A Message for Warehouse Operators
And
Security Guidelines for Warehouse Operators

Kingchem LLC is a participant in the Customs-Trade Partnership Against Terrorism (C-TPAT).

C-TPAT is a voluntary joint government-business initiative to build cooperative relationships that strengthen the overall supply chain, and border security. Every person who is involved in logistics, distribution, or supply chain management will be affected by ongoing efforts to create a more secure global trading system. Importers are now expected to be able to demonstrate that all aspects of this process are under control throughout the supply chain.

As a C-TPAT participant, Kingchem LLC must assess, improve, and communicate more comprehensive safety procedures for cargo security. U.S. Customs and Border Protection requires a complete self-assessment that encompasses:

- Procedural Security
- Physical Security
- Access Control
- Information Technology Security
- Security Awareness Training
- Personnel Security
- Conveyance Security
- Business Partners

As part of the process of evaluating our supply chain security, Kingchem LLC is required to obtain information concerning the security procedures used by our supply chain partners. As our business partner, it is necessary for your firm to develop, implement, and follow security processes and procedures consistent with the C-TPAT security criteria. We have attached a list of the C-TPAT guidelines for warehouse operators. Since your company is one of our partners in the supply chain, we request that you provide **one** (1) of the following documents to verify compliance with C-TPAT guidelines:

- A Copy of C-TPAT Certification
- Certification of participation in a foreign Customs security program
- Written/electronic documentation from a corporate officer attesting to compliance
- Complete the security questionnaire attached to this communication

Please provide this information to us as soon as you receive our communications to you requesting it. Partners must furnish an updated certification on a yearly basis.

If you should have any questions, please contact us by replying to the email by which you received this message, or at telephone number: +1-201-825-9988, or fax number: +1-825-9148.

For your convenience we have provided further information below (C-TPAT Security Guidelines for Warehouse Operators) regarding the C-TPAT program and security concerns

Regards,
Kingchem LLC

C-TPAT Security Guidelines for Warehouses

As of this writing, Customs and Border Protection had not issued specific guidelines for warehouse operators; however, reviewing the guidelines and criteria for other business partners, it is possible to determine some general requirements that would be applicable to warehouse operators. Some warehouse facilities may be certified as part of the carrier, NVOCC, or other consolidator C-TPAT program. Warehouse operators should continue to look for CBP to publish specific guidelines for warehouse facilities.

Remember, these guidelines are not a substitute for any information that CBP publishes.

Business Partner Requirements

- Warehouses must have written and verifiable processes for the screening selection of business partners including customers, contractors, carriers, and vendors.

- Warehouse operators should ensure that contract companies who provide transportation, security, and cargo handling related services commit to C-TPAT Security Guidelines.

- For those business partners eligible for C-TPAT certification (importers, ports, terminals, brokers, carriers, etc.) the warehouse operator must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are, or are not, C-TPAT certified. Non-C-TPAT business partners may be subject to additional scrutiny by warehouse.

- Periodic reviews should be performed on service providers to detect weakness, or potential weakness, in security.

Conveyance Security

Conveyance (tractor and trailer) integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material.

Container and Trailer Seals

The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain. Any warehouse responsible for loading containers for import to, or export from, the United States must ensure that all seals meet or exceed the current PAS ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers and trailers, to include procedures for recognizing and reporting compromised seals and/or containers/trailers to US Customs and Border Protection or the appropriate foreign authority. Only designated employees should distribute seals.

- **Container and Trailer Storage**
  Containers and trailers under warehouse control must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

Physical Access Controls

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

- **Employees**
  An employee identification system must be in place for positive identification and access, control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges. Procedures for the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

- **Visitor Controls**
  Upon arrival, visitors must present photo identification for documentation purposes. All visitors should be escorted and visibly display temporary identification.

- **Deliveries (including mail)**
  Upon arrival, vendor ID and/or photo identification must be presented for documentation purposes by all vendors.

- **Challenging and Removing Unauthorized Persons**
  Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to CBP upon written request, to the extent permitted by law.

- **Pre-Employment Verification**
  Application information, such as employment history and references, must be verified prior to employment.

- **Background checks / investigations**
  Consistent with foreign, federal, state and local regulations, background checks and investigations should be conducted for prospective employees. Periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**
  Companies must have procedures in place to remove identification, as well as facility and system access for terminated employees.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

- **Documentation Processing**
  Procedures must be in place to ensure that all documentation 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 compute access and information.

- **Manifesting Procedures**
  To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

- **Cargo Discrepancies**
  All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. CBP and/or other appropriate law

enforcement agencies must be notified if illegal or suspicious activities are detected.

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 the company has in place to address a situation and how to report it. Additional training should be provided to employees in sensitive areas.

- Additionally, specific training should be offered to assist employees in recognizing internal conspiracies and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

Warehouses should incorporate the following C-TPAT physical security guidelines throughout their facilities as applicable:

- **Fencing**
  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 and Gate Houses**
  Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

- **Parking**
  Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas.

- **Building Structure**
  Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

- **Locking Devices and Key Controls**
  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.

- **Lighting**
  Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, fence lines and parking areas.

- **Alarms Systems & Video Surveillance Cameras**
  Alarm systems and video surveillance cameras should be used to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Information Technology Security

Information Technology (IT) integrity must be maintained to protect data from unauthorized access or manipulation.

- **Password Protection**
  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 training provided to employees.

Accountability

A system must be in place to identify the abuse of IT, including improper access, tampering, or altering of business data. All system violators will be subject to appropriate disciplinary action.