Genesco

GENESCO Inc.’s C-TPAT Security Expectations for Vendors and Manufacturers

C-TPAT

Customs-Trade
Partnership Against Terrorism

Introduction

In direct response to 9/11, the U.S. Customs Service, now U.S. Customs and Border Protection (CBP) challenged the trade community to partner with CBP to design a new approach to supply chain security focused on protecting the United States against acts of terrorism by improving security while simultaneously speeding the flow of compliant cargo and conveyances. The result was the Customs-Trade Partnership Against Terrorism (C-TPAT) – an innovative, voluntary government/private sector partnership program.

C-TPAT builds on the best practices of CBP/industry partnerships to strengthen supply chain security, encourage cooperative relationships and to better concentrate CBP resources on areas of greatest risk. It is a dynamic, flexible program designed to keep pace with the evolving nature of the terrorist threat and the changes in the international trade industry, thus ensuring the program's continued viability, effectiveness and relevance. Flexibility and customization are important characteristics of C-TPAT.

Genesco Inc. became a certified C-TPAT member in 2003. Genesco Inc. is committed to keeping our supply chain secure to agreed security standards through self policing and implementing changes as needs arise. The current security guidelines for C-TPAT program members address a broad range of topics including personnel, physical and procedural security; access controls; education, training and awareness; manifest procedures; conveyance security; threat awareness; and documentation processing. Companies that apply to C-TPAT must sign an agreement with CBP that commits their organization to the program's security guidelines. These guidelines offer a customized solution for the members, while providing a clear minimum standard that approved companies must meet.

Genesco has taken steps internally to protect its supply chain against security breaches and acts of terrorism. Likewise, we are now contractually requiring our business partners to enhance their safety and security procedures according to the following C-TPAT security criteria. Following is a general summary of the C-TPAT security requirements, versions in both English and Chinese. Please direct any questions via email to: GlobalCompliance@genesco.com.

Minimum Security Criteria for C-TPAT; Foreign Manufacturers - English

These minimum security criteria are fundamentally designed to be the building blocks for foreign manufacturers to institute effective security practices designed to optimize supply chain performance to mitigate the risk of loss, theft, and contraband smuggling that could potentially introduce terrorists and implements of terrorism into the global supply chain. The determination and scope of criminal elements targeting world commerce through internal conspiracies requires companies, and in particular, foreign manufacturers to elevate their security practices.

At a minimum, on a yearly basis, or as circumstances dictate such as during periods of heightened alert, security breach or incident, foreign manufacturers must conduct a comprehensive assessment of their international supply chains based upon the following C-TPAT security criteria. Where a foreign manufacturer out-sources or contracts elements of their supply chain, such as another foreign facility, warehouse, or other elements, the foreign manufacturer must work with these business partners to ensure that pertinent security measures are in place and are adhered to throughout their supply chain. The supply chain for C-TPAT purposes is defined from point of origin (manufacturer/supplier/vendor) through to point of distribution – and recognizes the diverse business models C-TPAT members employ.

C-TPAT recognizes the complexity of international supply chains and security practices, and endorses the application and implementation of security measures based upon risk[1]. Therefore, the program allows for flexibility and the customization of security plans based on the member’s business model.

Appropriate security measures, as listed throughout this document, must be implemented and maintained throughout the Foreign manufacturer’s supply chains - based on risk[2].

Business Partner Requirements

Foreign manufacturers must have written and verifiable processes for the selection of business partners including, carriers, other manufacturers, product suppliers and vendors (parts and raw material suppliers, etc).

Security procedures
For those business partners eligible for C-TPAT certification (carriers, importers, ports, terminals, brokers, consolidators, etc.) the foreign manufacturer must have documentation (e.g., C-TPAT certificate, SVI number, etc.) indicating whether these business partners are or are not C-TPAT certified.

For those business partners not eligible for C-TPAT certification, the foreign manufacturer must require that their business partners to demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation (e.g., contractual obligations; via a letter from a senior business partner officer attesting to compliance; a written statement from the business partner demonstrating their compliance with C-TPAT security criteria or an equivalent World Customs Organization (WCO) accredited security program administered by a foreign customs authority; or, by providing a completed foreign manufacturer security questionnaire). Based upon a documented risk assessment process, non-C-TPAT eligible business partners must be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer.

Point of Origin

Foreign manufacturers must ensure that business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin, assembly or manufacturing. Periodic reviews of business partners' processes and facilities should be conducted based on risk, and should maintain the security standards required by the foreign manufacturer.

Participation/Certification in a Foreign Customs Administration Supply Chain Security Program

Current or prospective business partners who have obtained a certification in a supply chain security program being administered by foreign Customs Administration should be required to indicate their status of participation to the foreign manufacturer.

Security Procedures

On U.S. bound shipments, foreign manufacturers should monitor that C-TPAT carriers that subcontract transportation services to other carriers use other C-TPAT approved carriers, or non-C-TPAT carriers that are meeting the C-TPAT security criteria as outlined in the business partner requirements.

As the foreign manufacturer is responsible for loading trailers and containers, they should work with the carrier to provide reassurance that there are effective security procedures and controls implemented at the point-of-stuffing.

<u>Container and Trailer Security</u>

Container and trailer integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers and trailers. A high security seal must be affixed to all loaded containers and trailers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standard for high security seals.

In those geographic areas where risk assessments warrant checking containers or trailers for human concealment or smuggling, such procedures should be designed to address this risk at the manufacturing facility or point-of-stuffing.

Container Inspection

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:

- Front wall
- Left side
- Right side

- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

Trailer Inspection

Procedures must be in place to verify the physical integrity of the trailer structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. The following five-point inspection process is recommended for all trailers:

- Fifth wheel area - check natural compartment/skid plate
- Exterior - front/sides
- Rear - bumper/doors
- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
-
- Outside/Undercarriage

Container and Trailer Seals

The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain, and remains a critical part of a foreign manufacturers’ commitment to C-TPAT. The foreign manufacturer must affix a high security seal to all loaded trailers and containers bound for the U.S. All seals must 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 for integrity purposes.

Container and Trailer Storage

Containers and trailers under foreign manufacturer control or located in a facility of the foreign manufacturer 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.

Visitors

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and should visibly display temporary identification.

Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated.

Challenging and Removing Unauthorized Persons

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

<u>Personnel Security</u>

Processes must be in place to screen prospective employees and to periodically check current employees.

Pre-Employment Verification

Application information, such as employment history and references must be verified prior to employment.

Background Checks / Investigations

Consistent with foreign regulations, background checks and investigations should be conducted for prospective employees. Once employed, 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, facility, and system access for terminated employees.

<u>Procedural Security</u>

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 information 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 computer access and information.

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

Shipping and Receiving
Departing cargo being shipped should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Procedures should also be established to track the timely movement of incoming and outgoing goods.

Cargo Discrepancies
All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if anomalies, illegal or suspicious activities are detected - as appropriate.

Physical Security

Cargo handling and storage facilities in international locations must have physical barriers and deterrents that guard against unauthorized access. Foreign manufacturer should incorporate the following C-TPAT physical security criteria throughout their supply chains 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, cargo handling and storage areas, fence lines and parking areas.

Alarms Systems and Video Surveillance Cameras

Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

Information Technology Security

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 provided to employees in the form of training.

Accountability

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

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 and contraband smugglers 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 the shipping and receiving areas, as well as those receiving and opening mail.

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

[1] *Foreign manufacturers shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, C-TPAT membership, potential terrorist threat via open source information, having inadequate security, past security incidents, etc.).*

[2] *Foreign manufacturer shall have a documented and verifiable process for determining risk throughout their supply chains based on their business model (i.e., volume, country of origin, routing, potential terrorist threat via open source information, etc.)*

最终文本
海关-商业伙伴反恐计划（C-TPAT）
外国制造商安全标准

本最低安全标准是为使外国制造商实施高效安全实务以优化供应链的绩效，从而减少恐怖分子以及恐怖主义的实施行为通过丢失、盗窃和走私货物渗入全球供应链的危险而设计的基本结构单元。犯罪团伙通过内部阴谋破坏世界商贸活动的倾向和活动范围要求公司，尤其是外国制造商，提高它们的安全实务。

外国制造至少必须每年一次，或者根据情况的需要，比如在高度警戒、发生安全违反或安全事故的期间，根据下面所述的C-TPAT安全标准对它们的国际供应链进行全面评估。如果外国制造商将它们供应链的某些部分外包或承包给比如另一个外国机构、仓库或其他部门，则外国制造商必须与这些商业伙伴一起确保在整个供应链中相关的安全措施都得以实施和遵守。C-TPAT所定义的供应链是支从原发点（制造商/供应商/卖主）一直到销售点的整个过程，并且适用于C-TPAT成员所使用的各种不同的商业模式。

C-TPAT认识到国际供应链以及安全实务的复杂性，并且支持基于风险的存在而对安全措施的应用和实施[注1]。因此，本计划允许基于成员的商业模式而灵活实施客户化的安全计划。

本文所列举的适当的安全措施必须基于风险的性质在外国制造商的整个供应链中得以实施和维持[注2]。

商业伙伴要求

外国制造商对于商业伙伴的选择，包括承运人、其他制造商、产品供应商和卖主（零件和原材料供应商等）必须有书面的、可核准的程序。

- 安全程序

  对于那些符合C-TPAT认证条件的商业伙伴（承运人、进口商、港口、码头、经纪人、并装业者等），外国制造商必须有文件证据（比如C-TPAT证书、SVI编号等）表明这些商业伙伴是否经过C-TPAT认证。对那些不符合C-TPAT认证条件的商业伙伴，外国制造商应要求它们的商业伙伴出示它们达到C-TPAT安全标准的书面/电子确认书（比如合同义务；由商业伙伴的一位高级官员签字保证合规的信件；由商业伙伴出示一份书面声明表明其符合C-TPAT安全标准或一个外国海关主管部门管理为世界海关组织（WCO）所认可的同等安全计划的要求；或者，提供一份完整的外国制造商安全问卷）。基于一项被记录的风险评估程序，外国制造商必须对不符合C-TPAT条件的商业伙伴进行核准，以验证其是否达到C-TPAT的安全标准。

- 原发点

  外国制造商必须确保商业伙伴遵照C-TPAT安全标准制定安全程序和规程，以强化在原发点装运、组装或制造的完整性。基于风险的性质应对商业伙伴的程序和设施定期进行审核，并且保持外国制造商所要求的安全标准。

- 参与外国海关主管机关的供应链安全计划及获得认证的情况

  获得外国海关主管机关管理的供应链安全计划认证的当前或未来的商业伙伴应被要求向外国制造商表明其参与计划的状况。

- 安全程序

  对于运往美国的货物，外国制造商应监督将运输服务分包给其他承运人的C-TPAT承运人用的是其他为C-TPAT所批准的承运人，或者如果是非C-TPAT批准的承运人，则其达到商业伙伴要求里所描述的C-TPAT安全标准。

  因为外国制造商须对将货物装运上拖车或集装箱负责，因此它们应该与承运人一起工作以确保在装运时实施了有效的安全程序和控制措施。

1．外国制造商应基于它们的商业模式对它们整个供应链中存在的风险应该有记录在案的、可核准的确定程序（运输量、原产国、航线、C-TPAT成员资格、通过公开信息渠道获悉的潜在恐怖威胁、存在的安全隐患、过去的安全事故等）。

2．外国制造商应基于它们的商业模式对它们整个供应链中存在的风险应该有记录在案的、可核准的确定程序（运输量、原产国、航线、C-TPAT成员资格、通过公开信息渠道获悉的潜在恐怖威胁等）。

最终文本

集装箱及拖车的安全

集装箱及拖车的完整性应得到维护以确保不会混入未经许可的物品和/或人。在装运货物的时候，应该有恰当地贴封条和保持装运集装箱和拖车的完整性的程序。所有运往美国的装有货物的集装箱和拖车都必须贴上高度安全封条。所有封条都必须符合或超出现行PAS ISO 17712对高度安全封条的标准。

在风险评估有理由要求检查集装箱或拖车是否藏匿有人员或走私货物的地理区域，在制造场所或装运地应该有检查是否存在该等风险的程序。

- 集装箱检查

  在装运前应该有查验集装箱结构物理完整性的程序，包括门的锁闭系统的可靠性。本计划建议对所有集装箱进行如下七点检查程序：

  - 前壁
  - 左侧
  - 右侧
  - 地板
  - 顶部
  - 内/外门
  - 外部/起落架

- 拖车检查

  在装运前应该有查验拖车结构物理完整性的程序，包括门的锁闭系统的可靠性。本计划建议对所有集装箱进行如下七点检查程序：

  - 第五轮区域——检查自然隔间/车底护板
  - 外部——前面/侧面
  - 尾部——保险杠/门
  - 前壁
  - 左侧
  - 右侧
  - 地板
  - 顶部
  - 内/外门
  - 外部/起落架

- 集装箱及拖车的封条

  集装箱和拖车的封条，包括封条持续的完整性，是一条安全的供应链的重要组成部分，并且是外国制造商忠实执行C-TPAT计划的关键部分。外国制造商必须给所有运往美国的装有货物的集装箱和拖车贴上高度安全封条。所有封条都必须符合或超出现行PAS ISO 17712对高度安全封条的标准。

  应该制定有书面的程序规定对封条的管理以及如何贴到装有货物的集装箱和拖车上，包括识别和向美国海关和边境保护局或适当的外国主管部门报告受损的封条和/或集装箱/拖车的程序。只有被指定的雇员才能分发表示完整性的封条。

- 集装箱和拖车的存放

  受外国制造商控制或位于外国制造商场所的集装箱和拖车必须被存放在安全的区域以免有未经许可的人员进入和/或篡改。应该有报告和解决未经许可擅自进入集装箱/拖车或集装箱/拖车的存放区域的程序。

物理进入控制

进入控制用来防止未经许可进入设施的现象，维持对雇员和来访者的控制以及保护公司的财产。进

入控制必须包括在所有的进入点对所有雇员、来访者和卖主的积极识别。

- 雇员

  应该安装雇员识别系统以便进行积极的识别和进入控制。只有确有工作需要的人才能被允许金融安全区域。公司管理人员或安全人员必须对雇员、来访者和卖主的识别标志的发放和回收进行恰当的控制。发放和回收识别标志以及更换进入手段（比如钥匙、钥匙卡等）的程序必须被记录在案。

- 来访者

  来访者在抵达时必须出示带有照片的身份证明以作记录。所有来访者都必须有人陪同，并且必须可视地展示临时性的识别标志。

- 交货（包括邮件）

  所有卖主在抵达时必须出示适当的卖主身份和/或带有照片的身份证明以作记录。所有运达的包裹和邮件在散发出去前必须定期进行检查。

- 质询及将未经许可进入的人员带离现场

  应该有识别、质询和确认未经许可进入/身份不明的人员的程序。

个人安全

应该有审查预期雇佣的雇员和定期审查现有雇员的程序。

- 雇佣前审核

  在雇佣员工前应审核申请表信息，比如雇员的工作经历和推荐信。

- 背景检查/调查

  对于预期雇佣的雇员应按照外国法规的规定检查和调查其背景情况。在雇佣员工后，应根据事情的原由和/或雇员职位的敏感性对其进行定期检查和调查。

- 个人离职程序

  公司对于离职的雇员必须有去除身份证明标志、设备和进入系统设施的程序。

程序安全

应该制定有确保供应链中货物在运输、搬运和存放过程中的完整性和安全性的安全措施。

- 文档程序

  应该制定有程序确保用于商品/货物清理的所有信息易读、完整、准确以及不会被更改、丢失或引入错误的信息。文档控制必须包括保护计算机不被擅自闯入以及保护计算机信息的程序。

- 报告程序

  为确保货物的完整性，必须有确保从商业伙伴处接收到的信息被准确和及时报告的程序。

- 装运和接收货物

  被装运后将要离岸的货物应该与货物单的信息相符。货物应该被准确地描述，重量、标签、标记和件数应被列明和核准。离岸的货物应该与购货订单或装运订单上的内容进行校对。在货物被接收或发放前应对装运或接收货物的驾驶员进行积极的身份认定。同时还应该建立跟踪进出货物及时动向的程序。

- 货物差异

  所有货物的短缺、超额和其他重大的差异或异常情况都必须得到合理的解决和/或调查。如果发现有异常情况、非法或可疑活动，必须报告海关和/或其他适当的执法机关。

物理安全

位于国际场所的货物搬运和存放设施必须安置有物理障碍物和制止物以阻止人员未经许可进入里面。在适用的范围内，外国制造商应在它们的供应链中始终遵循以下的C-TPAT物理安全标准。

- 围栏

  货物搬运和存放设施的区域四周必须用围栏包围起来。货物搬运装置应该有内部围栏以将国内、国际、高价值和危险品货物隔离开。所有的围栏都必须经常检查其完整性及是否有损坏现象。

- 大门和门房

  车辆和/或人员进出的大门应该有人把守和/或被监视。大门的数量应该在保证适当进出和安全的基础尽可能保持最少。

- 停车场

私人载客车辆应被禁止进入停车场或临近货物搬运和存放区域。

- 建筑物
  建筑物的建筑材料应能阻止非法进入。通过定期检查和维修保持建筑物的完整性。
- 锁闭装置和钥匙控制
  所有外部和内部的窗子、大门和围栏都必须有锁闭装置以确保安全。管理人员或安全人员必须控制所有锁和钥匙的发放。

最终文本

- 照明
  在设施的内部和外部应该有适当的照明设施，包括在以下一些区域：进口和出口、货物搬运和存放区域、围栏线和停车场。
- 警报系统和监视摄像头
  应该安装警报系统和监视摄像头以监视货物搬运和存放场所以及防止未经许可的人员进入货物搬运和存放区域。

信息技术安全

- 口令保护
  自动化系统必须使用需要定期更换口令的个人担保账户。必须制定并实施信息技术安全政策、程序和标准，同时应对雇员进行培训。
- 解释责任
  必须有识别滥用信息技术，包括不当进入、干扰或篡改商业数据的体系。所有扰乱系统的人都必须因其滥用信息技术的行为而受到适当的纪律处分。

安全培训及忧患意识

安全人员应该制定并保持一项忧患意识计划以便识别以及培养对供应链的各个点上恐怖分子和走私者所带来的威胁的意识。雇员必须了解公司应对某种状况以及如何进行报告的程序。对在装运和接收货物领域工作以及接收和打开信件的雇员应该进行额外的培训。

此外，应该提供特定的培训以帮助雇员保持货物的完整性、识别内部阴谋以及保护进出控制。这些计划应该给积极参与的雇员提供奖励。