



SECURITY RECOMMENDATIONS FOR BUSINESS PARTNERS

US Customs & Border Protection is asking all of its C-TPAT Program members to promote adherence to the C-TPAT program by contracting service providers who provide transportation, cargo handling, and security services committed to C-TPAT Security Guidelines most closely associated with the particular enrollment sector.

CBP administrators for C-TPAT is also requesting to all partners to refrain from the practice of subcontracting (to non CTPAT participants) beyond a second party or “double brokering” and ensure that other providers within their supply chain also do the same.

Note: CBP believes double brokering weakens the supply chain as it lessens the accountability of those within the supply chain and puts the original stakeholder at a greater risk of supply chain incident.

C-TPAT Commercial Partners should develop and implement a sound plan to enhance security procedures. These are general recommendations that should be followed on a case-by-case basis depending on the company’s size and structure, and may not be acceptable or applicable to all companies.

The company should have a written security policy in place that addresses the following areas:

Physical Security

All buildings should be constructed of materials which resist unlawful entry and protect against outside intrusion. Physical security should include:

- Adequate locking devices for external and internal doors, windows, gates, and fences
- Adequate lighting provided inside and outside the facility to include parking areas
- Segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged, or otherwise fenced-in area
- Separate parking area for private vehicles from the shipping, loading dock, and cargo areas
- Internal/external communications systems in place to contact internal security personnel or local law enforcement police

Access Controls

Unauthorized access to facilities should be prohibited. Controls should include:

- Positive identification of all employees, visitors, and vendors
- Procedures for challenging unauthorized/unidentified persons

Access Control Employee Responsibilities

- Never allow someone to enter the facility behind you without using their own security access device (key, card, code, etc.) In case of visitors they must go through reception area
- Never share your keys, keycards or passwords. Personnel should challenge any person without a photo ID or who does not belong to the company

Procedural Security

Procedures should be in place to protect against un-manifested material being introduced into the warehouse and supply chain. Security controls should include:

- Designated security officer to supervise the introduction/removal of cargo
- Properly marked, weighed, counted, and documented cargo/cargo equipment verified against manifest documents
- Procedures for verifying seals on containers, trailers, and railcars
- Procedures for detecting and reporting shortages and overages
- Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company
- Proper storage of loaded and empty containers to prevent unauthorized access

Personnel Security

Companies should conduct employment screening and interviewing of prospective employees to include:

- Periodic background checks and application verifications

Education and Training Awareness

A security awareness program should be provided to employees including:

- Recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls

Service Provider Security

Internal controls for selection of service providers:

- Written standards for service providers' physical and procedural security
- Procedure to request if service providers participate in C-TPAT, CIP, or BASC



Information Security

All personnel who use a computer or handle documents should be instructed in company information management policies to include:

- Procedures to ensure that all information received and used in the process of handling or clearing merchandise is legible and protected against the exchange, loss or introduction of erroneous information
- Automated systems should be protected using passwords, encryption software, firewalls, and anti-virus software
- Strict access to all data files including limited remote access with secure identification
- Computer room should have strictly limited access to authorized computer support personnel

IT Employee Responsibilities

- Maintain computer and data security
- Participate in the annual security audit/assessment when requested.
- Safeguard keys, keycards, passwords and other security codes or cards.

Emergency Preparedness

Emergency plans must be in place and all employees must be familiar with the plans:

- Plans must include means for emergency responders to gain access to the area
- Emergency plans must be integrated within the company and employees must be trained in these plans
- The company's emergency plan must be coordinated with emergency responders from the community