



**The following is a list of the minimum security criteria for membership in the US Customs (CBP) Customs-Trade Partnership Against Terrorism (C-TPAT) Program.**

- Conduct comprehensive assessment of their international supply chains based upon C-TPAT security guidelines. This includes business partners throughout the supply chain. This starts at the point of origin.
- Aircraft integrity must be maintained to prevent introduction of personnel or material.
- Air carriers must have written and verifiable processes for the screening and selection of business partners. Air carriers must have written documentation indicating their business partners are C-TPAT certified. Air carrier business partners who are not C-TPAT certified must provide written documentation that they are meeting the security requirements of C-TPAT screening procedures to check contracted service provider validity, financial soundness, ability to meet contractual security requirements, and the ability to correct security deficiencies as needed.
- Cargo container security must be maintained to protect against the introduction of unauthorized material or person(s).
- Container inspection to verify physical integrity (top, bottom, inside, outside).
- Access controls for facilities to prevent unauthorized access.
- Employee and visitor identification system and controls.
- Proper vendor ID and/or photo ID must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated. Challenge procedures are in place.
- Personnel security includes screening of perspective employees and periodical checks of current employees. A permanent list (foreign and domestic) should be maintained that includes name, date of birth, national identification number or social security number and position held.
- Background checks would be conducted consistent with foreign, federal, state and local regulations. The Customs Border and

Protection could require this information to be submitted to them upon request.

- Procedures must be in place to ensure the integrity of all documentation used in clearing of cargo.
- Cargo received from business partners abroad must be properly manifested, documented, and maintained in a system that verifies the weight, quantity, etc.
- Participation in the Advanced Passenger Information System (APIS) and Automated Manifest System (AMS).
- A threat program to maintain security awareness of threats posed by terrorist at each point in the supply chain and a means to report it.
- Specific training should be offered to assist employees in maintaining cargo integrity. Employees must be able to recognize internal conspiracies. Unannounced security audits should be performed in accordance with defined guidelines.
- Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage. Gates for vehicle or personnel must be staffed or monitored.
- Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas. Buildings must be constructed of materials that resist unlawful entry. 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. Adequate lighting must be provided for inside and outside of facilities.
- Alarms systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas. IT integrity must be maintained to protect data from unauthorized access or manipulation. Automated systems must use individually assigned accounts that require a periodic change of passwords. Training of IT policies and procedures are required for employees. Discrepancies must be able to be identified.

10.3.2006