

## Customs – Trade Partnership against Terrorism (C-TPAT)

**Scope:** Customs and the international trade community working in partnership to prevent the introduction of weapons of mass destruction into the international supply chain from point of origin to point of distribution. Importers must have written and verifiable procedures in place to meet the scope of this program.

Companies have various security initiatives to protect information, employees and physical assets. C-TPAT encompasses all of these security efforts. For global companies, it is logical to rename their security initiatives and put them under the umbrella of C-TPAT in order to relieve stress on import cargo delays. CBP (Customs Border & Protection) claims that the chance of a Customs exam is reduced 6 times for C-TPAT importers.

Post terrorist event – CBP is likely to temporarily close our borders to all trade in the event of a significant terrorist event such as the detonation of a weapon of mass destruction within the United States. The length of the border closure will vary depending on the circumstances of the terrorist attack. CBP has indicated that the first shipments that would be allowed to enter the United States would be those that are for a C-TPAT importer AND from a CSI port.

C-TPAT eligible parties are: Air, Sea and Rail carriers, Domestic Truckers, Terminals, Consolidators, Importers, Custom Brokers and invited foreign manufacturers.

### Nine steps to C-TPAT success:

- Business partner selection
- Container security
- Physical Access control
- Employee validation
- Documentation integrity
- Security training and awareness
- Cargo security while on premises
- Building integrity
- Information technology security

## **Business Partner Selection**

Wacker must have a written and verifiable process for the selection of business partners including manufacturers, product suppliers and vendors. When possible, CBP recommends the use of C-TPAT business partners. For those business partners not eligible for C-TPAT, Wacker must require its business partners to demonstrate that they are meeting C-TPAT (or WCO equivalent) security criteria.

## **Container Security**

Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S.

## **Physical Access Control**

Wacker must have sufficient access controls to prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. An employee identification system must be in place for positive identification and access control purposes. Visitors must present photo identification for documentation purposes upon arrival and should be escorted and visibly display temporary identification. Arriving packages and mail should be periodically screened. Procedures must be in place to identify and challenge unauthorized/unidentified persons.

## **Employee validation**

Employment application information must be verified prior to employment. Consistent with applicable laws, *background checks* should be conducted for prospective employees. Periodic checks should be performed based on cause, and/or the sensitivity of the employee's position. There must be procedures in place to remove identification, facility, and system access for terminated employees.

## **Documentation Integrity**

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. Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. 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 that Wacker has in place to address a situation and how to report it.

## **Cargo Security While on Premises**

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

## **Building Integrity**

Buildings must be constructed of materials that resist unlawful entry. All external and internal windows, gates and fences must be secured with controlled locking devices. Adequate lighting must be provided inside and outside the facility. Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

## **Information Technology Security**

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. 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.