manning entry and exit gates, and should include roving patrols to monitor sensitive areas, and areas that handle and store cargo.

MPTO security personnel should conduct routine liaison with government police personnel assigned to the port, and vessel security personnel. If a Facility Security Officer (FSO) has been designated per MTSA/ISPS, the FSO should be the MPTO's point-of-contact for all C-TPAT's matters relating to security.

- **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.

- **Searches**

All individuals and vehicles entering and leaving the terminal should be required to enter or exit through a gate with a guard and must be made aware that they are subject to be searched. The right to search must be in accordance with the right of local, federal and labor laws.

- **Visitors / Vendors / Service Providers**

Visitors, vendors, government officials, and service providers must present photo identification for documentation purposes upon arrival at MPTOs facility, and a visitor log must be maintained. Identification must be checked to ensure that it is valid, i.e., drivers license or a government issued identification card that is not expired. Visitors, vendors and service providers should also state where they are proceeding to within the port to conduct business.

Passengers accompanying service providers (truck drivers) should also be challenged to determine the reason for entering the port. Measures described by the approved MTSA/ISPS security plan addressing the escort of visitors and service providers, including, when appropriate, the use of temporary identification will be followed. For U.S. MPTOs, once fully implemented, the provisions of the Transportation Workers Identity Card (TWIC) will serve to satisfy the criteria of providing valid identification.

- **Challenging and Removing Unauthorized Persons**

Procedures must be in place to identify, challenge and address trespassers, unauthorized or unidentified persons. If individuals are encountered that appear to be stowaways, or absconders from vessels, CBP personnel at domestic ports must be notified immediately. If you are operating in an international location the appropriate foreign authorities must be notified, in addition to the CSI Team Leader if you are operating in a port with a CSI contingent.

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. Once fully implemented, the provisions of the Transportation Workers Identity Card (TWIC) will serve to satisfy the criteria of conducting background checks of U.S. MPTO employees.

- **Pre-Employment Verification**

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

- **Background checks / Investigations**

In accordance with foreign, federal, local, and state laws, background checks and investigations must be conducted for prospective employees as appropriate. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**

MPTOs 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, control, release, and storage of cargo. Procedures must be in place to prevent unauthorized personnel from gaining access to the port or terminal facility, and containers. MPTOs receiving container and vessels from overseas ports of departure that have a known propensity for human concealment in containers, should implement procedures designed to address this particular risk upon arrival of the vessel and containers at the port. CBP will inform the MPTO when it is aware of a high risk of human concealment or stowaways at particular ports or geographic regions. In domestic U.S. locations, CBP and/or other appropriate law enforcement agencies must be notified if illegal or highly suspicious activities are detected - as appropriate. In international locations, appropriate law enforcement agencies and the Team Leader of the local CSI contingent should be notified.

- **Cargo Controls**

Cargo should be tallied at the time of delivery to the consignee or his agent. In the event of any discrepancies at the time of delivery, a manifest discrepancy report must be completed and provided to CBP. In cases of improper diversion or delivery of cargo/containers, MPTO must notify CBP or appropriate foreign authority.

- **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.

- **Container Opening**

If containers are opened for inspection by Customs or other authorities, the container doors should immediately be closed, locked and resealed immediately upon completion of the inspection. The replacement seal that is being placed on the container must be recorded on the shipping document along with the reason for removing the original seal. MPTO must implement the seal controls as outlined in the Container Security section of this document. The replacement seal must be a PAS ISO 17712 high security seal that must be documented as well.

Container/Cargo Release

Cooperation with CBP on ensuring that inbound containers be made readily available to CBP is a major commitment as a C-TPAT member. The MPTO must carry out its responsibility to set-aside those containers that have been designated by CBP for examination prior to being released into the commerce of the U.S. The containers that have been designated for examination by CBP must be delivered expeditiously to the exact location specified by CBP. Any containers that are released or misdelivered without CBP authorization by a MPTO could result in suspension or removal from the C-TPAT program.

- **Vessel Automated Manifest System**

U.S. MPTOs that are members of C-TPAT will be required to participate in the Automated Manifest System (AMS). Participation in AMS will provide the MPTOs an important communication capability regarding cargo/container holds and releases. At the exit gate, the U.S. MPTOs must query each container in AMS to ensure that the container has been approved for release by CBP.

Security Training and Awareness

A security awareness program should be established and maintained by the MPTO to recognize and foster awareness of security vulnerabilities to the port, vessels and maritime cargo. On an annual basis, employees must be made aware of the procedures the MPTO has in place to report a security concern or incident. Annual refresher training on security and threat awareness should be developed and administered to all employees. Additionally, specific training should be offered on an annual basis to assist employees in maintaining port security, vessel and cargo integrity, recognizing internal conspiracies, and protecting access controls.

Physical Security

MPTO shall establish written and verifiable procedures to prevent unauthorized personnel from gaining access to the ports, vessels, and to prevent tampering with cargo conveyances while they are in MPTO's custody. 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. MPTO should incorporate the following C-TPAT physical security criteria as applicable.

- **Fencing**

Perimeter fencing should enclose the entire port area, and 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 and Private Vehicles**

Access to terminal by private passenger vehicles should be limited as much as possible in order to lessen opportunities to introduce contraband into the terminal area or to remove items from the terminal.

If access is given to private passenger vehicles, they should be prohibited from parking in or adjacent to cargo handling and storage areas, and vessels. Trucks with cabs/condos should be locked at all time while left unattended in the port to prevent absconders or stowaways from hiding in the conveyance to gain access outside of the port.

- **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 the port, terminal facilities, vessels, cargo handling and storage areas.

Information Technology Security

Information Technology Security (IT) is also a cornerstone of supply chain security as the trade continues to transform increasingly to a paperless environment. Through the use of more automated systems, the opportunities to commit document fraud and internal conspiracies increases. IT security guidelines should be in place such as password protection and user accountability. If outside technicians or programmers are utilized to work on internal systems, these individuals should be monitored to ensure that sensitive data is not accessed.

- **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

MPTOs 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 a breach of security is identified, the MPTO 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 MPTO's senior management to discuss such concerns and to identify appropriate remedial measures to be taken.

Non-Compliance

While CBP has the authority to suspend or remove a MPTO 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.