

Importer Security Recommendations for C-TPAT



Importers

Develop and implement a sound plan to enhance security procedures throughout your supply chain. Where an importer does not control a facility, conveyance or process subject to these recommendations, the importer agrees to make every reasonable effort to secure compliance by the responsible party. The following 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 applicable to all.

Procedural Security: Procedures should be in place to protect against unmanifested material being introduced into the supply chain. Security controls should include the supervised introduction/removal of cargo, the proper marking, weighing, counting and documenting of cargo/cargo equipment verified against manifest documents, the detecting/reporting of shortages/overages, and procedures for verifying seals on containers, trailers, and railcars. The movement of incoming/outgoing goods should be monitored. Random, unannounced security assessments of areas in your company's control within the supply chain should be conducted. Procedures for notifying Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected, or suspected, by the company should also be in place.

Physical Security: All buildings and rail yards should be constructed of materials, which resist unlawful entry and protect against outside intrusion. Physical security should include perimeter fences, locking devices on external and internal doors, windows, gates and fences, adequate lighting inside and outside the facility, and the segregation and marking of international, domestic, high-value, and dangerous goods cargo within the warehouse by a safe, caged or otherwise fenced-in area.

Access Controls: Unauthorized access to facilities and conveyances should be prohibited. Controls should include positive identification all employees, visitors, and vendors. Procedures should also include challenging unauthorized/unidentified persons.

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 the recognition of internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should offer incentives for active employee participation in security controls.

Manifest Procedures: Companies should ensure that manifests are complete, legible, accurate, and submitted in a timely manner to Customs.

Conveyance Security: Conveyance integrity should be maintained to protect against the introduction of unauthorized personnel and material. Security should include the physical search of all readily accessible areas, the securing of internal/external compartments and panels, and procedures for reporting cases in which unauthorized personnel, unmanifested materials, or signs of tampering, are discovered.