最低安全標準– 外國製造商

2020 年 1 月

注：標準的編號可能不連續。未列出編號的標準不適用於外國製造商。

第一個關注領域：企業安全

1. **安全願景與責任** – 海關商貿反恐聯盟（CTPAT）成員所實施的供應鏈安全計劃如要保持有效，必須得到公司高層管理人員的支持。將安全性注入公司文化，確保成為整個公司的優先事項，這主要是公司領導層的責任。

編號	標準	實施指南	必須/應該
1.1	在促進安全文化方面，CTPAT 成員應通過一份支持聲明，表明其對供應鏈安全和 CTPAT 計劃的承諾。該聲明應由公司高層官員簽名之後，張貼於公司適當的地點。	支持聲明應強調保護供應鏈免遭如毒品販運、恐怖主義、人口走私和非法違禁品等犯罪活動破壞的重要性。應該支持和簽署聲明的公司高層官員可包括總裁、首席執行官、總經理或安全總監。張貼地點包括公司網站、公司關鍵區域的海報上（接待前台、包裝、倉庫等）和/或作為公司安全性研討會的一部分等等。	應該
1.2	為了構建完善的供應鏈安全計劃，公司應將所有相關部門代表納入跨部門團隊。 這些新的安全措施應納入在公司現有的程序中，創造一個更加可持續的結構，並強調確保供應鏈安全人人有責。	供應鏈安全所涵蓋的範圍比傳統安全計劃要廣得多，與許多部門的安全緊密關聯，如人力資源、資訊技術和進/出口辦公室。從長遠來看，建立在安全部門的傳統供應鏈安全計劃可能不太可行，因為執行安全措施的責任集中在少數員工身上，容易受到關鍵人員流失的影響。	應該

編號	標準	實施指南	必須/應該
1.3	供應鏈安全計劃必須經由適當的明文審查規定來設計、支持和實施。審查的目的是為了要記錄系統執行時，有關人員對職責負責，並且按照安全計劃的設計執行所有安全程序。審查計劃必須根據公司營運和風險等級的相關變化進行更新。	對 CTPAT 進行審查的目的是為了確保員工遵守公司的安全程序。審查流程不必複雜。成員根據其在供應鏈中的角色、商業模式、風險等級以及特定地點/場所之差異來決定審查的範圍及深入程度。 較小的公司可制定非常簡單的審查方法，而大型跨國企業集團可能需要更大規模的流程，並可能需要考慮各種因素，例如當地法律規定等。一些大型公司可能已有稽查工作人員，可協助進行安全審查。 成員可以選擇針對某些特定程序進行小規模審查。對於供應鏈安全至關重要的特殊領域，例如檢查和封條控制，可以進行針對這些領域的審查。但是，定期進行全面總檢查有助於確保安全計畫的各方面都按照設計發揮作用。假使成員已在年度審查中納入該類檢查，便足以滿足該標準。 對於具有高風險供應鏈（由其風險評估決定）的成員，其審查流程可包括模擬或桌面演練，以確保員工了解實際發生安全事件時如何應對。	必須
1.4	公司內部的 CTPAT 聯絡人必須對 CTPAT 計劃的規定充分了解。這些人員需要就與計劃相關的問題定期向上級管理層提供最新情況，包括任何審查的進展或結果、與安全相關的演練以及 CTPAT 認證。	CTPAT 希望所指定的聯絡人能夠積極主動地與其供應鏈安全專家進行互動，及時回應。成員可以加派其他可以幫助支持該職能的人員，並在 CTPAT 門戶網站上將其列為聯絡人。	必須

2. **<u>風險評估</u>** – 恐怖組織和犯罪集團針對供應鏈的持續威脅，凸顯出成員必須評估這些不斷演變的威脅其現有和潛在的風險。CTPAT 認識到，當公司的供應鏈涉及多個商業夥伴時，這些供應鏈的安全保障將更為複雜。當公司擁有多個供應鏈時，應將重點放在具有較高風險的地理區域/供應鏈上。

在決定供應鏈的風險為何時，成員必須考慮各種因素，例如商業模式、供應商的地理位置以及特定供應鏈可能具備的特殊情況。

關鍵詞定義：風險 – 衡量不測事件所造成的潛在危害，包括其威脅、脆弱性和後果。風險等級取決於威脅發生的可能性。發生的可能性高，通常等於高風險。風險可能無法排除，但可透過來管控降低 - 即減少漏洞或降低對業務的整體影響。

編號	標準	實施指南	必須/應該
2.1	CTPAT 成員必須對其供應鏈中的風險等級進行評估和記錄。 CTPAT 成員必須進行全面風險評估（risk assessment, RA），以識別可能存在安全漏洞的環節。RA 必須識別威脅、評估風險並採用可持續措施減少漏洞。成員必須考慮到 CTPAT 對其在供應鏈角色中的具體要求。	全面風險評估（RA）由兩個關鍵部分組成。第一部分是成員自我評估其設施內的安全實踐、程序和政策，以確認符合 CTPAT 最低安全標準，並對管理層如何管控風險進行全面評估。 RA 的第二部分是國際風險評估。這部分包括根據成員的商業模式和在供應鏈中的角色來確定地理威脅。在審視每種威脅對成員供應鏈安全的可能影響時，成員需要一種方法來評估或區分風險等級。一種簡單的方法是將風險分成低級、中級和高級。 CTPAT 制定了五步風險評估指南（Five Step Risk Assessment），以幫助成員進行全面風險評估中的國際風險評估部分，該指南可在美國海關暨邊境保護局（U.S. Customs and Border Protection, CBP）網站查找 https://www.cbp.gov/sites/default/files/documents/CTPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf。 對於擁有大量供應鏈的成員，主要關注點應放在風險較高的領域。	必須
2.2	風險評估的國際部分應記錄或詳細標示成員貨物在供應鏈中從原發地到進口商配送中心的運送流程。流程圖應包括所有直接或間接參與貨物出口/運輸的商業夥伴。	制定供應鏈流程圖時，首先要考慮高風險區域。 在記錄所有貨物的移動情況時，成員應考慮所有適用的參與方，包括僅處理進出口文件的，如報關行，以及可能不直接處理貨物但可能具有操作控制權的，例如無船公共運送人（Non Vessel Operated Common Carriers, , NVOCCs）或第三方物流企業（Third Party Logistics	應該

編號	標準	實施指南	必須/應該
	在適用的情況下，流程圖應包括記錄貨物如何進出運輸設施/貨運樞紐，並註明貨物是否會在某定點“靜待”多時。貨物在“靜待”狀態等待下一段行程時，更容易出問題。	Providers , 3PL）。如果任何運輸環節是分包出去的，也應列入考慮，因為間接方層次越多，涉及的風險就越大。 制定流程圖涉及更深入地了解供應鏈的運作。除了可識別風險外，還可用於查找供應鏈低效環節，有利於降低成本或縮短產品運抵時間。	
2.3	風險評估必須每年審查一次，或者根據風險因素進行更頻繁的審查。	可能需要每年進行不只一次的風險評估審查情況包括：來自特定國家/地區的威脅等級提高、警報升級的時段增加、安全漏洞或事件發生之後、商業夥伴改變和/或變更公司結構/所有權，例如併購等。	必須
2.4	CTPAT 成員應備有危機管理、業務連續性、安全復原計劃和恢復業務的書面程序。	危機可能包括由於網路攻擊、火災或武裝人員劫持承運商司機而導致貿易數據移動中斷。根據風險以及成員在何處營運或尋得貨源，應急計劃可以包括其他安全通知或支持，以及如何尋回被損毀或被盜的物品並恢復正常運作。	應該

3. <u>商業夥伴</u> **–** CTPAT 成員往來的商業夥伴，國內外皆有。至關重要的是，成员必须確保直接處理貨物和/或進出口文件的商業夥伴采取適當的安全措施，來保護貨物在整個國際供應鏈中的安全。當商業夥伴將某些工作分包出去時，整個流程會變得更複雜，在進行供應鏈風險分析時必須列入考慮。

關鍵詞定義：商業夥伴 – 商業夥伴乃為個人或公司，其行為可能影響貨物安全監管鏈，該類貨物透過 CTPAT 成員供應鏈向美國進口或從美國出口。商業夥伴可以是提供服務以滿足公司國際供應鏈內需求的任何一方。這些角色包括為 CTPAT 進口商或出口商成員或代表其進行貨物採購、文件準備、提供便利、處理、儲存和/或運送的所有（直接和間接）參與方。間接夥伴的兩個例子是分包承運商和由代理商/物流提供商所安排的海外綜合倉儲。

編號	標準	實施指南	必須/應該
3.1	CTPAT 成員必須備有基於風險的書面流程，以篩選新的商業夥伴和監督當前的合作夥伴。 此過程應包括檢查有關洗錢和資助恐怖分子的活動。為了協助完成此過程，請查閱 CTPAT 的基於貿易的洗錢和恐怖主義融資活動的警告指標 （Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities）。	審查公司是否合法的範例如下： •驗證公司的營業地址和在該地址的經營時間； •在網上對公司和其負責人進行研究； •核查業務證明人；以及 •索取信用報告。 直接商業夥伴是需要經過篩選的，例如製造商、產品供應商、相關廠商/服務提供商和運輸/物流提供商。任何與公司的供應鏈直接相關和/或處理敏感資料/設備的廠商/服務提供商也必須經過篩選；這包括經紀人或資訊技術（IT）契約提供商。進行篩查的深入程度取決於供應鏈的風險等級。	必須
3.4	商業夥伴篩選過程必須考慮合作夥伴是否是 CTPAT 成員或與美國簽有相互承認協議（Mutual Recognition Agreement, MRA）（或已批准 MRA）的授權經濟營運商（Authorized Economic Operator, AEO）計劃的成員。CTPAT 或已批准 AEO 認證是符合商業夥伴計劃要求可接受的證明，成員必須以證書為憑，並繼續監督商業夥伴以確保其證書持續有效。	商業夥伴的 CTPAT 認證可以通過其門戶網站的狀態驗證接口系統（Status Verification Interface）來確認。 如果商業夥伴認證來自與美國簽訂 MRA 的外國 AEO 計劃，則外國 AEO 認證將包括安全部分。成員可以訪問外國海關的網站，其 AEO 將列名於此，或者也可直接向其商業夥伴索取證書。 目前美國 MRA 包括：紐西蘭、加拿大、約旦、日本、韓國、歐盟	必須

編號	標準	實施指南	必須/應該
		（28 個成員國）、台灣、以色列、墨西哥、新加坡、多明尼加共和國和秘魯。	
3.5	當 CTPAT 成員將供應鏈環節外包或分包時，該成員必須進行盡職調查（通過訪查、問卷調查等），以確保其商業夥伴已採取符合或超過 CTPAT 最低安全標準（Minimum Security Criteria, MSC）的安全措施。	進出口商傾向於將很大一部分供應鏈活動外包。進口商（和某些出口商）通常屬於具影響力的交易當事方，如有必要，可要求其商業夥伴，在整個供應鏈中實施安全措施。對於不是 CTPAT 成員或 MRA 接受成員的商業夥伴，CTPAT 成員將進行盡職調查，以確保（在具備影響力的情況下）這些商業夥伴符合適用的安全標準。 進口商對商業夥伴進行安全評估來決定其對安全規定的遵守情況。必須收集多少商業夥伴安全計劃的資料取決於成員的風險評估。如供應鏈眾多，則優先考慮高風險區域。 確定商業夥伴是否符合最低安全標準，可以採用幾種方法來完成。根據風險，公司可以進行設施現場稽查，雇用承包商/服務提供商進行現場稽查或使用安全調查問卷。如果使用安全調查問卷，所需細節或證據的多寡取決於風險等級。高風險地區的公司可能需要提供更詳細的資料。如果成員向商業夥伴進行安全調查問卷，考慮要求下列各項： •填寫人的姓名和頭銜; •完成日期； •文件填寫人的簽名； •*公司高層官員、安全主管或授權公司代表的簽名，以證明問卷的準確性； •提供足夠的細節以便決定是否符合規定；以及 •根據風險，且在當地安全規程允許的情況下，包括提供照片證據、政策/程序副本以及填寫完整的表格，如國際運輸工具（Instruments of International Traffic）檢查清單和/或警衛日誌的副本。 *可以使用電子簽名。如果無法簽名或對其進行驗證，受訪者可以透	必須

編號	標準	實施指南	必須/應該
		過電子郵件證明問卷的有效性，並且證明答覆和任何支持證據均經主管/經理核准（要求提供姓名和頭銜）。	
3.6	如果在商業夥伴的安全評估過程中發現了弱點，則必須儘快處理，並且必須及時進行更正。成員必須通過書面證據確認缺失已得到解決。	CTPAT 認識到不同的修正所需的時間表也會有所不同。安裝實體設備通常比修改程序費時，但是一旦發現安全漏洞，便必須立即處理。例如，如果問題是更換損壞的圍欄，則必須立即開始採購程序（處理缺失），並且一旦可行時，儘快安裝新圍欄（糾正措施）。 根據所涉及的風險等級和弱點的重要性，某些問題可能需要立即處理。例如，如果該缺失可能危及貨櫃的安全，便必須儘快解決。 文件證據的範例可包括所增派的保全人員合同副本、顯示新安裝的安全攝影機或入侵報警器的照片或檢查清單的副本等。	必須
3.7	為確保其商業夥伴繼續遵守 CTPAT 的安全標準，成員應定期或根據情況/風險更新其對商業夥伴的安全評估。	定期審查商業夥伴的安全評估非常重要，才能確保安全計劃的持續和妥善運行。如果成員對商業夥伴安全計劃評估從未進行更新，當曾經可行的計劃不再有效時，便無法得知，該成員的供應鏈將因而面臨風險。 合作夥伴的安全評估核查頻率取決於成員的風險評估流程。較高風險供應鏈的核查將比低風險的供應鏈更加頻繁。如果商業夥伴的安全狀況是以實地訪查的方式來評估，則也可考慮加以利用進行其他必要訪查的機會。例如交叉培訓人員，使負責品管的人員也可以進行安全核查。 在某些情況下，可能必須更加頻繁地更新自我評估，包括貨源國威脅水平提高、貨源位置發生變化、新的關鍵商業夥伴（實際處理貨物或為設施提供安全服務的商業夥伴）。	應該

編號	標準	實施指南	必須/應該
3.8	貨物輸往美國時，如果成員將運輸服務分包給另一家公路承運商，則必須使用 CTPAT 認證的公路承運商或透過書面契約，列明其為向成員直接提供服務的公路承運商。契約必須規定遵守所有最低安全標準的要求。	承運商應向其提貨和交貨的設施提供分包承運商和司機的名單。分包商名單如有任何更改，均應立即告知相關合作夥伴。 在審查服務提供商符合規定的情況時，成員應核實分包的公司是實際運輸貨物的公司，並且未經批准不得再分包。 成員應僅將運輸服務分包一次。如果允許再分包的特例，當貨物再次分包時，必須通知 CTPAT 成員和託運人。	必須
3.9	CTPAT 成員應備有社會合規計劃，明文規定至少確保公司進口到美國的商品均非透過被禁止的勞工形式，無論全部或部分，來開採、生產或製造的，即強迫勞動、監獄勞工、契約勞工或契約童工。	私人部門為保護勞工權利而在其營運和供應鏈中所做的努力可以增進人們對勞工法律和標準的了解，並減少不良的勞工實踐。這些努力還為改善勞資關係創造環境，並增加公司收益。 1930 年關稅法第 307 條（Section 307 of the Tariff Act）（美國法典 19 U.S.C. § 1307）禁止從外國進口任何全部或部分由強迫勞動或契約童工，包括強迫童工，開採、生產或製造的商品。 國際勞工組織第 29 號公約（Labor Organization’s Convention No. 29）將強迫勞動定義為在懲罰的脅迫下，迫使任何人提供的所有工作或服務，且該人並非出於自願。 社會合規計劃是公司一系列的政策和實踐，旨在確保最大程度地遵守其涉及社會和勞工議題的行為準則。社會合規指的是企業如何承擔責任保護環境，以及員工的健康、安全和權利、其經營所在的社區以及供應鏈中工人的生活和社區。	應該

4. <u>網路安全</u> – 在當今的數位世界中，網路安全為其關鍵以保護公司最寶貴的資產 – 智慧財產權、客戶資訊、財務和貿易數據、員工記錄以及其他種種。隨著網路的連接越來越廣泛，公司資訊系統受到破壞的風險也隨之增加。該威脅涉及所有類型和規模的企業。確保公司資訊技術（IT）和數據安全的措施至關重要，所列標準為成員的整體網路安全計劃提供了基礎。

關鍵詞定義：網路安全 - 網路安全是一種行動或者過程，旨在保護電腦、網路、程式和數據免受意外或未經授權的取得、更改或破壞。它是一個過程，識別、分析、評估和傳達與網路相關的風險，考慮成本和利弊，從而接受、避免、轉移或將風險降低到可接受的水平。

資訊技術（IT） – IT 包括電腦、存儲、網路和其他實體設備、基礎建設和程序，以便建立、處理、儲存、保護和交換所有形式的電子數據。

編號	標準	實施指南	必須/應該
4.1	CTPAT 成員必須備有全面的書面網路安全政策和/或程序，以保護 IT 系統。書面的 IT 政策至少必須涵蓋所有個別的網路安全標準。	鼓勵成員遵循基於公認的行業框架/標準的網路安全協議。*美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）是提供網路安全框架（Cybersecurity Framework）（https://www.nist.gov/cyberframework）的組織之一，根據現有標準、指南和實踐提供自願性指導，以幫助管理和減少內外部的網路安全風險。其可用於幫助確定可降低網路安全風險的優先選項，也是協調政策、業務和技術方法以管理該風險的工具。本框架是對組織的風險管理流程和網路安全計劃的補充。目前尚未制定網路安全計劃的機構亦可參考該框架來進行制定。 *NIST 是美國商務部下屬的非監管聯邦機構，負責促進和維護測量標準，也是聯邦政府技術標準的開發者。	必須
4.2	為了保護 IT 系統免受常見的網路安全威脅，公司必須在成員的電腦系統中安裝足夠的軟體/硬體，以防止惡意軟體（病毒、間諜軟體、蠕蟲、特洛伊木馬等）和內部/外部入侵（防火牆）。成員必須確保其安全軟體是最新的，並定期進行安全更新。成員必須制定政策和程序以防止透過社交工程所發動的攻擊。如果發生數據洩漏或匿名攻擊事件導致數據		必須

編號	標準	實施指南	必須/應該
	和/或設備的損失，該程序必須包括恢復（或取代）IT 系統和/或數據的規定。		
4.3	使用網路系統的 CTPAT 成員必須定期測試其 IT 基礎建設的安全性。如果發現脆弱性，必須儘快採取糾正措施。	安全的電腦網路對企業至關重要，要確保受到保護，就需要定期進行測試。這可以透過定時脆弱性掃描來完成，就像保全人員檢查企業的門窗是否打開一樣。脆弱性掃描（vulnerability scan, VS）可以識別電腦上的漏洞（開放的端口和 IP 地址）、其操作系統和安裝在電腦上，駭客可用來進入公司 IT 系統的軟體。VS 將其掃描結果和脆弱性已知數據庫進行比對，並提出修正報告供企業採取行動。坊間有許多免費和商業版本的 VS 軟體。 測試的頻率將取決於各種因素，包括公司的商業模式和風險等級。例如，只要企業的網路基礎建設有所改變，便應該運行這些測試。但是，因為任何規模的企業所面臨的網路攻擊都在增加，因此設計測試計劃時須將之列入考慮。	必須
4.4	網路安全政策應解決成員如何與政府和其他商業夥伴共享有關網路安全威脅資訊的問題。	鼓勵成員與政府和供應鏈中的商業夥伴共享有關網路安全威脅的資訊。資訊共享是美國國土安全部使命的關鍵部分，目的是建立對惡意網路活動的態勢感知。CTPAT 成員可加入國家網路安全和通信整合中心（National Cybersecurity and Communications Integration Center, NCCIC）（https://www.us-cert.gov/nccic）。NCCIC 與公私營部門合作夥伴共享資訊，以建立對脆弱性、事件和緩解措施的意識。網路和工業控制系統使用者可免費訂閱資訊產品、提要和服務。	應該
4.5	必須建立一個系統來識別未經授權接入 IT 系統/數據或濫用政策和程序的情況，包括不當接入內部系統或外部網站以及員工或合同員工對業務數據的竄改或變更。所有違規者都必須受到適當的紀律處分。		必須
4.6	網路安全政策和程序必須根據風險或情況，每年進行一次或更頻繁的審查。審查之後，如有必要，必須更新政策和程序。	遭到網路攻擊就是政策不到一年就需更新的例子。利用從攻擊中得到的經驗教訓，將有助於加強成員的網路安全政策。	必須

編號	標準	實施指南	必須/應該
4.7	必須根據職務描述或所分配的職責來限制使用者接入權限。必須定期審查接入權限，以確保對敏感系統的接入是根據工作要求進行的。員工離職後，必須取消電腦和網路接入權限。		必須
4.8	有權接入 IT 系統的個人必須使用單獨分配的帳戶。 必須透過使用加強密碼、密碼短語或其他形式的身份認證來保護對 IT 系統的接入，使其免受滲透。必須保障 IT 系統使用者接入的安全。 如果有證據顯示密碼和/或密碼短語被竊或合理懷疑遭竊取，便必須儘快更改。	為了防止 IT 系統被滲透，必須通過認證過程來保護使用者接入。複雜的登入密碼或密碼短語、生物辨識技術和電子身份證是三種不同類型的身份認證過程。最好使用一種以上的程序。這些程序被稱為雙重認證（two-factor authentication, 2FA）或者多重認證（multi-factor authentication, MFA）。MFA 最為安全，因為它要求使用者在登入過程中提供兩個或更多證據（身分認證）以驗證其身份。 MFA 可以用來防止利用弱密碼或身份認證被竊而發生的網路入侵。MFA 可以要求個人使用其所擁有的，如隨機密碼產生器，或其物理特徵，即生物辨識特徵，來增強密碼或密碼短語（你所知道的），從而阻止這些攻擊向量。 如果使用密碼，則密碼必須很複雜。NIST 特別出版物 800-63B：數位身份指南（Digital Identity Guidelines），包括密碼指導（https://pages.nist.gov/800-63-3/sp800-63b.html），建議使用長且容易記住的密碼短語，而不要使用帶有特殊字符的單詞。這些較長的密碼短語（NIST 建議最多允許使用 64 個字符）由易於記住的句子或短語所組成，因此較難破解。	必須
4.9	允許使用者遠端接入到網路的成員必須使用安全技術，例如虛擬專用網（virtual private networks, VPN），讓員工得以在辦公室以外的地點可以安全接入公司的內部網路。成員還必須備有程序防止未經授權者進行遠端接入。	VPN 不是保護遠端接入網路的唯一選擇。MFA 也是一種方法。要求員工必須鍵入隨機密碼產生器的動態安全代碼之後才能接入網路，就是 MFA 的一個例子。	必須

編號	標準	實施指南	必須/應該
4.10	如果成員允許員工使用個人設備從事公司工作，則所有此類設備都必須遵守公司的網路安全政策和程序，包括定期的安全更新和安全接入公司網路的方法。	個人設備包括 CD、DVD 和隨身碟之類的存儲媒體，如果允許員工將其個人設備連接到其所使用的系統，則必須格外小心，因為這些數據存儲設備可能受到惡意軟體的感染，進而透過公司網路傳播。	必須
4.11	網路安全政策和程序應包括防止使用盜版或無正當許可的技術產品的措施。	電腦軟體是創建它的實體所擁有的智慧財產權（IP）。無論以何種方式取得軟體，未經製造商或出版商的明確許可而安裝軟體均屬違法。出版商總是通過授權給予許可，並明確軟體授權份數。未授權許可的軟體可能會因無法更新而無法發揮作用，且還更容易帶有惡意軟體，造成電腦及所存資訊變得無用。未經授權許可的軟體也不會獲得任何保證或支持，如果遇到問題，公司只能自己想辦法。使用未經授權許可的軟體也會引發法律後果，包括嚴厲的民事懲罰和刑事訴訟。軟體盜版導致合法授權軟體使用者的成本增加，並減少可用於研發新軟體的投資資本。 成員最好制定一項政策，要求所購買的新媒體必須保留產品密鑰標籤和真實性證書。CD，DVD 和隨身碟附有全息防偽標識，以確保其為真品，防止偽造。	應該
4.12	數據應每週或酌情備份一次。所有敏感和機密數據均應以加密格式存儲。	丟失數據對組織內部人員所產生的影響會有所不同，因此應該進行數據備份。建議每日進行備份以防生產或共享伺服器數據洩露/丟失。個別系統可能不需要那麼頻繁的備份，這取決於所涉及的資訊類型。 用於存儲備份的媒體最好存放在異地設施中。備份數據的設備與生產工作的設備不應使用同一網路。將數據備份到雲端可視為存放於“異地”設施。	應該
4.13	進行定期庫存清點時，必須包括所有存有進出口敏感信息的媒介、硬體或其他 IT 設備。報廢時，必須按照 NIST 媒體清除指南（Guidelines for Media Sanitization）或其他適當的行業指南對其進行適當的清除和/或銷毀。	某些類型的電腦媒體是硬碟驅動器、可移動驅動器、CD-ROM 或 CD-R 光碟、DVD 或隨身碟驅動器。 NIST 已制定政府數據媒體銷毀標準。成員可查閱該標準來清除和銷毀 IT 設備和媒體。 有關媒體清除（Media Sanitization），可查閱：	必須

編號	標準	實施指南	必須/應該
		https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	

第二個關注領域：運輸安全

5. <u>**交通運輸工具和國際運輸工具的安全**</u> – 走私經常涉及對交通運輸工具和國際運輸工具（IIT）的改裝，或將違禁品隱藏在 IIT 內。本標準涵蓋的安全措施旨在防範、偵測和/或阻止對 IIT 結構進行改變或暗藏於 IIT 的行爲，其可能導致未經授權的物資或人員有機可乘。

在裝櫃環節，必須制定程序檢查 ITT 並妥善加封。處於運送中或“靜待”狀態的貨物受到的控制較少，因此更容易遭滲透。也就是為什麼鉛封控制和追踪運送中的貨物/交通運輸工具的方法是關鍵安全標準。

供應鏈的破壞最常發生在運輸過程中。因此，成員必須保持警惕，確保在整個供應鏈中遵守這些關鍵的貨物標準。

關鍵詞定義：國際運輸工具（IIT）- IIT 包括國際貿易商品運輸中，到岸的（無論滿載或空載）、使用中的、將使用的貨櫃、平板櫃、集裝器（unit load devices, ULDs）、堆高機、貨物車、運輸罐、箱子、滑木箱、棧板、墊板、織物用芯子或其他特殊貨櫃。

編號	標準	實施指南	必須/應該
5.1	交通運輸工具和國際運輸工具（IIT）必須存放在安全的區域，以防止未經授權的進入，導致 IIT 結構改變，或者（如適用）封條/櫃門損毀。	對交通運輸工具和 IIT（無論空載或滿載）的安全存放對於防止未經授權的進入非常重要。	必須
5.2	CTPAT 的檢查流程必須具備安全和農業檢查的書面程序。	隨著涉及改裝交通運輸工具或 IIT 的走私日益猖獗，成員因此必須對其進行檢查，查找可見的有害生物和嚴重的結構問題。因為防範經由交通運輸工具和 IIT 所造成的有害生物污染也是至關重要的問題，因此在安全檢查過程中增加了農業的部分。 有害生物污染的定義是指可見的任何形式的動物、昆蟲或其他無脊椎動物（活的或死的、在生命週期的任何階段，包括卵鞘或卵筏），或源自任何動物的有機物質（包括血液、骨頭、毛髮、皮肉、分泌物、排泄物）；可繁殖或不可繁殖的	必須

編號	標準	實施指南	必須/應該
		植物或植物產品（包括水果、種子、葉子、枝、根、樹皮）；或其他有機材料，包括真菌；或土壤或水。其未包含在 IIT（例如貨櫃、集裝器等）的貨物清單中。	
5.3	CTPAT 成員必須確保進行下列有系統的 CTPAT 安全和農業檢查。這些檢查的規定將取決於供應鏈是陸路（加拿大或墨西哥）還是源自海外（海運和空運）而有所不同。在裝櫃之前，必須檢查所有空的 IIT，並且當交通運輸工具通過陸地邊界進入美國時，也必須對其進行檢查。 透過鐵路或多式聯運經海、空、陸路邊界（適用時）運輸的 CTPAT 貨物檢查要求： 必須對所有空貨櫃和集裝器（ULDs）進行七點檢查；並且必須對所有空的冷藏貨櫃和 ULD 進行八點檢查： 1. 前壁； 2. 左側； 3. 右側； 4. 地板； 5. 天花板/頂部； 6. 內門/外門，包括門鎖機關的可靠性； 7. 外部/底盤；以及 8. 冷藏貨櫃上的風扇罩。 通過陸路邊界公路交通運輸工具的附加檢查要求： 交通運輸工具/IIT 的檢查必須在交通運輸工具/IIT 存放場進行。 在可行的情況下，必須在進出存放場時和裝櫃點進行檢查。這些系統性檢查必須包括 17 點檢查：	對 IIT 和交通運輸工具進行安全和農業檢查，以確保其結構未被改裝來隱藏違禁品或受到可見的農業害蟲污染。 海外供應鏈裝櫃時需檢查所有的 IIT。但是，如果海□ /空運供應鏈風險較高，則可能需要更廣泛的檢查程序，包括對交通運輸工具和/或對海港碼頭或航空物流設施的檢查。通常，通過陸路過境點的貨物風險較高，因此交通運輸工具和 IIT 要經過多次檢查。 IIT 包括海運貨櫃、冷藏貨櫃/拖車、公路拖車、平板拖車、槽貨櫃、鐵路/悶罐車、漏斗式儲料罐和 ULD。 CTPAT 門戶網站的公共圖書館（Public Library Section）備有交通运输工具/IIT 安全和農業檢查的培訓材料。	必須

編號	標準	實施指南	必須/應該
	<u>拖拉機：</u> 1.保險槓/輪胎/輪轂； 2.門、工具箱和鎖定機關； 3.電箱箱； 4.空氣呼吸器； 5.油箱； 6.內部駕駛室/臥舖；以及 7.箱頂/車頂。 **<u>拖拽卡車：</u>** 1.第五輪區域-檢查自然隔間/防滑板； 2.外部-正面/側面； 3.後部-保險槓/門； 4.前壁； 5.左側； 6.右側； 7.地板； 8.天花板/頂棚； 9.內/外門和鎖定機關；以及 10.外部/底盤。		

編號	標準	實施指南	必須/應該
5.4	交通運輸工具和 IIT（視情況而定）必須配備外部硬件，以便合理地預防其遭拆除。在加裝任何鉛封裝置之前，必須全面檢查貨櫃的門、把手、桿、搭扣、鉚釘、托架和門鎖裝置的所有其他部件，是否有變造和任何硬件不匹配的情況。	考慮使用帶有防變造合頁的貨櫃/拖車。成員還可以在門的至少兩個合頁上放置保護板或銷軸，和/或在每一側的至少一個合頁上放置黏性膠/膠帶。	必須
5.5	所有交通運輸工具和空的 IIT 檢查均應記錄在檢查表上，其須包含下列各項： •貨櫃/拖車/IIT 編號； •檢查日期； •檢查時間； •進行檢查的員工姓名；以及 •所檢查的 IIT 具體位置。 如果檢查受到監督，主管還應在表上簽名。 完整的貨櫃/IIT 檢查清單應作為裝運單據包的一部分。收貨人應在收到商品之前收到完整的裝運單據包。		應該
5.6	所有安全檢查應在進出受到控制的區域內進行，如果有的話，應透過閉路電視系統監控。		應該

編號	標準	實施指南	必須/應該
5.7	如果在交通運輸工具/IIT 檢查中發現可見的有害生物污染，則必須進行清洗/吸塵。文件必須保留一年以證明符合這些檢查要求。	將所發現的污染物類型、發現地點（交通運輸工具上的發現點）以及消除方法記錄下來，有助於幫助成員防止未來再次發生。	必須
5.8	根據風險，管理人員應該在運輸工作人員完成交通運輸工具/IIT 檢查之後，對交通運輸工具進行隨機搜查。 應該定期進行交通運輸工具的搜查，並根據風險提高頻率。搜查應在沒有預警的情況下隨機進行，因此無法預測。檢查應在交通運輸工具環節薄弱的各個地點進行：承運商堆場、卡車裝載後以及前往美國邊境的途中。	對交通運輸工具進行監督搜查來防範發生內部陰謀的情況。 最好的做法是由主管將物品（例如玩具或彩盒）藏在交通運輸工具中，看看現場測試篩查員/交通運輸工具操作員是否會發現。 監督人員可以是對高層安全管理層負責的安全經理，也可指定其他管理人員。	應該
5.14	CTPAT 成員應與其運輸提供商合作，從起點到終點跟踪交通運輸工具。與服務提供商簽訂的服務協議應納入跟踪、報告和共享數據的具體要求。		應該
5.15	託運人應有權進入承運商的 GPS 車隊監控系統，以便跟踪其貨物的動向。		應該
5.16	陸路邊境運輸在靠近美國邊境時，對臨時停靠應採取“不停靠”政策。	貨物靜止就會有風險。預定的停靠不在本政策的範圍之內，但必須在整體跟踪和監視過程中加以考慮。	應該

編號	標準	實施指南	必須/應該
5.24	在高風險地區以及即將抵達邊境口岸前，CTPAT 成員應對運往美國的貨物採取“最後機會”核查程序，檢查交通運輸工具/IIT 是否有遭到變造的痕跡，包括對交通運輸工具的目視檢查和執行 VVTT 鉛封核查程序。該檢查應由受過適當培訓的人員來進行。 V – 查看鉛封和貨櫃的門鎖裝置，確保沒問題； V – 比對核實裝貨單據的鉛封號碼； T – 拉扯鉛封以確保妥善加封； T – 擰轉子彈封，確保各個部件不會鬆動、彼此分離或鉛封的部分有任何鬆動。		應該
5.29	如果發現任何對貨物或交通運輸工具安全性的可信（或檢測到的）威脅，成員必須（在可行的範圍內儘快）警告供應鏈中任何可能受到影響的商業夥伴，以及在適當的情況下，通知執法部門。		必須

6. **封條安全** – 拖車和貨櫃的加封，包括封條持續保持完整，乃為確保供應鏈安全的關鍵要素。封條安全包括制定全面的書面鉛封政策來處理封條安全的各個方面，根據 CTPAT 規定正確使用封條，正確加封 IIT，並核實妥善加封。

編號	標準	實施指南	必須/應該
6.1	CTPAT 成員都必須制定詳細的高保安鉛封書面流程，說明封條在設施中和運輸過程中的發放與管控。該流程必須提供封條被更動、變造、鉛封號碼有誤時，所應採取的步驟，包括對事件的記錄、通知合作夥伴的流程以及對事件的調查。調查結果必須加以記錄，並且儘快採取糾正措施。 這些書面程序必須保留在操作基層，以方便獲取。每年至少審核一次，必要時進行更新。 書面封條管控必須包含以下內容： **控制對封條的取得：** •封條的管理僅限於被授權人員。 •安全存放。 **庫存、分配和跟踪（封條記錄）：** •記錄收到的新封條。 •發放記錄過的封條。 •利用記錄追踪封條。 •只有經過培訓的授權的人員才能加封 IIT。 **控制運輸過程中的封條：** •提領被加封的 IIT 時（或停靠以後），要檢查封條是否完好無損，沒有變造的痕跡。 •確認鉛封號碼與裝運單據相符。 **運輸過程中拆封的情況：** •如果是因為檢查貨物而拆封，記錄所更換的鉛封號碼。 •司機必須立即通知調度員拆封的情況，說明何為拆封人，並提供新的		必須

編號	標準	實施指南	必須/應該
	鉛封號碼。 •承運商必須立即通知託運人、代理人和進口商鉛封變更事宜並提供新鉛封號碼。 •託運人必須立即記錄新的鉛封號碼。 **封條異樣：** •保存被更動或變造的封條，以協助調查。 •調查異樣；之後採取糾正措施（如有必要）。 •在適用的情況下，向 CBP 和相關外國政府報告鉛封遭破壞的情況，以協助調查。		
6.2	所有可加封的 CTPAT 貨物在裝櫃/包裝之後，必須立即由責任方（即託運人或替其工作的包裝商）用符合或超出國際標準化組織（International Organization for Standardization, ISO）17712 最新標準的高保安封條進行加封。合格的鋼纜封和子彈封均可接受。所有的封條都必須牢固並妥善加封在運送 CTPAT 成員貨物至/自美國的 IIT 上。	如果有安全凸輪的話，所使用的高保安封條必須裝在凸輪的位置而不是右側門的把手上。鉛封必須放在貨櫃右側門最中間的垂直桿的底部。如果沒有安全凸輪的話，也可以把鉛封放在貨櫃右側門最中間的左側把手鎖件上。如果使用的是子彈封，建議將鉛封的螺栓部分或插入件朝上，使得螺栓部分在搭扣上方。	必須
6.5	CTPAT 成員（有封條庫存者）必須記錄所使用的高保安封條符合或超過當前最新的 ISO 17712 標準。	檢測實驗室所出具符合 ISO 高保安封條標準的證書是可接受的合格證據。CTPAT 成員應當了解其所購買的鉛封如何顯示遭外力毀損。	必須
6.6	有封條庫存的 CTPAT 成員，其公司管理層或安全主管必須進行封條稽查，包括定期清點庫存封條，將封條庫存記錄和裝運單據相互比對。所有稽查都必須有所記錄。 作為整體鉛封審核流程的一部分，碼頭主管和/或倉庫經理必須定期核查交通運輸工具和 IIT 上的鉛封號碼。		必須

編號	標準	實施指南	必須/應該
6.7	必須遵守 CTPAT 的鉛封核查程序以確保所有高保安封條（子彈封/鋼纜封）妥善安裝在 IIT 上，並按設計發揮作用。該流程被稱為 VVTT 流程： V – 查看鉛封和貨櫃的門鎖裝置，確保沒問題； V – 比對核實裝貨單據的鉛封號碼； T – 拉扯鉛封以確保妥善加封； T – 擰轉子彈封，確保各個部件不會鬆動、彼此分離或鉛封的部分有任何鬆動。	使用鋼纜封時，要將其纏繞包住垂直桿的矩形硬件底座，以防止鉛封上下移動。裝上鉛封之後，要將鋼纜兩頭多餘的部分去掉。VVTT 流程對鋼纜封的要求是要確保拉緊鋼纜。鉛封放置好後，拉扯鋼纜以確定鎖體內的鋼纜不會滑脫。	必須

7. <u>程序安全 –</u> 程序安全包括進出口流程、文件記錄以及貨物儲存處理要求等許多方面。其他重要的程序標準涉及報告事件和通知相關執法部門。另外，CTPAT 往往要求制定書面程序，因其有助於程序長期保持一致。但是，書面程序所需細節多寡取決於各種因素，例如公司的商業模式或程序所涵蓋的內容。

CTPAT 認識到供應鏈所使用的技術日新月異。標準中所提及的術語如書面程序、文件和表格，不意味全是紙質版。電子文本、簽名和其他數位技術都可滿足這些要求。

本計劃並非是個“一刀切”模式。各公司必須（根據其風險評估）自行決定如何實施和維護各種程序。但是，更為有效的是將安全流程納入到現有程序中，而不是另外制定一份安全程序手冊。如此一來，創建的架構會更有持續性，並有助於強調供應鏈安全是每個人的責任。

編號	標準	實施指南	必須/應該
7.1	如果貨物將整夜或長期暫存，必須採取措施防止未經授權的人接近。		必須
7.2	必須定期檢查貨物準備區和周邊區域，以確保不受可見的有害生物污染。	必要時，可以使用誘餌、誘捕器或其他障礙物等預防措施。清除雜草或減少植物叢生有助於防範有害生物在貨物準備區的滋生。	必須
7.4	貨物裝櫃至貨櫃/IIT 時，應由安全官員/經理或其他指定人員進行監督。		應該
7.5	作為正確安裝鉛封有據可查的證據，應在裝櫃點拍照。在可行的範圍內，應將這些圖像以電子方式轉發到目的地，以進行核實。	相片證據可以包括在裝櫃點拍攝的照片，以記錄貨物標記、裝載過程、鉛封放置的位置以及正確安裝的鉛封。	應該
7.6	必須實施程序來確保商品/貨物清關所需的資料清晰、完整、準確，避免資料傳遞有誤、丟失或引用錯誤；並按時報告。		必須
7.7	如果使用紙質文件，表格和其他進出口相關文件都應該受到保護，以防止被未經授權使用。	使用上鎖的文件櫃等措施可以防範未經授權使用包括貨單在內的空白表格。	應該

編號	標準	實施指南	必須/應該
7.8	託運人或其代理人必須確保提單（bill of ladings, BOLs）和/或艙單準確反映提供給承運商的資料，承運商則必須進行盡職調查確保文件準確無誤。BOL 和艙單必須及時提交 CBP。所提交的提單必須顯示承運商取得運往美國貨物的外國起始地點/設施。重量和件數都必須準確。	承運商提取加封的 IIT 時，可依賴託運人託運說明中的資料。 要求將鉛封號碼電子列印在 BOL 或其他出口文件上有助於防止鉛封被更換以及造假相關文件來配合新的鉛封號碼。 但是，某些供應鏈的貨物在運輸過程中會受到外國海關或者 CBP 的檢查。IIT 被政府拆封檢查後，必須重新記錄新的鉛封號碼。在某些情況下，可以手寫。	必須
7.23	CTPAT 成員必須制定報告事件的書面程序，包括說明設施內部提高事件處理層級的流程。 制定通知程序來報告發生在世界各地且會影響成員供應鏈安全的任何可疑活動或安全事件（如截獲毒品、發現偷渡客等）。發生任何全球性事件時，在適用的情況下，成員必須告知供應鏈安全專家、最近的出入境口岸、相關執法部門以及受影響供應鏈中的商業夥伴。必須在交通運輸工具或 IIT 跨越邊界前，儘可能快地通知 CBP。 通知程序必須包括正確的聯絡資訊，列出所需要通知的人員和執法部門的姓名與電話號碼。程序必須定期审查，以確保聯絡資訊正確無誤。	必須通知 CBP 的例子包括（但不限於）： •發現對貨櫃/IIT 或高安全性封條遭到毀損； • 在交通運輸工具或 IIT 中發現隱藏隔間； • 在 IIT 上使用未登記的新鉛封； • 走私違禁品，包括人員、偷渡客； •未經授權進入交通運輸工具、火車、船隻或航空母艦； •勒索、索取保護費、威脅和/或恐嚇； • 未經授權使用商業實體識別（例如進口商備案（Importer of Record, IOR）編號、承運商標準數字編碼（Standard Carrier Alpha code, SCAC）等）。	必須
7.24	必須制定程序用於識別、問訊和處理未經授權/身份不明的人員。工作人員必須了解如何質問不明/未經授權人員、如何應對情況，並熟悉將未經授權人員遣離該地點的流程。		必須
7.25	CTPAT 成員應建立可匿名舉報與安全相關問題的機制。收到指控後，進行調查。如適用，應採取糾正措施。	如果可以匿名舉報，諸如盜竊、詐欺和內部陰謀等問題會更易於被舉發。 成員可設立熱線或類似機制，讓擔心遭到報復的人匿名舉報。建議保留所有舉報報告，用以證明已進行調查並予以糾正。	應該

編號	標準	實施指南	必須/應該
7.27	任何短缺、超額或其他重大差異或異常都必須進行適當的調查並加以解決。		必須
7.28	到岸貨物應與貨物艙單上的資料一致。離港貨物應與採購訂單或交貨單進行核對。		應該
7.29	貨物具體鉛封號碼應在出發前發送給收貨人。		應該
7.30	鉛封號碼應以電子方式列印在提單或其他裝運單據上。		應該
7.37	一旦發生重大安全事件，成員們在得知後，必須立即啟動事件後分析，以便決定供應鏈可能遭到破壞的環節為何。該分析不得妨礙/干擾政府執法機構所進行的任何已知調查。公司的事件後分析結果必須做記錄，儘可能迅速完成。如執法機關允許，當供應鏈安全專家（SCSS）提出請求時，向其提供。	安全事件是指經由規避、躲避或違反安全措施的入侵，其已造成或將導致犯罪行為。安全事件包括恐怖主義行為、走私（毒品、人口等）以及出現偷渡客。	必須

8. **農業安全 –** 農業是美國最大的產業和就業部門，同時也是受到外來動植物污染威脅的產業，包括土壤、有機肥、種子以及可能帶有入侵性和破壞性病害蟲的動植物材料。消除各類交通運輸工具和貨物中的污染物可減少 CBP 將貨物暫時扣押、延遲和商品退回或處理。確保遵守 CTPAT 的農業要求有助於保護美國的關鍵產業以及全球食物供應鏈。

關鍵詞定義：有害生物污染 - 國際海事組織將有害生物污染定義為可見的任何形式的動物、昆蟲或其他無脊椎動物（活的或死的、在生命週期的任何階段，包括卵鞘或卵筏），或源自任何動物的有機物質（包括血液、骨頭、毛髮、皮肉、分泌物、排泄物）；可繁殖或不可繁殖的植物或植物產品（包括水果、種子、葉子、枝、根、樹皮）；或其他有機材料，包括真菌；或土壤或水。其未包含在 IIT（例如貨櫃、集裝器等）的貨物清單中。

編號	標準	實施指南	必須/應該
8.1	CTPAT 成員必須根據其商業模式制定書面程序，防止可見的有害生物污染，包括遵守木質包裝材料（Wood Packaging Materials, WPM）法規。在整個供應鏈中，必須採取可見的有害生物防治措施。有關木質包裝材料法規的措施必須符合《國際植物保護公約》（International Plant Protection Convention, IPPC）的《國際植物檢疫措施標準第 15 號》（International Standards for Phytosanitary Measures No. 15, ISPM 15）。	木質包裝材料（WPM）的定義是用於支撐、保護或運送商品而使用的木頭或木製品（不包括紙製品）。WPM 如托盤、板條箱、盒子、捲軸和墊艙物料等，很多時候可能都是以未經充分加工或處理清除或消滅有害生物的木材原料所製成的，因此成為有害生物輸入和傳播途徑。墊艙物料尤其具有輸入和傳播有害生物的高風險。 IPPC 是聯合國糧食及農業組織（United National's Food and Agriculture Organization）所監督的多邊條約，旨在確保採取協調一致的有效行動，防治並控制有害生物和污染物的輸入和傳播。 ISPM 15 包括國際認可的措施，適用於 WPM，以大幅降低可能大部分與其有關的有害生物輸入和傳播風險。ISPM 15 影響所有 WPM，要求剝皮之後，經過熱處理或溴化甲烷燻蒸，再加蓋或烙印 IPPC 合格標記，其俗稱為『小麥印章』。不受 ISPM 15 管制的產品都是用其他材料製成的，如紙類、金屬、塑膠或木板產品（如定向刨花板、硬質纖維板和三夾板）。	必須

第三個關注領域：人員與場地實體安全

9. **場地實體安全** – 貨物裝卸和儲存設施，IIT 存放區以及國內外準備進出口文件的設施必須設有實體屏障和嚇阻設備，以防範未經授權者進入。

CTPAT 的基石之一是其靈活性，因此安全計劃應根據公司情況來制定。場地實體安全的需求差異大大取決於成員在供應鏈中的角色、商業模式以及風險等級。場地實體安全標準提供多個嚇阻/障礙手段，避免未經授權接近貨物、敏感設備和/或資料。成員應在整個供應鏈中採取這些安全措施。

編號	標準	實施指南	必須/應該
9.1	所有貨物裝卸/和儲存設施，包括托車場和辦公室，都必須設有實體屏障和/或嚇阻設施，以防範未經授權者進入。		必須
9.2	貨物裝卸和儲存設施周邊應以圍欄圍住。裝卸貨物的設施應設置內部圍欄，以保證貨物和貨物裝卸區的安全。根據風險情況，還應加裝內部圍欄以分隔不同類型的貨物，如國內、國際、高價值和/或危險材料。圍欄的完整和損壞情況應由指定人員定期檢查。圍欄如有損壞，應儘快修復。	除了圍欄以外，也可使用其他可接受的屏障，如分隔牆、無法穿越的或會造成阻礙的自然屏障，如陡峭的懸崖或茂密的樹叢等。	應該
9.4	車輛和/或人員出入的大門（以及其他出口點）必須有人值守或監控。可以根據當地法律和勞工法對個人與車輛進行搜查。	建議將大門設置的數量為最低必要，兼顧適當通行和確保安全。其他出口點爲未設閘門的設施入口。	必須
9.5	應禁止私人車輛停放在貨物裝卸和儲存區或緊鄰區域，也不得停放在交通運輸工具旁。	停車場應設於圍欄外和/或操作區外，或者至少要與貨物裝卸和儲存區保持相當的距離。	應該
9.6	設施內外部必須提供足夠的照明，如適用，包括以下區域：出入口、貨物裝卸和儲存區、圍欄沿線和停車場。	在照明設備中加裝自動定時器或光感測器啟動適當安全照明，會更加有效。	必須

編號	標準	實施指南	必須/應該
9.7	應利用保全技术監視設施，以防止未經授權進入敏感區域。	用來保護/監控敏感區域和出入口的電子保全技术包括：防盜警報系統（周邊和內部），也被稱為入侵偵測系統（Intrusion Detection Systems, IDS）；門禁控制裝置；以及視訊監控系統（video surveillance systems, VSS），包括閉路電視攝影機（Closed Circuit Television Cameras, CCTVs）。CCTV/VSS 系統可以包括類比攝影機（基於同軸電纜）、IP 網路攝影機（基於網路）、錄影裝置和視訊管理軟體。 視訊監控可保護的安全/敏感區域包括：貨物裝卸和儲存區、保存進口文件的發貨/收貨區、IT 伺服器、IIT 存放區、IIT 檢查區以及封條存放區。	應該
9.8	依靠保全技术保護人身安全的成員必須制定書面政策和程序來管理對技術的使用、維護和保護。 這些政策和程序至少必須規定： •只有得到授權的人員才能進入技術控制和管理地點； •已定期實施測試/檢查技術的程序； •檢查應包括核實所有設備運作正常，如適用，並核實設備放置正確； •檢查和性能測試的結果應加以記錄； •如需進行糾正，應儘快實施，並將糾正措施加以記錄； •檢查記錄應保存足夠的時間，以便稽核。 如使用第三方中央監控站（異地），CTPAT 成員必須備有書面程序，規定關鍵的系統功能和驗證序程，例如（但不限於）安全代碼更改、增減授權人員、密碼修改、以及進入系	保全技术需定期測試以確保正常運作。可遵循的一般指針如下： •維修後、對建築物或設施進行大修、改造或增建期間和之後，需檢測安全系統。系統組件可能被有意或無意間受到損壞。 •電話或網路服務發生任何重大更改後，需檢測安全系統。任何可能對系統與監控中心溝通產生影響的部分，都必須重複檢查。 •確保視訊設置正確，如動作感應錄影、動作偵測警報、每秒圖像幀數（image per second, IPS）和畫質等。 •確保鏡頭（或保護攝影機的球型罩）的清潔，準確對焦。不可被障礙物或強光限制其可見性。 •確保保全攝影機放置正確，並保持在正確的位置（攝影機可能被有意或無意遭移動）。	必須

編號	標準	實施指南	必須/應該
	統或遭到拒絕。 保全技术政策和程序必須每年審查並更新。根據風險情況，可增加頻率。		
9.9	CTPAT 成員在設計和安裝保全技术時，應使用有授權許可/經認證的資源。	當今的保全技术非常複雜，且日新月異。公司往往採購錯誤，以至於在需要的時候無法發揮作用和/或付出不必要的高昂費用。尋求合格的指導有助於買方根據需求和預算選擇適合的技術。 根據美國國家電氣承包商協會（National Electrical Contractors Association, NECA），全美目前有 33 個州規定保全和警報系統安裝人員必須持有專業執照。	應該
9.10	必須對所有保全技术基礎建設進行實體保護，以防止未經授權進入。	保全技术基礎建設包括電腦、保全軟體、電子控制面板、錄影監控或閉路電視攝影機、攝影機和錄影所需的電源和硬體。	必須
9.11	保全技术系統應配置備用電源，以確保突然失去直接電源時，系統仍能繼續運行。	企圖闖入的犯罪分子可能會試圖切斷保全技术的電源，以便避開監控。因此，保全技术配置替代電源是至關重要的。替代電源可以是輔助發電來源或備用電池。備用發電機也可用於照明等其他關鍵系統。	應該
9.12	如使用攝影機系統，攝影機應監控設施場地和敏感區域，以阻止未經授權的進入。如發生未經授權進入敏感區的情況，應利用警報系統通知公司。	如適用，敏感區域可包括貨物裝卸和儲存區、保存進口文件的發貨/收貨區、IT 伺服器、IIT 存放區、IIT 檢查區和封條存放區。	應該
9.13	如安裝攝影機系統，確保攝影機的位置能覆蓋設施中與進出口流程有關的關鍵區域。 攝影機畫質應設在最清晰的設定，並設置為全天候錄影。	正確放置攝影機是至關重要的，以便在設施的控制範圍內，儘可能對實體“監管鏈”進行錄影。 根據風險，關鍵區域或流程可包括貨物裝卸和儲存區、發貨/收貨區、貨物裝載流程、鉛封流程、交通運輸工具的進出、IT 伺服器、貨櫃檢查區（安全和農業檢查）、封條存放區以及任何與確保國際貨運安全有關的其他領域。	必須

編號	標準	實施指南	必須/應該
9.14	如使用攝影機系統，其應具備警告/通知功能，可以發出“操作/記錄失敗”的信號。	錄影監控系統的故障有可能是人為的，其為了避免留下闖入供應鏈的證據，從而使系統失靈。操作失敗信號功能會傳送電子通知，告知預先指定人員設備需要立即進行檢查。	應該

編號	標準	實施指南	必須/應該
9.15	如使用攝影機系統，必須（由管理層、安全或其他指定人員）對錄影片段進行定期、隨機檢查，以核查是否依法正確執行貨物安全程序。審查結果必須予以書面總結，包括所採取的任何糾正措施，並保存足夠的時間，以便進行稽查。	如果檢查錄影片段只是為了找尋原因（作為安全事件調查的一部分），則無法充分發揮安裝攝影機的好處。攝影機不僅僅只是調查工具，如能善加利用，可防範於未然。 錄影片段的隨機檢查應針對實體監管鏈，以確保貨物安全並遵守所有的安全規程。可進行檢查的流程如下： •貨物裝卸活動； •貨櫃檢查； •裝載流程； •鉛封流程； •交通運輸工具的進出；以及 •貨物運離等。 **審查目的：**審查是為了評估全面遵守安全流程的情況以及是否有效。找出落差或弱點並加以糾正，以期改進安全流程。成員可根據風險（既往事件或有關員工未遵守裝卸區安全流程的匿名舉報等），定期進行審查。 **書面總結中應包括的項目：** •審查日期； •審查錄影片段的日期； •來自哪個攝影機/區域； •簡要說明情況；以及 •如有必要，所採取的糾正措施。	必須
9.16	如使用攝影機，用來監視貨物的關鍵進出口流程錄影片段應保存足夠的時間，以完成調查。	如果發生安全事件，便需要進行調查。因此，妥善保存監控包裝（用於出口）和裝載/鉛封流程的錄影片段極為重要，才能調查供應鏈受到破壞的環節。 為了進行監控，CTPAT 建議，從貨物抵達分銷第一站算起，至少再將錄影片段保存 14 天。這是清關後，貨櫃首次被打開。	應該

10. **<u>場地實體門禁管制</u>** – 門禁管制可防止未經授權者進入設施/區域，有助於管理員工和訪客，並保護公司資產。門禁管制包括在各個入口核實所有員工、訪客、服務提供商和廠商的身份。

編號	標準	實施指南	必須/應該
10.1	CTPAT 成員必須有發放、變更和取消識別證和門禁卡的書面程序。 在適用的情況下，必須建立員工識別系統以核實身份和管制進出。敏感區域的進出權限取決於工作描述或指定職責。員工離職時，必須取消其門禁卡。	門禁卡包括員工識別證、訪客和廠商臨時識別證、生物辨識系統、感應鑰匙卡、代碼和鑰匙。員工離職時，使用離職清單確保返還和/或取消所有門禁卡。小公司員工相互認識，因此無須使用識別系統。一般而言，公司員工人數超過 50 名，便需要使用識別系統。	必須

編號	標準	實施指南	必須/應該
10.2	訪客、廠商和服務提供商必須在到達時出示帶照片的身份證件，並登記拜訪細節。所有來訪者均應有人陪同。另外，應向所有訪客和服務提供商發放臨時識別證。如使用臨時識別證，必須全程配戴。 訪客日誌必須包括以下內容： •到訪日期； •訪客姓名； •驗證帶照片的身份證件（驗證類型如駕照或國民身份證）。熟悉的訪客，如固定廠商，可不用核實有照證件，但仍必須經過登記才能進出設施； •到達時間; •公司聯絡人；以及 •離開時間。		必須
10.3	在接收或放行貨物之前，必須核實收送貨物的司機身份。其必須向有權允許進入設施的員工出示政府所頒發帶有照片的身份證件，以驗證其身份。如果出示該類證件不可行，設施員工則可以接受其雇主公路承運公司所發放、可識別的有照證件。		必須

編號	標準	實施指南	必須/應該
10.4	必須備有提貨物日誌以登記司機，並詳細記錄其提貨時的交通運輸工具。司機抵達設施提貨時，設施員工必須將其登入在提貨日誌中。司機離開時，必須登出。日誌必須妥善保管，司機不得接近。 提貨日誌應包括下列各項： •司機姓名； •到達日期和時間； •雇主； •卡車號碼； •拖車號碼； •離開時間； •離開時貨物上的鉛封號碼。	訪客日誌也可作為提貨日誌，只要記錄額外資料即可。	必須
10.7	到達之前，承運商應通知設施提貨預計到達時間、司機姓名和卡車號碼。在可操作的情況下，CTPAT 成員應當只接受提前預約的交貨與提貨。	該標準有助於託運人和承運商避免假冒提貨。假冒提貨是透過欺騙盜取貨物的犯罪陰謀，包括卡車司機使用假證件和/或成立假公司以便盜取貨物。 如果承運商有固定的司機從某個設施提貨時，最好的做法是由設施保存一份帶有照片的司機名單。如此一來，即使無法事先得知提貨司機，仍可確認其為核准至該設施提貨的司機。	應該
10.8	應定期篩查收到的包裹和郵件，以防夾帶违禁品。	違禁品包括但不限於爆炸物、非法毒品和貨幣。	應該
10.10	如雇用保全人員，書面政策和程序必須包含其工作指示。管理層必須透過稽查和政策審查定期核查遵守和適用情況。	儘管任何設施皆可派駐保全人员，但派駐地點通常為製造設施、海港、配送中心、IIT 存放場、拼裝業主和貨運代理人的作業場所。	必須

11. <u>人員安全</u> – 公司的人力資源是其最關鍵的資產之一，但也可能是最薄弱的安全環節之一。本標準側重於員工篩选和職前核查等問題。許多安全違規都是內部陰謀所造成的，也就是一名或多名員工合謀規避安全程序來滲透供應鏈。因此，成員必須進行盡職調查，以確保敏感職位上的員工可靠並值得信賴。敏感職位包括直接處理貨物或其文件的人員以及控制進入敏感區域或設備的人員。此類職位包括但不限於發貨、收貨、郵件收發室、司機、調度員、保全人员、任何參與裝載貨物、交通運輸工具追踪和/或鉛封控制的人員。

編號	標準	實施指南	必須/應該
11.1	必須制定書面程序篩查應聘員工並定期核查現任員工。聘用前，在法律允許的範圍內，必須儘可能地核實其就業經歷和進行資歷查核。	CTPAT 了解某些國家的勞工法和隱私法可能不允許核實所有的應聘訊息。但在允許的範圍內，應盡職調查，對其進行核查。	必須
11.2	根據適用的法律限制以及可用的犯罪記錄數據庫，進行員工背景調查。根據職位的敏感性，員工審查要求應擴展包括臨時和合同員工。僱用後，應根據原因和/或員工職位的敏感性定期進行重新調查。 員工背景調查應透過市、州、省和全國的數據庫進行包括身份和犯罪記錄的核查。CTPAT 成員及其商業夥伴決定是否聘用時，在當地法規允許的範圍內，應考慮背景調查的結果。背景調查不限於核實身份和犯罪記錄。在風險較高的領域，可能需要更深入的調查。		應該
11.5	CTPAT 成員必須制定員工行為準則，其包括對員工的期望和定義可接受的行為。該行為準則必須包括懲罰和紀律處分程序。員工/合同員工必須簽名確認已閱讀並理解。該文件必須作為記錄保存在員工的檔案中。	制定行為準則有助於保護公司，並告知員工公司的期望。其旨在於制定並維護公司可接受的行為標準，助其樹立專業形象並建立強大的道德文化。即使是小公司也需要制定行為準則，但其設計或所包含的訊息不需複雜。	必須

12. **<u>教育、培訓和安全意識</u>** - CTPAT 安全標準設計來作為分層安全系統的基礎。如果其中一層受到影響，則另一層應防止安全受到破壞或向公司發出警告。執行和維護分層安全計劃需要多個部門和人員的積極參與和支持。培訓是維護安全計劃的關鍵之一。教育員工何為威脅以及為何其在公司供應鏈的保護中扮演重要角色，才能確保供應鏈安全計劃的成功與持久。而且，當員工對為何實施安全程序的原因有所了解之後，更有可能切實遵守。

編號	標準	實施指南	必須/應該
12.1	成員必須建立和維持安全培訓和安全意識計劃，以識別並增強對供應鏈中每個點的設施、交通運輸工具和貨物的安全漏洞的認識。這些漏洞可能被恐怖分子或違禁品走私者利用。培訓計劃必須全面，而且涵蓋 CTPAT 的所有安全規定。在敏感職位的人員必須接受針對該職位所承擔職責的附加專門培訓。 培訓是安全計劃的關鍵之一。員工了解為何採取安全措施，就更可能對其切實遵守。安全培訓必須根據員工的職能和職位，按規定定期舉辦。該培訓應作為新進員工入職培訓/職業技能培訓的一部分。 成員必須保存培訓證據，例如培訓記錄、簽到單（名冊）或電子培訓記錄。培訓記錄應包括培訓日期、參加培訓人員姓名和培訓主題。	培訓主題可以包括保護門禁管制、識別內部陰謀，以及報告可疑活動和安全事件的程序。如果可能，專門培訓應包括現場演示。如果進行現場演示，教員應留出時間讓學生演示該流程。 對於 CTPAT 而言，敏感職位包括直接處理進出口貨物或其文件的人員，以及控制進入敏感區域或設備的人員。這些職位包括但不限於發貨、收貨、郵件收發室、司機、調度員、保全人員、任何參與裝載貨物、交通運輸工具追踪和/或鉛封控制的人員。	必須

編號	標準	實施指南	必須/應該
12.2	負責對空的交通運輸工具和 IIT 進行安全和農業檢查的司機和其他人員必須接受培訓，以便對其交通運輸工具/ IIT 進行安全和農業檢查。 溫故培訓必須定期舉辦。發生事件或安全漏洞之後如有需要或者公司程序有所變更時，也應舉辦。 檢查培訓必須包括以下主題： •隱藏隔間的跡象； •隱蔽在天然隔間中的違禁品；以及 •有害生物污染的跡象。		必須
12.4	CTPAT 成員應制定措施，核實所提供的培訓符合其所有目標。	了解培訓並能在其崗位上（對敏感職位的員工而言）學以致用，是至關重要的。成員可以採用考試或測驗、模擬演習/演練或定期審查等方法來確定培訓效果。	應該
12.8	在適用的情況下，必須根據人員的職責和/或職位進行有關公司網路安全政策和程序的培訓，包括保護其密碼/密碼短語和電腦接入權限。	高品質的培訓是降低容易受到網路攻擊的關鍵。完善的網路安全培訓計劃通常是在正式的環境中訓練相關人員，而不是單單透過電子郵件或備忘錄來進行。	必須
12.9	操作和管理安全技术系統的人員必須接受各自領域的操作和維護培訓。可接受先前類似系統的工作經驗。透過操作手冊和其他方法所進行的自我培訓也是可接受的。		必須
12.10	員工必須接受如何報告安全事件和可疑活動的培訓。	報告安全事件或可疑活動的程序是安全計劃中極其重要的部分。有關如何報告事件的培訓可以包括在整體培訓之中。利用專門的培訓單元（根據工作職責），可進行對報告程序更詳細的培訓，包括流程的具體細節，例如報告內容、報告對象、如何報告事件以及報告完成以後的後續工作。	必須

發行號碼：1079-0420