最低安全标准—外国制造商

2020 年 1 月

注：标准的编号可能不连续。未列出编号的标准不适用于外国制造商。

第一个关注领域：企业安全

1. **安全愿景和责任** – 海关—商贸反恐伙伴计划（CTPAT）成员所实施的供应链安全计划如要保持有效，必须得到公司高级管理人员的支持。将安全性注入公司文化中，确保成为整个公司的优先事项，这主要是公司领导层的责任。

编号	标准	实施指南	必须 / 应该
1.1	在促进安全文化方面，CTPAT 成员应通过一份支持声明，表明其对供应链安全和 CTPAT 计划的承诺。该声明应由公司高级官员签名之后，张贴于公司适当的位置。	支持声明应强调保护供应链免诸如毒品贩运，恐怖主义，人口走私和非法违禁品等犯罪活动破坏的重要性。应该支持并签署声明的公司高级官员可包括总裁，首席执行官，总经理或安全总监。张贴地点包括公司网站、公司关键区域的海报上（接待前台、包装、仓库等）和/或作为公司安全性研讨会的一部分。	应该
1.2	为了构建完善的供应链安全计划，公司应将所有相关部门代表纳入跨部门团队。 这些新的安全措施应纳入到公司现有的程序中，创造一个更加可持续的结构，并强调确保供应链安全人人有责。	供应链安全所涵盖的范围比传统安全计划要广得多，与许多部门的安全紧密关联，如人力资源、信息技术和进/出口办公室。从长远来看，建立在安全部门上的传统供应链安全计划可能不太可行，因为执行安全措施的责任集中在少数员工中，容易受到关键人员流失的影响。	应该
1.3	供应链安全计划必须通过适当的明文审查规定来设计、支持和实施。审核的目的是为了要记录系统执行时，有关人	对 CTPAT 进行审查的目的是为了确保员工遵守公司的安全程序。审查过程不必复杂。成员根据其在供应链中的角色，商业模	必须

编号	标准	实施指南	必须 / 应该
	员对职责负责，并且按照安全计划的设计执行所有安全程序。审查计划必须根据公司运营和风险等级的相关变化进行更新。	式，风险等级以及特定地点/场所之差异来决定审查的范围及深入程度。 较小的公司可制定非常简单的审查方法，而大型跨国企业集团可能需要更大规模的流程，并可能需要考虑各种因素，例如当地法律规定等。一些大型公司可能已有稽核人员，可协助进行安全审查。 成员可以选择针对某些特定程序进行小规模审查。对于供应链安全至关重要的特殊领域，例如检查和封条控制，可进行针对这些领域的审查。但是，定期进行全面总检查有助于确保安全计划的各方面都按照设计发挥作用。如果成员已在年度审查中纳入该类检查，便足以满足该标准。 对于具有高风险供应链（由其风险评估决定）的成员，其审查流程可包括模拟或桌面演练，以确保员工了解实际发生安全事件时如何应对。	
1.4	公司内部的 CTPAT 联系人必须对 CTPAT 计划的规定充分了解。这些人员需要就与计划相关的问题定期向上级管理层提供最新情况，包括任何审核的进度或结果、与安全相关的演练以及 CTPAT 认证。	CTPAT 希望所指定的联系人能够积极主动与其供应链安全专家进行互动，及时回应。成员可以加派其他可以帮助支持该职能的人员，并在 CTPAT 门户中将其列为联系人。	必须

2. <u>风险评估</u> – 恐怖组织和犯罪集团针对供应链的持续威胁，突显出成员必须评估这些不断演变的威胁其现有和潜在的风险。CTPAT 认识到，当公司的供应链涉及多个业务伙伴时，这些供应链的安全保障将更为复杂。当公司拥有多个供应链时，应将重点放在具有较高风险的地理区域/供应链上。

在决定供应链的风险为何时，成员必须考虑各种因素，例如商业模式、供应商的地理位置以及特定供应链可能具备的特殊情况。

关键词定义：风险 – 衡量不测事件所造成的潜在危害，包括其威胁、脆弱性和后果。风险等级取决于威胁发生的可能性。发生的可能性高，通常等于高风险。风险可能无法排除，但可通过管控来降低 – 即减少漏洞或降低对业务的整体影响。

编号	标准	实施指南	必须 / 应该
2.1	CTPAT 成员必须对其供应链中的风险等级进行评估和记录。 CTPAT 成员必须进行总体风险评估（risk assessment, RA），以识别可能存在安全漏洞的环节。RA 必须识别威胁、评估风险并采用可持续措施来减少漏洞。成员必须考虑 CTPAT 对其在供应链角色中的具体要求。	总体风险评估（RA）由两个关键部分组成。第一部分是成员自我评估其设施内的安全实践、程序和政策，以确认符合 CTPAT 最低安全标准，并对管理层如何管理风险进行全面评估。 RA 的第二部分是国际风险评估。 这部分包括根据成员的商业模式和在供应链中的角色来确定地理威胁。在审视每种威胁对成员供应链安全的可能影响时，成员需要一种方法来评估或区分风险等级。一种简单的方法是将风险分为低级、中级和高级。 CTPAT 制定了五步风险评估指南（Five Step Risk Assessment），以帮助成员进行总体风险评估中的国际风险评估部分，该指南可在美国海关和边境保护局（U.S. Customs and Border Protection, CBP）网站查找 https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. 对于拥有广泛供应链的成员，主要关注点应放在风险较高的领域。	必须
2.2	风险评估的国际部分应记录或详细标示成员货物在供应链中从原发点到进口商配送中心的运送流程。流程图应包括所有直接或间接参与货物出口/运输的业务伙伴。	制定供应链流程图时，首先要考虑高风险区域。 在记录所有货物的移动情况时，成员应考虑所有适用的参与方，包括仅处理进出口文件的， 如报关行，以及可能不直接处理货物但可能具有操作控制权的，如无船承运人（Non Vessel Operated Common Carriers, NVOCCs）或第三方物流供应商（Third Party Logistics	应该

编号	标准	实施指南	必须 / 应该
	在适用的情况下，流程图应包括记录货物如何进出运输设施/货物枢纽，并注明货物是否會在某定点“静待”多时。货物在“静待”状态等待下一个行程时，更容易出问题。	Providers, 3PLs）。如果任何运输环节是分包出去的，也应列入考虑，因为间接方的层次越多，涉及的风险就越大。 制定流程图涉及更深入地了解供应链的运作。除了可识别风险外，还可用来查找供应链低效环节，有利于降低成本或缩短产品运抵时间。	
2.3	风险评估必须每年审查一次，或者根据风险因素进行更频繁的审核。	可能需要每年进行不只一次以上的风险评估情况包括：来自特定国家/地区的威胁级别提高、警报升级的时段增加、安全漏洞或事件发生之后、业务伙伴改变和/或变更公司结构/所有权，例如并购等。	必须
2.4	CTPAT 成员应制定书面程序，以处理危机管理、业务连续性、安全恢复计划和业务恢复。	危机可能包括由于网络攻击、火灾或武装人员劫持承运人司机而导致贸易数据移动中断。根据风险以及成员在何处运营或寻得货源，应急计划可以包括其他安全通知或支持；以及如何寻回被损毁或被盗的物品并恢复正常运营。	应该

3. **业务伙伴** – CTPAT 成员往来的业务伙伴，国内外皆有。至关重要的是，成员必须确保直接处理货物和/或进出口文件的业务伙伴采取适当的安全措施，来保护货物在整个国际供应链中的安全。当业务伙伴将某些工作分包出去时，整个流程会变得更复杂，在进行供应链风险分析时必须列入考虑。

关键词定义：业务伙伴 – 业务伙伴乃为个人或公司,其行为可能影响货物安全监管链，该类货物通过 CTPAT 成员供应链向美国进口或从美国出口。业务伙伴可以是提供服务以满足公司国际供应链内需求的任何一方。这些角色包括为 CTPAT 进口商或出口商成员或代表其进行货物采购、单据准备、简化、处理、储存和/或运输的所有（直接和间接）参与方。间接业务伙伴的两个例子是分包承运人和由代理商/物流提供商所安排的海外合并仓库。

编号	标准	实施指南	必须 / 应该
3.1	CTPAT 成员必须备有基于风险的书面流程，以筛选新的业务伙伴和监督当前的合作伙伴。此过程应包括检查有关洗钱和资助恐怖分子的活动。为了协助完成此过程，请查阅 CTPAT 的基于贸易的洗钱和恐怖主义融资活动的警告指标（Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities）。	审查公司是否合法的范例如下： •验证公司的营业地址和在该地址的经营时间； •在互联网上对公司和其负责人进行研究； •核查业务证明人；以及 •索取信用报告。 直接业务伙伴是需要经过筛选的，例如制造商、产品供应商、相关厂商/服务提供商和运输/物流提供商。任何与公司的供应链直接相关和/或处理敏感信息/设备的厂商/服务提供商也必须经过筛选；这包括经纪人或信息技术 IT 合同提供商。进行筛选的深入程度取决于供应链的风险等级。	必须
3.4	业务伙伴筛选过程必须考虑合作伙伴是否是 CTPAT 成员或与美国签有相互认可協議（Mutual Recognition Agreement, MRA）（或已批准 MRA）的授权经济运营商（Authorized Economic Operator, AEO）计划的成员。CTPAT 或已批准 AEO 认证是符合业务伙伴计划要求可接受的证明，成员必须以证书为凭，并继续监督业务伙伴以确保其认证持续有效。	业务伙伴的 CTPAT 认证可以通过其门户的状态验证界面系统（Status Verification Interface）来确认。 如果业务伙伴认证来自与美国签订 MRA 的外国 AEO 计划，则外国 AEO 认证将包括安全部分。成员可以访问外国海关的网站，其 AEO 将列名于此，或者也可直接向其业务伙伴索取认证。 目前美国 MRA 包括：新西兰、加拿大、约旦、日本、韩国、欧盟（28 个成员国）、台湾、以色列、墨西哥、新加坡、多米尼加共和国和秘鲁。	必须

编号	标准	实施指南	必须 / 应该
3.5	当 CTPAT 成员将供应链环节外包或分包时，该成员必须进行尽职调查（通过访查、问卷调查等），以确保其业务伙伴已采取符合或超过 CTPAT 最低安全标准（Minimum Security Criteria, MSC）的安全措施。	进出口商倾向于将很大一部分供应链活动外包。进口商（和某些出口商）通常属于具影响力的交易当事方，如有必要，可要求其业务伙伴，在整个供应链中实施安全措施。对于不是 CTPAT 或 MRA 接受成员的业务伙伴，CTPAT 成员将进行尽职调查，以确保（在具备影响力的情况下）这些业务伙伴符合适用的安全标准。 进口商对业务伙伴进行安全评估来决定其对安全要求的遵守情况。必须收集多少业务伙伴安全计划的信息取决于成员的风险评估。如果供应链众多，则优先考虑高风险区域。 确定业务伙伴是否符合最低安全标准，可以采用几种方法来完成。根据风险，公司可以进行设施现场稽核、雇用承包商/服务提供商进行现场稽核或使用安全调查问卷。如果使用安全调查问卷，所需细节或证据的多寡取决于风险等级。高风险地区的公司可能需要提供更详细信息。如果成员向业务伙伴进行安全调查问卷，考虑要求下列各项： •填写者的姓名和头衔； •完成日期； •文件填写人的签名； •*公司高级官员、安全主管或授权公司代表的签名，以证明问卷的准确性； •提供足够的细节以便决定是否合规；和 •根据风险，且在当地安全规程允许的情况下，包括提供照相证据、政策/程序副本以及填写完整的表格，如国际运输工具（Instruments of International Traffic）检查清单和/或警卫日志的副本。 *可以使用电子签名。如果无法签名或对其进行验证，受访者可以通过电子邮件证明问卷的有效性，并且证明答复和任何支持证据均经主管/经理核准（要求提供姓名和职务）。	必须

编号	标准	实施指南	必须 / 应该
3.6	如果在业务伙伴的安全评估过程中发现了弱点，则必须尽快处理，并且必须及时进行更正。成员必须通过书面证据确认缺失已得到解决。	CTPAT 认识到不同的修正所需的时间表也会有所不同。安装实体设备通常比修改程序费时，但是一旦发现安全漏洞，便必须立即处理。例如，如果问题是更换损坏的围栏，则必须立即开始采购程序（处理缺失），并且一旦可行时，尽快安装新围栏（纠正措施）。 根据所涉及的风险等级和弱点的重要性，某些问题可能需要立即处理。例如，如果该缺失可能危及集装箱的安全，便必须尽快解决。 文件证据的范例可包括所增派的保安人员合同副本、显示新安装的安全录摄像机或入侵报警器的照片或检查清单的副本等。	必须
3.7	为确保其业务伙伴继续遵守 CTPAT 的安全标准，成员应定期或根据情况/风险更新其对业务伙伴的安全评估。	定期检查业务伙伴的安全评估非常重要，才能确保安全计划的持续和妥善运行。如果成员对业务伙伴安全计划评估从未进行更新，当曾经可行的计划不再有效时，便无法得知，该成员的供应链将因而面临风险。 合作伙伴的安全评估核查频率取决于成员的风险评估流程。较高风险供应链的核查将比低风险的供应链更加频繁。如果业务伙伴的安全状况是以实地访查的方式来评估，则也可考虑加以利用进行其他必要访查的机会。例如交叉培训人员，使负责质量控制的人员也可以进行安全核查。 在某些情况下，可能必须更加频繁地更新自我评估，包括货源国威胁水平提高、货源地點發生变化、新的关键业务伙伴（实际处理货物或为设施提供安全服务等的业务伙伴）。	应该

编号	标准	实施指南	必须 / 应该
3.8	货物输往美国时，如果成员将运输服务分包给另一家公路承运人，则必须使用 CTPAT 认证的公路承运人或通过书面合同，列明其为向成员直接提供服务的公路承运人。合同必须规定遵守所有最低安全标准的要求。	承运人应向其提货和交货的设施提供分包承运人和司机的清单。分包商清单有任何更改，均应立即告知相关合作伙伴。 在审查服务提供商的合规情况时，成员应核实分包的公司是实际运输货物的公司，并且未经批准不得再分包。 成员应仅将运输服务分包一次。如果允许再分包的特例，当货物再次分包时，必须通知 CTPAT 成员和托运人。	必须
3.9	CTPAT 成员应备有社会合规计划，明文规定至少确保公司进口到美国的商品均非通过被禁止的劳工形式， 无论全部或部分，来开采、生产或制造的，即强迫劳动、监狱劳工、契约劳工或契约童工。	私营部门为保护劳工权利而在其运营和供应链中所做的努力可以增进人们对劳工法律和标准的了解，并减少不良的劳工实践。这些努力还为改善劳资关系创造环境，并增加公司的收益。 1930 年关税法第 307 条（Section 307 of the Tariff Act）(美国法典 19 U.S.C. § 1307）禁止从外国进口任何全部或部分由强迫劳动或契约童工（包括强迫童工）开采、生产或制造的商品。 国际劳工组织第 29 号公约（Labor Organization’s Convention No. 29）将强迫劳动定义为在惩罚的胁迫下，迫使任何人提供的所有工作或服务，且该人并非出于自愿。 社会合规计划是公司一系列的政策和实践，旨在确保最大程度地遵守其涉及社会和劳工议题的行为准则。社会合规指的是企业如何承担责任保护环境、以及员工的健康、安全和权利、其经营所在的社区以及供应链中工人的生活和社区。	应该

4. **网络安全** – 在当今的数字世界中，网络安全为其关键以保护公司最宝贵资产 - 知识产权、客户信息、财务和贸易数据、员工记录以及其他种种。随着互联网的连接越来越广泛，公司信息系统受到破坏的风险也随之增加。该威胁涉及所有类型和规模的企业。确保公司信息技术（IT）和数据安全的措施至关重要，所列标准为成员的整体网络安全计划提供了基础。

关键词定义：网络安全 – 网络安全是一种活动或过程，旨在保护计算机、网络、程序和数据免受意外或未经授权的取得、更改或破坏。它是一个过程，识别、分析、评估和传达与网络相关的风险，考虑成本和利弊，从而接受、避免、转移或将风险降低到可接受水平。

信息技术（IT） – IT包括计算机、存储、网络和其他实体设备、基础设施和程序，以便建立、处理、储存、保护和交换所有形式的电子数据。

编号	标准	实施指南	必须 / 应该
4.1	CTPAT 成员必须备有全面的书面网络安全政策和/或程序，以保护 IT 系统。书面的 IT 政策至少必须涵盖所有个别的网络安全标准。	鼓励成员遵循基于公认的行业框架/标准的网络安全协议。 *美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）是提供网络安全框架（Cybersecurity Framework）（https://www.nist.gov/cyberframework）的组织之一，根据现有标准、指南和实践提供自愿性指导，以帮助管理和减少内外部的网络安全风险。其可用于帮助确定可降低网络安全风险的优先选项，也是协调政策、业务和技术方法以管理该风险的工具。本框架是对组织的风险管理流程和网络安全计划的补充。目前尚未有网络安全计划的组织亦可参考该框架来进行制定。 * NIST 是美国商务部下属的非监管联邦机构，负责促进和维护测量标准，也是联邦政府技术标准的开发者。	必须

编号	标准	实施指南	必须 / 应该
4.2	为了保护 IT 系统免受常见的网络安全威胁，公司必须在成员的计算机系统中安装足够的软件/硬件来，以防止恶意软件（病毒、间谍软件、蠕虫、特洛伊木马等）和内部/外部入侵（防火墙）。成员必须确保其安全软件是最新的，并定期进行安全更新。成员必须制定政策和程序以防止通过社交工程进行的攻击。如果发生数据泄露或匿名攻击事件导致数据和/或设备损失，该程序必须包括恢复（或取代）IT 系统和/或数据的规定。		必须
4.3	使用网络系统的 CTPAT 成员必须定期测试其 IT 基础設施的安全性。如果发现漏洞，则必须尽快采取纠正措施。	安全的计算机网络对企业至关重要，要确保受到保护，就需要定期进行测试。这可以通过定时漏洞扫描来完成，就像保安人员检查企业的门窗是否打开一样。漏洞扫描（vulnerability scan, VS）可以识别计算机上的漏洞（开放的端口和 IP 地址）、其操作系统以及安装在计算机上，黑客可用来进入公司 IT 系统的软件。VS 将其扫描结果与已知的漏洞数据库进行比对，并提出修正报告供企业采取行动。坊间有许多免费和商业版本的 VS 软件。 测试的频率取决于各种因素，包括公司的商业模式和风险等级。例如，只要公司的网络基础架构有所改变，便应该运行这些测试。但是，因为任何规模的企业所面临的网络攻击都在增加，因此设计测试计划时须将之列入考虑。	必须
4.4	网络安全政策应解决成员如何与政府和其他业务伙伴共享有关网络安全威胁信息的问题。	鼓励成员与政府和供应链中的业务伙伴共享有关网络安全威胁的信息。信息共享是美国国土安全部使命的关键部分，目的是建立对恶意网络活动的态势感知。 CTPAT 成员可加入国家网络安全与通信一体化中心（National Cybersecurity and Communications Integration Center, NCCIC）（https://www.us-cert.gov/nccic）。 NCCIC 与公私营部门合作伙伴共享信息，以建立对漏洞、事件和缓解措施的意识。网络和工业控制系统用户可免费订阅信息产品、提要和服务。	应该

编号	标准	实施指南	必须 / 应该
4.5	必须建立一个系统来识别未经授权的 IT 系统/数据访问或滥用政策和程序的情况，包括对内部系统或外部网站的不当访问以及员工或合同员工对业务数据的窜改或变更。所有违规者都必须受到适当的纪律处分。		必须
4.6	网络安全政策和程序必须根据风险或情况，每年进行一次或更频繁的审查。审查之后，如有必要，必须更新政策和程序。	遭到网络攻击就是政策不到一年就需更新的例子。利用从攻击中得到的经验教训，将有助于加强成员的网络安全政策。	必须
4.7	必须根据职务描述或所分配的职责来限制用户访问权限。必须定期审查访问权限，以确保对敏感系统的访问是根据工作要求进行的。员工离职后，必须取消计算机和网络访问权限。		必须
4.8	有权访问 IT 系统的个人必须使用单独分配的帐户。 必须通过使用加强密码、密码短语或其他形式的身份认证来保护对 IT 系统的访问，使其免受渗透。必须保障 IT 系统用户访问的安全。 如果有证据显示密码和/或密码短语被窃或合理怀疑遭窃取，变必须尽快更改。	为了防止 IT 系统被渗透，必须通过认证过程来保护用户访问。复杂的登录密码或密码短语、生物识别技术和电子身份证是三种不同类型的身份认证过程。最好使用一种以上的程序。这些程序被称为双因素身份认证（two-factor authentication, 2FA）或多因素身份认证（multi-factor authentication, MFA）。MFA 是最安全的，因为它要求用户在登录过程中提供两个或更多证据（身份认证）以验证其身份。 MFA 可以用来防止利用密码过弱或身份认证被窃而发生的网络入侵。MFA 可以要求个人使用其所拥有的，如随机密码生成器，或其物理特征，即生物辨识特征，来增强密码或密码短语（你所知道的），从而阻止这些攻击向量。 如果使用密码，则密码必须很复杂。NIST 特别出版物 800-63B：数字身份指南（Digital Identity Guidelines），包括密码指导（https://pages.nist.gov/800-63-3/sp800-63b.html），建议使用长而且容易记住的密码短语，而不要使用带有特殊字符的单词。这些较长的密码短语（NIST 建议最多允许使用 64 个字符）由易于记住的句子或短语所组成，因此较难破解。	必须

编号	标准	实施指南	必须 / 应该
4.9	允许用户远程连接到网络的成员必须使用安全技术，例如虚拟专用网（virtual private networks, VPN），让员工得以在办公室以外的地点可以安全访问公司的内部网络。成员还必须备有程序防止未经授权用户进行远程访问。	VPN 不是保护远程访问网络的唯一选择。MFA 是另一种方法。要求员工键入其随机密码生成器的安全代码之后才能访问网络，就是 MFA 的一个例子。	必须
4.10	如果成员允许员工使用个人设备从事公司工作，则所有此类设备都必须遵守公司的网络安全政策和程序，包括定期的安全更新和安全访问公司网络的方法。	个人设备包括 CD、DVD 和 U 盘之类的存储介质。如果允许员工将其个人设备连接到其所使用的系统，则必须格外小心，因为这些数据存储设备可能受到恶意软件的感染，进而通过公司网络传播。	必须
4.11	网络安全政策和程序应包括防止使用盗版或无正当许可的技术产品的措施。	计算机软件是创建它的实体所拥有的知识产权（IP）。无论以何种方式取得软件，未经制造商或出版商的明确许可而安装软件均属违法。出版商总是通过授权给予许可，并明确软件授权份数。未授权许可的软件可能会因无法更新而无法发挥作用，且还更容易带有恶意软件，造成计算机及所存信息变得无用。未经授权许可的软件也不会获得任何保证或支援，如果遇到问题，公司只能自己想办法。使用未经授权许可的软件也引发法律后果，包括严厉的民事惩罚和刑事诉讼。软件盗版导致合法授权软件用户的成本增加，并减少可用于研发新软件的投资资本。 成员最好制定一项政策，要求所购买的新介质必须保留产品密钥标签和真实性证书。 CD、DVD 和 U 盘附有全息防伪标志，以确保其为正品，防止伪造。	应该
4.12	数据应每周或酌情备份一次。所有敏感和机密数据均应以加密格式存储。	丢失数据对组织内部人员所产生的影响会有所不同，因此应该进行数据备份。建议每日进行备份以防生产或共享服务器数据泄露/丢失。个别系统可能不需要那么频繁的备份，这取决于所涉及的信息类型。 用于存储备份的介质最好存放在异地设施中。备份数据的设备与生产工作的设备不应使用同一网络。将数据备份到云端可视为存放于“异地”设施。	应该

编号	标准	实施指南	必须 / 应该
4.13	进行定期库存清点时，必须包括所有存有进出口敏感信息的介质、硬件或其他 IT 设备。报废时，必须按照 NIST 介质清除指南（Guidelines for Media Sanitization）或其他适当的行业指南对其进行适当的清除和/或销毁。	某些类型的计算机介质是硬盘驱动器、可移动驱动器、CD-ROM 或 CD-R 光盘、DVD 或 U 盘驱动器。 NIST 已制定政府数据媒体销毁标准。成员可查阅 NIST 标准来清除和销毁 IT 设备和介质。 有关介质清除（Media Sanitization），可查阅： https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	必须

第二个关注领域：运输安全

5. <u>交通运输工具和国际运输工具的安全</u> – 走私经常涉及对交通运输工具和国际运输工具（IIT）的改装，或将违禁品隐藏在 IIT 内。此标准涵盖的安全措施旨在防范、侦测和/或阻止对 IIT 结构进行改变或暗藏于 IIT 的行为，其可能导致未经许可的物资或人员有机可乘。

在装柜环节，必须制定程序检查 IIT 并妥善加封。处于运送中或“静待”状态的货物受到的控制较少，因此更容易遭渗透。也就是为什么铅封控制和追踪运送中的货物/交通运输工具的方法是关键安全标准。

供应链的破坏最常发生在运输过程中。因此，成员必须保持警惕，确保在整个供应链中遵守这些关键的货物标准。

关键词定义：国际运输工具（IIT） – IIT 包括国际贸易商品运输中，到岸的（无论满载或空载）、使用中、将要使用的集装箱、平板柜、单位装载设备（unit load devices, ULDs）、叉车、货厢车、运输罐、箱子、滑木箱、托盘、垫板、织物用芯子或特殊集装箱。

编号	标准	实施指南	必须 / 应该
5.1	交通运输工具和国际运输工具（IIT）必须存放在安全的区域，以防止未经授权的进入，导致 IIT 结构改变，或者（如适用）封条/柜门损毁。	交通运输工具和 IIT（无论空载或满载）的安全存放对于防止未经授权的进入非常重要。	必须
5.2	CTPAT 的检查过程必须具备安全和农业检查的书面程序。	随着涉及改装交通运输工具或 IIT 的走私日益猖獗，成员因此必须对其进行检查，查找可见的有害生物和严重的结构问题。因为防范通过交通运输工具和 IIT 所造成的有害生物污染也是至关重要的关注，因此在安全检查过程中增加了农业的部分。 有害生物污染的定义是指可见的任何形式的动物、昆虫或其他无脊椎动物（活的或死的、在生命周期的任何阶段，包括卵鞘或卵筏），或源自任何动物的有机物质（包括血液、骨	必须

编号	标准	实施指南	必须 / 应该
		头、毛发、皮肉、分泌物、排泄物）；可繁育或不可繁育的植物或植物产品（包括果实、种籽、叶、枝、根，树皮）；或其他有机材料，包括真菌；或土壤或水。其未包含在 I IT（例如集装箱、单位装载设备等）的货物清单中。	
5.3	CTPAT 成员必须确保进行下列有系统的 CTPAT 安全和农业检查。这些检查的规定将取决于供应链是陆路（加拿大或墨西哥）还是源自海外（海运和空运）而有所不同。在装柜之前，必须检查所有空的 IIT，并且当交通运输工具越过陆地边界进入美国时，也必须对其进行检查。 <u>通过铁路或多式联运经海、空、陆路边界（适用时）运输的 CTPAT 货物检查要求：</u> 必须对所有空集装箱和单位装载设备（ULDs）进行七点检查；并且必须对所有空的冷藏集装箱和 ULD 进行八点检查： 1. 前壁： 2. 左侧； 3. 右侧； 4. 地面； 5. 天花板/顶部； 6. 外门/内门，包括门锁机关的可靠性； 7. 外部/底盘；以及 8. 冷藏柜上的风扇罩。 <u>通过陆路边界公路交通运输工具的附加检查要求：</u> 交通运输工具/IIT 的检查必须在交通运输工具/ IIT 存放场进行。 在可行的情况下，必须在进出存放场时和装柜点进行检查。这些系统性检查必须包括 17 点检查：	对 IIT 和交通运输工具进行安全和农业检查，以确保其结构未被改装来隐藏违禁品或受到可见的农业害虫污染。 海外供应链装柜时需检查所有的 IIT。但是，如果海运/空运供应链风险较高，则可能需要包括更广泛的检查程序，包括对交通运输工具和/或对海港码头或航空后勤设施的检查。通常，通过陆路过境点的货物风险较高，因此交通运输工具和 IIT 要经过多次检查。 IIT 包括海运集装箱、冷藏集装箱/拖车、公路拖车、平板拖车、罐式集装箱、铁路/棚车，料斗和 ULD。 CTPAT 門戶的公共圖書館（Public Library Section）备有安交通运输工具/IIT 安全和农业的培训材料。	必须

编号	标准	实施指南	必须 / 应该
	拖拉机： 1. 保险杠/轮胎/轮辋； 2. 门、工具间和锁定机关； 3. 电池箱； 4. 空气呼吸机； 5. 燃料箱； 6. 内部驾驶室/卧舱；以及 7. 车顶/顶棚， **拖车**: 1. 第五轮区域 – 检查自然隔间/防滑板； 2. 外部 – 前端/侧面； 3. 后部 – 保险杠/门； 4. 前壁； 5. 左侧； 6. 右侧； 7.地板； 8. 天花板/顶棚； 9. 内门/外门和锁定机关；以及 10.外部/底盘。		
5.4	交通运输工具和 IIT（视情况而定）必须配备外部硬件，以便合理地预防其遭拆除。在加装任何铅封装置之前，必须全面检查集装箱的门、把手、杆、搭扣、铆钉、托架和门锁装置的所有其他零件，是否有变造和任何硬件不匹配的情况。	考虑使用带有防变造合页的集装箱/拖车。成员还可以在门的至少两个合页上放置保护板或销，和/或在每一侧的至少一个合页上放置粘性密封/胶带。	必须
5.5	所有交通运输工具和空的 IIT 检查均应记录在检查表上，其须包含下列各项： •集装箱/拖车/IIT 编号；		应该

编号	标准	实施指南	必须 / 应该
	•检查日期； •检查时间； •进行检查的员工姓名；和 •所检查的 IIT 具体位置。 如果检查受到监督，主管还应在表上签名。 完整的集装箱/IIT 检查表应作为装运单据包的一部分。收货人应在收到商品之前收到完整的装运单据包。		
5.6	所有安全检查应在进出受到控制的区域内进行，如果有的话，应通过闭路电视系统进行监控。		应该
5.7	如果在交通运输工具/IIT 检查中发现可见的有害生物污染，则必须进行清洗/吸尘。文件必须保留一年以证明符合这些检查要求。	将所发现的污染物类型、发现地点（交通运输工具上的发现点）以及消除方法记录下来，有助于帮助成员防止未来再次发生。	必须
5.8	根据风险，管理人员应在运输工作人员完成交通运输工具/IIT 检查之后，对交通运输工具进行随机搜查。 应当定期进行交通运输工具的搜查，并根据风险提高频率。搜查应在没有警告的情况下随机进行，因此无法预测。检查应针对交通运输工具环节薄弱的各个地点进行：承运人堆场、卡车装载后以及在前往美国边境的途中。	对交通运输工具进行监督搜查来防范发生内部阴谋的情况。 最佳的做法是由主管将物品（例如玩具或彩盒）藏在交通运输工具中，看看现场测试筛查员/交通运输工具操作员是否会发现。 监督人员可以是对高级安全管理层负责的安全经理，也可指定其他管理人员。	应该
5.14	CTPAT 成员应与其运输提供商合作，从起点到终点跟踪交通运输工具。与服务提供商签订的服务协议应纳入跟踪、报告和共享数据的具体要求。		应该
5.15	托运人应有权进入承运人的 GPS 车队监控系统，以便跟踪其货物的动向。		应该

编号	标准	实施指南	必须 / 应该
5.16	陆路边境运输在靠近美国边境时，对临时停靠应采取“不停靠”政策。	货物静止就会有风险。预定的停靠不在本政策的范围之内，但必须在整体跟踪和监视过程中加以考虑。	应该
5.24	在高风险地区以及即将抵达边境口岸前，CTPAT 成员应对运往美国的货物采取“最后机会”核查程序，检查交通运输工具/IIT 是否有遭到变造的痕迹，包括对交通运输工具的目视检查和 执行 VVTT 铅封核查程序。该检查应由受过适当培训的人员来进行。 V – 查看铅封和集装箱的门锁装置；确保没有问题； V – 比对核实装货单据的铅封号码； T – 拉扯铅封以确保妥善加封； T – 拧转子弹封，确保各个组件不会松动、彼此分离或铅封的部分有任何松动。		应该
5.29	如果发现任何对货物或交通运输工具安全性的可信（或检测到的）威胁，成员必须（在可行的范围内尽快）警告供应链中任何可能受影响的业务伙伴，以及在适用的情况下，通知执法部门。		必须

6. **封条安全** – 拖车和集装箱的加封，包括封条持续保持完整，乃为确保供应链安全的关键要素。封条安全包括制定全面的书面铅封政策来处理封條安全的各个方面，根据 CTPAT 规定正确使用封条，正确加封 IIT，并核实妥善加封。

编号	标准	实施指南	必须 / 应该
6.1	CTPAT 成员都必须制定详细的高安全性鉛封书面流程，说明封条在设施中和运输过程中的发放与管控。该流程必须提供封条被更动、变造或鉛封号有误时，所该采取的步骤，包括对事件的记录、通知合作伙伴的流程以及对事件的调查。调查结果必须加以记录，并且尽快采取纠正措施。 这些书面流程必须保留在操作基层，以方便获取。每年至少审核一次，必要时进行更新。 书面封条管控必须包含以下内容： **控制对封条的取得：** • 封条的管理仅限于被授权人员。 • 安全存放。 **库存、分配与追踪（封条记录）：** • 记录收到的新封条。 • 发放记录过的封条。 • 利用记录追踪封条。 • 只有经过培训的授权人员才能加封 IIT。 **控制运输过程中的封条：** •提领被加封的 IIT 时（或停靠以后），要检查封条是否完好无损，没有被编造的痕迹。 • 确认鉛封号码与装运单据相符。 **运输过程中拆封的情况：** •如果是因为检查货物而拆封，记录所更换的鉛封号码。 •司机必须立即通知调度员拆封的情况，说明何为拆封人，并提供新的鉛封号码。		必须

编号	标准	实施指南	必须 / 应该
	• 承运人必须立即通知托运人、代理人和进口商鉛封变更事宜并提供新鉛封号码。 • 托运人必须立即记录新的鉛封号码。 **封条異樣：** • 保存被更动或变造的封条，以协助调查。 • 调查异样；之后采取纠正措施（如有必要）。 • 在适用的情况下，向 CBP 及相关外国政府报告铅封遭破坏的情况，以协助调查。		
6.2	所有可加封的 CTPAT 货物在装櫃/包装之后，都必须立即由责任方（即托运人或替其工作的包装人）用符合或超过国际标准化组织（International Organization for Standardization, ISO）17712 最新标准的高安全性封条进行加封。合格的钢丝封和子弹封均可接受。所有的封条都必须牢固并妥善加封在运送 CTPAT 成员货物至/自美国的 IIT 上。	如果有安全凸轮的话，所使用的高安全性封条必须装在安全凸轮的位置而不是右侧门的把手上。鉛封必须放在集装箱右侧门最中间的垂直杆的底部。如果没有安全凸轮的话，也可以把鉛封放在集装箱右侧门最中间的左侧把手锁件上。如果使用的是子弹封，建议将鉛封的螺栓部分或插入件朝上，使得螺栓部分在搭扣上方。	必须
6.5	CTPAT 成员（有封条库存者）必须记录所使用的高安全性封条符合或超过当前最新的 ISO 17712 标准。	检测实验室所出具符合 ISO 高安全性封条标准的证书是可接受的合规证据。CTPAT 成员应当了解其所购买的鉛封如何显示遭外力毁损。	必须
6.6	有封条库存的 CTPAT 成员，其公司管理层或安全主管必须进行封条稽核，包括定期清点库存封条，将封条库存记录和装运单据相互比对。所有稽核都必须有所记录。 作为完整的鉛封稽核过程的一部分，码头主管和/或仓库管理人员必须定期核查交通运输工具和 IIT 上的鉛封编号。		必须

编号	标准	实施指南	必须 / 应该
6.7	必须遵守 CTPAT 的鉛封验证程序以确保所有的高安全性封条（子弹封/钢丝封）妥善安装在 IIT 上，并按设计发挥作用。该流程被称为 VVTT 程序： V – 查看铅封和集装箱的门锁装置；确保没有问题； V – 比对核实装货单据的铅封号码； T – 拉扯铅封以确保妥善加封； T – 拧转子弹封，确保各个组件不会松动、彼此分离或铅封的部分有任何松动。	使用钢丝封时，要将其缠绕包住垂直杆的矩形硬件底座，以防止鉛封上下移动。装上鉛封之后，要将钢丝两头多余的部分去掉。VVTT 流程对钢丝封的要求是要确保拉紧钢丝。鉛封放置好后，拉扯钢丝以确认锁体内的钢丝不会滑脱。	必须

7. <u>程序安全</u> - 程序安全包括进出口流程、文件记录以及货物储存处理要求等许多方面。其他重要的程序标准涉及报告事件和通知相关执法部门。此外，CTPAT 往往要求制定书面程序，因其有助于保持程序长期一致。但是，书面程序所需细节多寡取决于各种因素，例如公司的商业模式或程序所涵盖的内容。

CTPAT 认识到供应链所使用的技术日异。标准中所提及的术语如书面程序、文件和表格，不意味全是纸质版。电子文本、签名及其他数子技术都可满足这些要求。

本计划并非是个“一刀切”的模式；各公司必须（根据其风险评估）自行决定如何实施和维持各种程序。但是，更为有效的是将安全流程纳入到现有程序中，而不是另外制定一份安全程序手册。如此一来，创建的架构会更有持续性，并有助于强调供应链安全是每个人的责任。

编号	标准	实施指南	必须 / 应该
7.1	如果货物将整夜或长期暂存，必须采取措施防止未经授权的人接近。		必须
7.2	必须定期检查货物准备区和周边区域，以确保不受可见的有害生物污染。	必要时，可以使用诱饵、诱捕器或其他障碍物等预防措施。清除杂草或减少植物丛生有助于防范有害生物在货物准备区的滋生。	必须
7.4	货物装柜至集装箱或 IIT 时，应由安全官员/经理或其他指定人员进行监督。		应该
7.5	作为正确安装铅封有据可查的证据，应在装柜点拍照。在可行的范围内，应将这些图像以电子方式转发到目的地，以进行核实。	摄像证据可以包括在装柜点拍摄的照片，以记录货物标记、装载过程、鉛封放置的位置以及正确安装的鉛封。	应该
7.6	必须实施程序来确保商品/货物清关所需的信息清楚、完整、准确，避免信息传递有误、丢失或引用错误，并按时报告。		必须
7.7	如果使用的纸质文件，表格及其他进出口相关文件都应该受到保护，以防被未经授权使用。	使用上锁的文件柜等措施可以防范未经授权使用包括货单在内的空白表格。	应该

编号	标准	实施指南	必须 / 应该
7.8	托运人或其代理必须确保提单（bill of ladings, BOLs）和/或舱单正确反映提供给承运人的信息，承运人则必须进行尽职调查确保文件准确无误。BOL 和舱单必须及时提交 CBP。所提交的提单必须显示承运人取得运往美国货物的外国起始地点/设施。重量与件数都必须准确。	承运人提取加封的 IIT 时，可依赖托运人托运说明中的信息。 要求将鉛封号码电子打印在 BOL 或其他出口文件上有助于防止鉛封被更换以及造假相关文件来配合新的铅封号码。 但是，某些供应链的货物在运输过程中会受到外国海关或 CBP 的检查。IIT 被政府拆封检查后，必须重新记录新的鉛封号码。在某些情况下，可以手写。	必须
7.23	CTPAT 成员必须制定报告事件的书面程序，包括说明设施内部提高事件处理层级的流程。 制定通知程序来报告发生在世界各地且会影响成员供应链安全的任何可疑活动或安全事件（如缉获毒品、发现偷渡客等）。发生任何全球性事件时，在适用的情况下，成员必须告知供应链安全专家、最近的出入境口岸、相关执法部门以及受影响供应链中的业务伙伴。必须在交通运输工具或 IIT 跨越边境前，尽可能快地通知 CBP。 通知程序必须包括正确的联系信息，列出所需要通知的人员和执法部门的姓名与电话号码。程序必须定期审查，以确保联络信息正确无误。	必须通知 CBP 的例子包括（但不限于）： • 发现集装箱/IIT 或高安全性封条遭到毁损； • 在交通运输工具或 IIT 中发现隐密隔间； • 在 IIT 上使用未登记的新鉛封； • 走私违禁品，包括人员、偷渡者； • 未经授权进入交通运输工具、火车、船只或航空母舰； • 勒索、索取保护费、威胁以及/或恐吓； • 未经授权使用商业实体识别（如进口商备案（Importer of Record, IOR）编号、承运人标准数字编码（Standard Carrier Alpha code, SCAC）等）。	必须
7.24	必须制定程序用于识别、质问和处理未经授权/身分不明的人员。工作人员必须了解如何质问不明/未经授权人员、如何应对情况，并熟悉将未经授权人员遣离该地点的流程。		必须
7.25	CTPAT 成员应建立可匿名举报与安全相关问题的机制。收到指控后，进行调查。如适用，应采取纠正措施。	如果可以匿名举报，诸如盗窃、欺诈和内部阴谋等问题会更易于被举发。 成员可设立热线或类似机制，让担心遭到报复的人匿名举报。建议保留所有举报报告，用以证明已进行调查并予以纠正。	应该

编号	标准	实施指南	必须 / 应该
7.27	任何短缺、超额或其他重大差异或异常都必须进行适当的调查并加以解决。		必须
7.28	到岸货物应与货物舱单信息核对一致。离港货物应与采购订单或交货单进行核对。		应该
7.29	货物具体鉛封号码应在出发前发送给收货人。		应该
7.30	鉛封号码应以电子方式打印在提单或其他装运单据上。		应该
7.37	一旦发生重大安全事件，成员们在得知后，必须立即启动事件后分析，以便决定供应链可能遭到破坏的环节为何。该分析不得妨碍/干扰政府执法机构所进行的任何已知调查。公司的事件后分析结果必须做记录，尽可能迅速完成。如执法机关允许，当供应链安全专家（SCSS）提出請求时，向其提供。	安全事件是指经由规避、躲避或违反安全措施的入侵，其已造成或将导致犯罪行为。安全事件包括恐怖主义行为、走私（毒品、人口等）以及出现偷渡客。	必须

8. <u>农业安全</u> — 农业是美国最大的产业和最大的就业部门，同时也是受到外来动植物污染威胁的产业，包括土壤、有机肥、种子以及带有入侵性或破坏性病虫害的动植物材料。消除各类交通运输工具和货物中的污染物可减少 CBP 将货物暂时扣押、延迟和商品退回或处理。确保遵守 CTPAT 的农业要求也有助于保护美国的关键产业以及全球食物供应链。

关键词定义：有害生物污染 — 国际海事组织将有害生物污染定义为可见形式的动物、昆虫或其他无脊椎动物（活的或死的、在生命周期的任何阶段，包括卵鞘或卵筏），或源自任何动物的有机物质（包括血液、骨头、毛发、皮肉、分泌物、排泄物）；可繁育或不可繁育的植物或植物产品（包括果实、种籽、叶、枝、根，树皮）；或其他有机材料，包括真菌；或土壤或水。其未包含在 IIT（例如集装箱、单位装载设备等）的货物清单中。

编号	标准	实施指南	必须 / 应该
8.1	CTPAT 成员必须根据其商业模式制定书面程序，以防止可见的有害生物污染，包括遵守木质包装材料（Wood Packaging Materials, WPM）法规。在整个供应链对中，必须遵守可见的有害生物防治措施。有关木质包装材料的措施必须符合国际植物保护公约（International Plant Protection Convention, IPPC）的国际植物检疫措施标准第 15 号》（International Standards for Phytosanitary Measures No. 15, ISPM 15）。	木质包装材料（WPM）的定义是用于支撑、保护或运送商品而使用的木材或木制品（不包括纸制品）。WPM 如托盘、板条箱、盒子、卷轴和垫舱物料等，很多时候可能都是以未经充分加工或处理清除或消灭有害生物的木材原料所制成的，因此成为有害生物输入和传播途径。垫舱物料尤其具有输入和传播有害生物的高风险。 IPPC 是联合国粮食及农业组织（United National's Food and Agriculture Organization）所监督的多边条约，旨在确保采取协调一致的有效行动，防治并控制有害生物及污染物的输入和传播。 ISPM 15 包含国际认可的措施，适用于 WPM，以大幅降低可能大部分与其有关的有害生物输入和传播风险。ISPM 15 影响所有 WPM，要求剥皮之后，经过热处理或溴甲烷熏蒸，再加盖或烙印 IPPC 合规标记，其俗称为“小麦印章”。不受 ISPM 15 管制的产品都是用其他材料制成的，例如纸类、金属、塑料或木板产品（如定向刨花板、硬质纤维板和胶合板）。	必须

第三个关注领域：人员和场地实体安全

9. **场地实体安全** – 货物装卸和储存设施、IIT 存放区以及在国内外准备进出口文件的设施都必须设有实体屏障和吓阻设备，以防范未经授权者进入。

CTPAT 的基石之一是其灵活性，因此安全计划应根据公司情况来制定。场地实体安全的需求差异大大取决于成员在供应链中的角色、商业模式以及风险等级。场地实体安全标准提供多个吓阻/障碍手段，避免未经授权接近货物、敏感设备以及/或信息。CTPAT 成员应在整个供应链中采取这些安全措施。

编号	标准	实施指南	必须 / 应该
9.1	所有货物装卸和储存设施，包括拖车场和办公室，都必须设有实体屏障和/或吓阻设备，以防范未经授权者进入。		必须
9.2	货物装卸与储存设施周边应以围栏围住。装卸货物的设施应设置内部围栏，以保证货物和货物装卸区的安全。根据风险情况，还应加装内部围栏以分隔不同类型的货物，如国内、国际、高价值和/或危险材料。围栏的完整与损坏情况应由指定人员定期检查。围栏如有损坏，应尽快修复。	除了围栏以外，也可使用其他可接受的屏障，如分隔墙、无法穿越的或会造成阻碍的自然屏障，如陡峭的悬崖或茂密的树丛等。	应该
9.4	车辆和/或人员进出的大门（以及其他出口点）必须有人值守或监控。可以根据当地法律和劳动法对人员与车辆进行搜查。	建议大门设置的数量为最低必要，兼顾适当通行和确保安全。其他出口点为未设闸门的设施入口。	必须
9.5	应禁止私人车辆停放在货物装卸和储存区或紧邻区域，也不得停放在交通运输工具旁。	停车场应设于围栏外和/或操作区外，或者至少要与货物装卸和储存区保持相当的距离。	应该
9.6	设施内外部应有足够的照明，如适用，包括以下区域：进出入口、货物装卸和储存区、围栏沿线和停车场。	在照明设备中加装自动定时器或光传感器启动适当安全照明，会更加有效。	必须

编号	标准	实施指南	必须 / 应该
9.7	应利用安防技术监视设施，以防止未经授权进入敏感区域。	用来保护/监控敏感区域和出入口的电子安防技术包括：防盗警报系统（周边和内部），其也被称作入侵检测系统（Intrusion Detection Systems, IDS）；门禁管制设备；以及视频监视系统（video surveillance systems, VSS），包括闭路电视摄像机（Closed Circuit Television Cameras, CCTVs）。CCTV/VSS 系统可包括模拟摄像机（基于同轴电缆）、IP 网络摄像机（基于网络）、录像设备以及视频管理软件。 视频监控保护的安全/敏感区域包括：货物装卸和储存区、保存进口文件的发货/收货区、IT 服务器、IIT 存放场、IIT 检查区以及封条存放区。	应该
9.8	依靠安防技术确保场地安全的成员必须制定书面政策和程序来管理对技术的使用、维护和保护。 这些政策和程序至少必须规定： • 只有得到授权的人员才能进入技术控制和管理地点； • 已定期实施测试/检查技术的程序； • 检查应包括核实所有设备运作正常，如适用，并核实设备放置正确； • 检查和性能测试的结果应加以记录； • 如需要进行纠正，应尽快实施，并将纠正措施加以记录； •检查记录应保存足够的时间，以便稽核； 如使用第三方中央监控站（异地），CTPAT 成员必须备有书面程序，规定主要系统的功能以及身份验证程序，例如（但不限于）安全代码更改、增减授权人员、密码修改以及进入	安防技术需定期测试以确保运作正常。可遵循的一般指南如下： • 维修后、对建筑物或设施进行大修、改造或增建期间和之后，需检测安全系统。系统部件可能被有意或无意间受到损坏。 •电话或互联网服务发生任何重大更改后，需检测安全系统。任何可能对系统与监控中心沟通产生影响的部分，都必须重复检查。 • 确保视频设置正确，如动态激活摄影、动态侦测警报、每秒图像帧数（image per second, IPS）及画质等。 • 确保摄像头（或保护摄像机的球型罩）的清洁，准确对焦。不可被障碍物或强光限制其可见性。 • 确保安全摄像机放置正确，并保持在正确的位置（摄像机可能被有意或无意遭移动）。	必须

编号	标准	实施指南	必须 / 应该
	系统或遭到拒绝。 安防技术政策和程序必须每年审查并更新。根据风险情况，可增加频繁。		
9.9	CTPAT 成员在设计和安装安防技术时，应使用有授权许可/经认证的资源。	当今的安防技术非常复杂，且日新月异。公司往往采购错误，以至于在需要的时候无法发挥作用和/或付出不必要的高昂费用。寻求合格的指导有助于买方根据需求和预算选择适合的技术。 根据美国国家电器承包商协会（National Electrical Contractors Association, NECA），全美目前有 33 个州规定安防和警报系统安装人员必须持有专业执照。	应该
9.10	必须对所有安防技术基础设施进行实体保护，以防止未经授权进入。	安防系统基础设施包括计算机、安防软件、电子控制板、视频监控或闭路电视摄像机、摄像机和录像所需的电源及硬件。	必须
9.11	安防技术系统应配置备用电源，以确保突然失去直接电源时，系统仍能继续运行。	企图闯入的犯罪分子可能会试图切断安防技术的电源，以便避开监控。因此，安防技术配置替代电源是至关重要的。替代电源可以是辅助发电来源或备用电池。备用发电机也可用于照明等其他关键系统。	应该
9.12	如使用摄像机系统，摄像机应监控设施现场和敏感区域，以阻止未经授权的进入。如发生未经授权进入敏感区的情况，应利用警报系统通知公司。	如适用，敏感区域可包括货物装卸和储存区、保存进口文件的发货/收货区、IT 服务器、IIT 存放区、IIT 检查区和封条放存区。	应该
9.13	如安装摄像机系统，确保摄像机的位置能覆盖设施中与进出口流程有关的关键区域。 摄像机画质应设在最清晰的设定，并设置为全天候摄像。	正确放置摄像机是至关重要的，以便在设施的控制范围内，尽可能对实体“监管链”进行录像。 根据风险，关键区域或流程可包括货物装卸和储存区、发货/收货区、货物装载流程、铅封流程、交通运输工具的进出、IT	必须

编号	标准	实施指南	必须 / 应该
		服务器、集装箱检查区（安全和农业检查）、鉛封放存区以及任何与确保国际货运安全有关的其他领域。	
9.14	如使用摄像机系统，其应具备警告/通知功能，可以发出“操作/记录失败”的信号。	视频监控系统的故障有可能是人为的，其为了避免留下闯入供应链的证据，从而使系统失灵。操作失败信号功能会传送电子通知，告知预先指定人员设备需要立即进行检查。	应该

编号	标准	实施指南	必须 / 应该
9.15	如使用摄像机系统，必须（由管理层、安全或其他指定人员）对录像片段进行定期、随机检查，以核查是否依法正确执行货物安全程序。审查结果必须予以书面总结，包括所采取的任何纠正措施，并保存足够的时间，以便进行稽核。	如果检查录像片段只是为了找寻原因（作为安全事件调查的一部分），则无法充分发挥安装摄像机的好处。摄像机不仅仅只是调查工具，如能善加利用，可防范于未然。 录像片段的随机检查应针对实体监管链，以确保货物安全并遵守所有的安全规程。可进行检查的流程如下： • 货物装卸活动； • 集装箱检查； • 装载流程； • 铅封流程； • 交通运输工具的进出；以及 • 货物运离等。 **审查目的：**审查是为了评估全面遵守安全流程的情况以及是否有效。找出落差或弱点并加以纠正，以期改善安全流程。成员可根据风险（既往事件或有关员工未遵守装卸区安全流程的匿名举报等），定期进行审查。 **书面总结中应包括的项目：** • 审查日期； • 审察录像片段的日期； • 来自哪个摄像机/区域； • 简要说明情况；以及 • 如有必要，所采取的纠正措施。	必须
9.16	如使用摄像机，用來監控货物的关键进出口流程录像片段應保存足够的时间，以完成调查。	如果发生安全事件，便需要进行调查。因此，妥善保存监控包装（用于出口）和装载/铅封流程的录像片段极为重要，才能调查供应链受到破坏的环节。 为了进行监控，CTPAT 建议，从货物抵达分销第一站算起，至少再将录像片段保存 14 天。这是清关后，集装箱首次被打开。	应该

10. **<u>场地实体门禁管制</u> —** 门禁管制可防止未经授权者进入设施/区域，有助于管理员工和访客，并保护公司资产。门禁管制包括在各个入口核实所有员工、访客、服务提供商和厂商的身份。

编号	标准	实施指南	必须 / 应该
10.1	CTPAT 成员必须有发放、变更和取消识别证和门禁卡的书面程序。 在适用的情况下，必须建立员工识别系统以核实身份和管制进出。敏感区域的进出权限取决于工作描述或指定职责。员工离职时，必须取消其门禁卡。	门禁卡包括员工识别证、访客和厂商临时识别证、生物识别系统、感应钥匙卡、代码和钥匙。员工离职时，使用离职清单确保返还和/或取消所有门禁卡。小公司员工相互认识，因此无须使用识别系统。一般来说，公司员工人数超过 50 名，便需要使用识别系统。	必须

编号	标准	实施指南	必须 / 应该
10.2	访客、厂商以及服务提供商必须在到达时出示带照片的身份证件，并登记拜访细节。所有来访者均应有人陪同。此外，应向所有访客和服务提供商发放临时识别证。如使用临时识别证，必须全程配戴。 访客日志必须包括以下内容： • 到访日期； • 访客姓名； • 验证带照片的身份证件（验证类型如驾照或国民身份证）。熟悉的访客，如固定厂商，可不用核实有照证件，但仍必须经过登记才能进出设施； • 到达时间； • 公司联系人；以及 • 离开时间。		必须
10.3	在接收或放行货物之前，必须核实收送货物的司机身份。其必须向有权允许进入设施的员工出示政府所颁发带有照片的身份证件，以验证其身份。如果出示该类证件不可行，设施员工则可以接受其雇主公路承运公司所发放、可识别的有照证件。		必须

编号	标准	实施指南	必须 / 应该
10.4	必须备有提货日志以登记司机，并详细记录其提货时的交通运输工具。司机抵达设施提货时，该设施员工必须将其登入在提货日志中。司机离开时，必须登出。日志必须妥善保存，司机不得接近。 提货日志应包括下列各项： • 司机姓名； • 到达日期与时间； • 雇主； • 卡车编号； • 拖车编号； • 离开时间； • 离开时货车上的鉛封号码。	访客日志也可作为提货日志，只要记录额外信息即可。	必须
10.7	在到达前，承运人应通知设施提货预计到达时间、司机姓名和卡车编号。在可操作的情况下，CTPAT 成员应当只接受提前预约的交货与提货。	该标准有助于托运人和承运人避免假冒提货。假冒提货是通过欺骗盗取货物的犯罪阴谋，包括卡车司机使用假证件和/或成立假公司以便盗取货物。 如果承运人有固定的司机从某个设施提货时，最好的做法是由设施保存一份带有照片的司机名单。如此一来，即使无法事先得知提货司机，仍可确认其为核准至该设施提货的司机。	应该
10.8	应定期篩查收到的包裹和邮件，以防夹帶违禁品。	违禁品包括但不限于爆炸物、非法毒品和货币。	应该
10.10	如雇佣保安人员，书面政策与程序必须包含其工作指示。管理层必须通过稽核和政策审查定期核查合规和适用情况。	尽管任何设施皆可派驻保安人员，但派驻地点通常为制造设施、海港、配送中心、IIT 存放场、拼装业主和货运代理人的作业场所。	必须

11. <u>人员安全</u> **—** 公司的人力资源是其最关键的资产之一，但也可能是最薄弱的安全环节之一。本标准侧重于员工筛选和职前核查等问题。许多安全违规都是由内部阴谋造成的，也就是一名或多名员工合谋规避安全程序來渗透供应链。因此，成员必须进行尽职调查，以确保敏感职位上的员工可靠并值得信赖。敏感职位包括直接处理货物或其文件的人员以及控制进入敏感区域或设备的人员。此类职位包括但不限于发货、收货、邮件收发室、司机、调度员、保安人员、任何参与装载货物、交通运输工具追踪和/或鉛封控制的人员。

编号	标准	实施指南	必须 / 应该
11.1	必须制定书面程序筛查应聘员工并定期核查现任员工。聘用前，在法律允许的范围内，必须尽可能地核实其就业经历和进行资历查核。	CTPAT 了解某些国家的劳工法和隐私法可能不允许核实所有的应聘信息。但在允许的范围内，应尽职调查，对其進行核查。	必须
11.2	根据适用的法律限制以及可用的犯罪记录数据库来进行员工背景调查。根据职位的敏感性，员工审查要求应扩展包括临时和合同员工。雇佣后，应根据原因和/或员工职位的敏感性定期进行重新调查。 员工背景调查应通过市、州、省和全国的数据库进行包括身份和犯罪记录的核查。CTPAT 成员及其业务伙伴决定是否聘用时，在当地法律允许的范围内，应考虑背景调查的结果。背景调查不限于核实身份和犯罪记录。在风险较高的领域，可能需要更深入的调查。		应该
11.5	CTPAT 成员必须制定员工行为准则，其包括对员工的期望并解释可接受的行为。该行为准则必须包括惩罚与纪律处分程序。员工/合同员工必须签名确认已阅读并理解。该文件必须作为记录保存在员工的档案中。	制定行为准则有助于保护公司并告知员工公司的期望。其旨在于制定形并维护公司可接受的行为标准，助其树立专业形象并且建立强大的道德文化。即使是小公司也需制定行为准则，但其设计或所包含的信息不需复杂。	必须

12. **<u>教育、培训与安全意识</u>** — CTPAT 安全标准设定来作为分层安全系统的基础。如果其中一层受到影响，则另一层应防止安全受到破坏或向公司发出警告。执行和维护分层安全计划需要多个部门和人员的积极参与和支持。培训是维护安全计划的关键之一。教育员工何为威胁以及为何其在公司供应链的保护中扮演重要角色，才能确保供应链安全计划的成功与持久。而且，当员工对为何实施安全程序的原因有所了解之后，更有可能切实遵守。

编号	标准	实施指南	必须 / 应该
12.1	成员必须建立并维持安全培训及安全意识计划，以识别并增强对供应链中每个点的设施、交通运输工具和货物的安全漏洞的认识。这些漏洞可能被恐怖分子或禁运品走私者利用。培训计划必须全面，而且覆盖 CTPAT 的所有安全规定。在敏感职位的人员必须接受针对该职位所应承担职责的附加专门培训。 培训是安全计划的关键之一。员工了解为何采取安全措施，就更可能对其切实遵守。安全培训必须根据员工的职能和职位，按规定定期举办，该培训应作为新进员工入职培训/职业技能培训的一部分。 成员必须保存培训证据，例如培训记录、签到单（名册）或电子培训记录。培训记录应包括培训日期、参加培训人员姓名和培训主题。	培训主题可以包括保护门禁管制、识别内部阴谋，以及报告可疑活动或安全事件的程序。如果可能，专门培训应包括现场演示。如果进行现场演示，教员应留出时间来让学生演示该流程。 对于 CTPAT 而言，敏感职位包括直接处理进出口货物或其文件的人员，以及控制进入敏感区域或设备的人员。这些职位包括但不限于发货、收货、邮件收发室、司机、调度员、保安人员、任何参与装在货物、交通运输工具追踪和以/或铅封控制的人员。	必须

编号	标准	实施指南	必须 / 应该
12.2	负责对空的交通运输工具和 IIT 进行安全和农业检查的司机和其他人员都必须接受培训，以便对其交通运输工具/IIT 进行安全性农业检查。 温故培训必须定期举办。发生事件或安全漏洞之后如有需要或者公司程序有所变更时，也应举办。 检查培训必须包含以下主题： • 隐蔽隔间的迹象； • 隐藏在天然隔间中的违禁品；以及 • 有害生物污染的迹象		必须
12.4	CTPAT 成员应制定措施，核实所提供的培训符合其所有目标。	了解培训并能在其岗位上（对敏感职位的员工来言）学以致用，是至关重要的。成员可以采用考试或测验、模拟练习/演习或定期审查等方法来确定培训效果。	应该
12.8	在适用的情况下，必须根据人员的职责和/或职位进行有关公司网络安全政策和程序的培训，包括保护其密码/密码短语和计算机访问权限。	高质量的培训是降低网络攻击易受性的关键。完善的网络安全培训计划通常是在正式的环境中训练相关人员，而不是单单通过电邮件或备忘录来进行。	必须
12.9	操作和管理安全技术系统的人员必须接受各自领域的操作和维护培训。可接受先前类似系统的工作经验。通过操作手册和其他方法所进行的自我培训也是可接受的。		必须
12.10	员工必须接受如何报告安全事件和可疑活动的培训。	报告安全事件和可疑活动的程序是安全计划中极其重要的部分。有关如何报告事件的培训可以包括在整体培训之中。利用专门的培训单元（根据工作职责），可进行对报告程序更详细的培训，包括流程的具体细节，例如报告内容、报告对象、如何报告事件以及完成报告以后的后续工作。	必须

发行号码: 1080-0420