

最终文本 ( 2006 年 8 月 29 日 )  
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出发点(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<sup>1</sup>。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护<sup>2</sup>。

#### 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。

- 出发点

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,以强化在出发点装运、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)。

### 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。在装运货物时，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。

- 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。