C-TPAT Minimum Security Criteria for Business Partners

Physical Security and Access Controls

- Must implement measures that assure the security of buildings, as well as those that monitor and control exterior and interior perimeters
- Must implement access controls that prohibit unauthorized access to facilities, conveyances, loading docks and cargo areas.
- Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.
- Access controls prevent unauthorized entry into facilities, maintain control of employees, visitors and individuals, and protect company assets.
- Procedures must be in place to prevent, detect and deter un-manifested material and unauthorized personnel from gaining access to conveyances and facilities.
- Physical security criteria in this section should be implemented throughout the supply chain, as applicable.

Procedural Security

- Measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, customs clearance and storage of cargo in the supply chain.
- Business partners must develop security processes consistent with C-TPAT security criteria to enhance the integrity of the shipment at its point of origin up to its point of final destination.
- Periodic reviews of business partners' processes and facilities should be conducted based on risk. These processes and facilities should maintain the security standards required by the C-TPAT member.

Container, Trailer and Rail Car Security

- Security must be maintained on all containers, trailers and rail cars used to import or export goods to protect them against the introduction of unauthorized material and/or persons.
- At the point of stuffing/packing, procedures must be in place to properly seal and maintain the integrity of the shipping container, trailer or rail car.

Data and Document Security

- A well-defined physical security policy and system controlling access to any office or secure area must be in place to ensure that there is no unauthorized access to computers and equipment.
- Measures must be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access.

Personnel Security

- Personnel security programs must incorporate the screening of employees and prospective employees.
- These programs should include periodic background checks on employees working in security-sensitive positions and the noting of unusual changes in an employee's apparent social and economic situation.

Security Training and Awareness

- A security awareness program should be in place to inform and regularly remind individuals of security responsibilities, issues and concerns.
- The security awareness program provided to employees should include recognizing internal conspiracies and fostering awareness of the threats posed by criminal and terrorist elements in the supply chain.

Business Partner Requirements

- When a company contracts out elements of its international supply chain, it is vital that the company works with its business partners to ensure that sound security measures are in place and adhered to in order to achieve an effective secure supply chain globally.
- Business partners that are not eligible for C-TPAT must be subject to a verification of their compliance with C-TPAT security criteria by the company through a documented risk-assessment process.

Supply Chain Security Planning

- Policies and procedures should be in place for companies to undertake a risk assessment of their supply chain, identify gaps and weaknesses, and implement strategies to mitigate risks