Tiêu chí Bảo mật Tối thiểu - Nhà sản xuất Nước ngoài

Tháng 1-2020

Lưu ý: Số tiêu chí có thể không theo thứ tự. Số ID không được liệt kê không áp dụng đối với Nhà sản xuất Nước ngoài.

Lĩnh vực Trọng tâm Đầu tiên: An ninh Doanh nghiệp

1. **Tầm nhìn và Trách nhiệm Bảo mật** – Để chương trình bảo mật chuỗi cung ứng của Thành viên CTPAT có hiệu quả và duy trì hiệu quả, cần phải có sự hỗ trợ của quản lý cấp trên của công ty. Xây dựng bảo mật thành một phần không thể thiếu trong văn hóa của công ty và đảm bảo đó là một ưu tiên của toàn công ty chủ yếu là trách nhiệm của lãnh đạo công ty.

ID	Tiêu chí	Hướng dẫn Thực hiện	Phải / Nên
1.1	Để thúc đẩy văn hóa bảo mật, các Thành viên CTPAT cần thể hiện cam kết của mình đối với bảo mật chuỗi cung ứng và với Chương trình CTPAT thông qua một tuyên bố hậu thuẫn. Tuyên bố nên được một quan chức cấp cao của công ty ký và được trưng bày ở các địa điểm thích hợp trong công ty.	Tuyên bố hậu thuẫn cần nhấn mạnh tầm quan trọng của việc bảo vệ chuỗi cung ứng tránh các hoạt động tội phạm như buôn bán ma túy, khủng bố, buôn người và buôn lậu trái phép. Các quan chức cấp cao của công ty là người hậu thuẫn và ký tên vào bản tuyên bố có thể bao gồm chủ tịch, tổng giám đốc điều hành, tổng quản đốc, hoặc giám đốc an ninh. Các nơi trưng bày tuyên bố hậu thuẫn bao gồm trang web của công ty, trên các áp phích tại các khu vực chính của công ty (quầy tiếp tân; đóng hàng; kho hàng, v.v.) và/hoặc là một phần trong các hội thảo bảo mật của công ty, v.v.	Nên
1.2	Để xây dựng Chương trình Bảo mật Chuỗi Cung ứng mạnh mẽ, công ty nên kết nối các đại diện từ tất cả các bộ phận liên quan vào một nhóm đa chức năng. Các biện pháp bảo mật mới này cần được đưa vào các quy trình hiện có của công ty nhằm tạo ra một cấu trúc bền vững hơn và	Bảo mật Chuỗi Cung ứng có phạm vi lớn hơn nhiều so với các chương trình bảo mật truyền thống. Nó đan xen với việc bảo mật trong nhiều bộ phận như Nhân sự, Công nghệ thông tin, và các văn phòng Xuất/Nhập khẩu. Các chương trình Bảo mật Chuỗi Cung ứng, vốn được xây dựng theo mô hình có tính truyền thống hơn và dựa vào bảo mật theo phòng ban, có thể ít khả thi hơn về lâu về dài vì	Nên

ID	Tiêu chí	Hướng dẫn Thực hiện	Phải / Nên
	để nhấn mạnh rằng bảo mật chuỗi cung ứng là trách nhiệm của mọi người.	trách nhiệm thực hiện các biện pháp bảo mật tập trung ít nhân viên hơn và do đó, có thể dễ bị ảnh hưởng do mất nhân sự chủ chốt.	
1.3	Chương trình bảo mật chuỗi cung ứng phải được thiết kế, hỗ trợ và thực hiện qua một phần đánh giá bằng văn bản phù hợp. Mục đích của phần đánh giá này là ghi nhận việc có sẵn một hệ thống, trong đó nhân viên chịu trách nhiệm đối với các nhiệm vụ của họ và tất cả các quy trình bảo mật vạch ra trong chương trình bảo mật đang được thực hiện như thiết kế. Kế hoạch đánh giá phải được cập nhật khi cần dựa trên những thay đổi thích hợp trong hoạt động và mức độ rủi ro của tổ chức.	Mục đích của việc đánh giá nhằm phục vụ cho các mục đích CTPAT nhằm đảm bảo rằng nhân viên tuân thủ các quy trình bảo mật của công ty. Quy trình đánh giá không cần phải phức tạp. Thành viên quyết định phạm vi đánh giá và mức độ chuyên sâu dựa trên vai trò của mình trong chuỗi cung ứng, mô hình kinh doanh, mức độ rủi ro và sự khác biệt giữa các địa điểm/mặt bằng cụ thể. Các công ty nhỏ có thể xây dựng một phương pháp đánh giá rất đơn giản; ngược lại, một tập đoàn lớn, đa quốc gia có thể cần một quy trình bao quát hơn và có thể cần xem xét các yếu tố khác nhau như yêu cầu pháp lý địa phương, v.v. Một số công ty lớn có thể đã có một đội ngũ kiểm toán viên có thể được tận dụng để giúp đánh giá bảo mật. Thành viên có thể quyết định sử dụng các đánh giá nhắm mục tiêu nhỏ hơn hướng vào các thủ tục cụ thể. Các lĩnh vực chuyên biệt, chủ chốt trong bảo mật chuỗi cung ứng như kiểm tra và kiểm soát niêm phong có thể trải qua các đánh giá cụ thể cho các lĩnh vực đó. Tuy nhiên, việc tiến hành đánh giá tổng thể định kỳ để đảm bảo rằng tất cả các lĩnh vực của chương trình bảo mật đang hoạt động như thiết kế là điều rất hữu ích. Nếu một thành viên đã tiến hành đánh giá như một phần của đánh giá hàng năm, quá trình đó có thể đã đủ để đáp ứng tiêu chí này. Đối với các thành viên có chuỗi cung ứng có rủi ro cao (được xác định bằng đánh giá rủi ro), các diễn tập mô phỏng hoặc giả lập có thể được đưa vào chương trình đánh giá để đảm bảo nhân viên sẽ biết cách phản ứng trong trường hợp xảy ra sự cố an ninh thực sự.	Phải
1.4	(Các) đầu mối liên lạc của công ty (POC) với CTPAT phải có kiến thức về các yêu cầu của chương trình CTPAT. Những cá nhân	CTPAT đòi hỏi POC được chỉ định là một cá nhân chủ động tham gia và giao tiếp tốt với Chuyên gia Bảo mật Chuỗi Cung ứng của mình.	Phải

ID	Tiêu chí	Hướng dẫn Thực hiện	Phải / Nên
	này cần cung cấp cập nhật thường xuyên cho quản lý cấp trên về các vấn đề liên quan đến chương trình, bao gồm tiến độ hoặc kết quả của các cuộc kiểm toán, diễn tập liên quan đến bảo mật và xác nhận CTPAT.	Thành viên có thể xác định thêm các cá nhân có thể giúp hỗ trợ chức năng này bằng cách liệt kê họ dưới dạng đầu mối liên hệ trên Cổng thông tin CTPAT.	

2. **<u>Đánh giá Rủi ro</u> –** Mối đe dọa liên tục của các nhóm khủng bố và các tổ chức tội phạm nhắm vào chuỗi cung ứng cho thấy các Thành viên cần phải đánh giá mức độ dễ bị tổn thương hiện thời và tiềm tàng từ các mối đe dọa đang biến động này. CTPAT nhận ra rằng khi một công ty có nhiều chuỗi cung ứng với nhiều đối tác kinh doanh, công ty sẽ phải đối mặt với sự phức tạp lớn hơn trong việc đảm bảo an ninh cho các chuỗi cung ứng này. Khi một công ty có nhiều chuỗi cung ứng, công ty nên tập trung vào các khu vực địa lý/chuỗi cung ứng có rủi ro cao hơn.

   Khi xác định rủi ro trong chuỗi cung ứng của mình, Thành viên phải xem xét các yếu tố khác nhau như mô hình kinh doanh, vị trí địa lý của nhà cung cấp và các khía cạnh khác có thể là đặc thù cho chuỗi cung ứng cụ thể.

   Định nghĩa Chính: Rủi ro – Một thước đo tác hại tiềm tàng từ một sự kiện không mong muốn bao gồm mối đe dọa, tính dễ bị tổn thương và hậu quả. Điều quyết định mức độ rủi ro là mối đe dọa có khả năng sẽ xảy ra như thế nào. Khả năng xảy ra cao thường sẽ tương đương với mức độ rủi ro cao. Rủi ro có thể không được loại bỏ, nhưng nó có thể được giảm thiểu bằng cách quản lý nó – hạ giảm mức độ dễ bị tổn thương hoặc tác động tổng thể đến doanh nghiệp.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
2.1	Thành viên CTPAT phải tiến hành và ghi lại mức độ rủi ro trong các chuỗi cung ứng. Thành viên CTPAT phải tiến hành đánh giá rủi ro tổng thể (RA) để xác định nơi có thể tồn tại lỗ hổng bảo mật. RA phải xác định các mối đe dọa, đánh giá rủi ro và kết hợp các biện pháp bền vững để giảm thiểu các lỗ hổng. Thành viên phải xem xét các yêu cầu CTPAT cụ thể	Đánh giá rủi ro tổng thể (RA) gồm hai phần chính. Phần đầu tiên là tự đánh giá các quy trình, thủ tục và chính sách bảo mật chuỗi cung ứng của Thành viên trong các cơ sở mà Thành viên kiểm soát để xác minh sự tuân thủ các tiêu chí bảo mật tối thiểu của CTPAT và đánh giá quản lý tổng thể về cách quản lý rủi ro. Phần thứ hai của RA là đánh giá rủi ro quốc tế. Phần này của RA bao gồm việc xác định (các) mối đe dọa địa lý dựa trên mô hình kinh doanh và vai trò của Thành viên trong chuỗi cung ứng. Khi xem xét tác động có thể có của mối đe dọa đối với an ninh của chuỗi cung ứng của thành viên, thành viên cần có phương pháp để đánh giá hoặc phân biệt các mức độ rủi ro. Một phương pháp đơn giản là đặt ra mức độ rủi ro giữa thấp, trung bình và cao.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
	đối với vai trò của thành viên trong chuỗi cung ứng.	CTPAT đã soạn hướng dẫn Đánh giá Rủi ro Năm bước để trợ giúp việc thực hiện phần đánh giá rủi ro quốc tế trong đánh giá rủi ro chung của thành viên và có thể xem trên trang web của Cơ quan Hải quan và Biên phòng Hoa Kỳ (CPB) tại https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. Đối với các Thành viên có chuỗi cung ứng rộng khắp, trọng tâm chính nên đặt vào các lĩnh vực có rủi ro cao hơn.	
2.2	Phần quốc tế trong đánh giá rủi ro nên ghi lại hoặc lập bản đồ vận chuyển hàng hóa của Thành viên trong toàn bộ chuỗi cung ứng, từ điểm xuất phát đến trung tâm phân phối của nhà nhập khẩu. Việc lập bản đồ nên bao gồm tất cả các đối tác kinh doanh liên quan trực tiếp và gián tiếp đến việc xuất khẩu/vận chuyển hàng hóa. Tùy tình hình, việc lập bản đồ nên bao gồm ghi lại cách thức hàng hóa di chuyển và ra vào khỏi các cơ sở vận chuyển/trung tâm vận chuyển hàng hóa và lưu ý xem hàng hóa có "nằm yên" tại một trong những địa điểm này trong một thời gian dài hay không. Hàng hóa dễ bị tổn thương hơn khi "nằm yên", chờ để di chuyển đến chặng tiếp theo của hành trình.	Khi xây dựng một quy trình để lập bản đồ chuỗi cung ứng, các lĩnh vực rủi ro cao nên được xem xét đầu tiên. Khi ghi lại sự chuyển động của mọi hàng hóa, Thành viên phải xem xét tất cả các bên có thể có liên quan - bao gồm cả những người sẽ chỉ xử lý các chứng từ xuất nhập khẩu như môi giới hải quan và những người khác có thể không trực tiếp xử lý hàng hóa, nhưng có thể kiểm soát hoạt động như các Hãng vận chuyển chung không vận hành tàu (NVOCC) hoặc nhà cung cấp dịch vụ hậu cần của bên thứ ba (3PL). Nếu bất kỳ phần nào của quá trình vận chuyển được giao cho nhà thầu phụ, điều này cũng cần phải được xem xét bởi vì càng có nhiều thành phần gián tiếp, rủi ro liên quan càng lớn. Việc lập bản đồ bao gồm việc tìm hiểu sâu hơn về cách thức hoạt động của chuỗi cung ứng. Bên cạnh việc xác định rủi ro, cũng nên tìm các lĩnh vực mà chuỗi cung ứng không hiệu quả, điều này có thể dẫn đến việc tìm cách giảm chi phí hoặc thời gian cần có để nhận sản phẩm.	Nên
2.3	Đánh giá rủi ro phải được xem xét hàng năm, hoặc thường xuyên hơn tùy vào các yếu tố rủi ro chi phối.	Các trường hợp có thể đòi hỏi xem xét đánh giá rủi ro thường xuyên hơn một lần mỗi năm bao gồm mức độ đe dọa gia tăng từ một quốc gia cụ thể, các giai đoạn cảnh báo tăng cao, sau khi xảy ra vi phạm hoặc sự cố an ninh, thay đổi đối tác kinh doanh và/hoặc thay đổi cấu trúc công ty/tỷ lệ sở hữu như sáp nhập và mua lại, v.v.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
2.4	Thành viên CTPAT nên có sẵn các quy trình bằng văn bản nhằm giải quyết việc quản lý khủng hoảng, tính liên tục của doanh nghiệp, kế hoạch phục hồi an ninh và nối lại hoạt động kinh doanh.	Khủng hoảng có thể bao gồm gián đoạn chuyển tải dữ liệu thương mại do một cuộc tấn công mạng, hỏa hoạn hoặc một lái xe của hãng vận chuyển bị tấn công bởi các cá nhân có vũ trang. Dựa trên rủi ro và nơi Thành viên hoạt động hoặc nhận nguồn cung cấp, các kế hoạch dự phòng có thể bao gồm các thông báo hoặc hỗ trợ bảo mật bổ sung; và cách thức phục hồi những gì đã bị hủy hoại hoặc bị đánh cắp và trở lại trạng thái hoạt động bình thường.	Nên

3. **Đối tác Kinh doanh –** Thành viên CTPAT tham gia với nhiều đối tác kinh doanh khác nhau, cả trong nước và quốc tế. Đối với những đối tác kinh doanh trực tiếp xử lý hàng hóa và/hoặc chứng từ xuất/nhập khẩu, Thành viên cần đảm bảo rằng các đối tác kinh doanh này có các biện pháp bảo mật thích hợp để tiếp nhận hàng hóa một cách an toàn trong chuỗi cung ứng quốc tế. Khi các đối tác kinh doanh thuê nhà thầu phụ cho một số chức năng nhất định, như thế là bổ sung thêm một mức độ phức tạp nữa vào quy trình, và điều này phải được xem xét khi tiến hành phân tích rủi ro của chuỗi cung ứng.

   Định nghĩa Chính: Đối tác Kinh doanh – Đối tác kinh doanh là bất kỳ cá nhân hoặc công ty nào mà hành động của họ có thể ảnh hưởng đến dây chuyền bảo đảm an toàn cho hàng hóa được nhập khẩu vào hoặc xuất khẩu từ Hoa Kỳ thông qua chuỗi cung ứng của Thành viên CTPAT. Đối tác kinh doanh có thể là bất kỳ bên nào cung cấp dịch vụ để đáp ứng một nhu cầu trong chuỗi cung ứng quốc tế của công ty. Những vai trò này bao gồm tất cả các bên (cả trực tiếp và gián tiếp) có liên quan trong việc mua, chuẩn bị tài liệu, tạo điều kiện, xử lý, lưu trữ, và/hoặc vận chuyển hàng hóa cho, hoặc đại diện cho, một Thành viên CTPAT nhập khẩu hay xuất khẩu. Hai ví dụ về các đối tác gián tiếp là các hãng vận chuyển được ký hợp đồng phụ và các kho gom hàng ở nước ngoài - được sắp xếp bởi một đại lý/nhà cung cấp dịch vụ hậu cần.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
3.1	Thành viên CTPAT phải có một quy trình dựa trên rủi ro bằng văn bản để sàng lọc các đối tác kinh doanh mới và để giám sát các đối tác hiện tại. Một yếu tố mà Thành viên nên đưa vào trong quy trình này là kiểm tra hoạt động liên quan đến rửa tiền và tài trợ khủng bố. Để hỗ trợ quá trình này, vui lòng tham khảo các Chỉ số cảnh báo của CTPAT về các hoạt động rửa tiền và tài trợ khủng bố dựa trên thương mại.	Sau đây là các ví dụ về một số yếu tố kiểm tra có thể giúp xác định xem một công ty có hợp pháp không: • Xác minh địa chỉ kinh doanh của công ty và thời gian họ hoạt động ở địa chỉ đó bao lâu; • Tiến hành nghiên cứu trên internet về cả công ty và các nhân sự chủ chốt; • Kiểm tra các nguồn giới thiệu doanh nghiệp; và • Yêu cầu báo cáo tín dụng. Ví dụ về các đối tác kinh doanh cần được sàng lọc gồm các đối tác kinh doanh trực tiếp như nhà sản xuất, nhà cung cấp sản phẩm, nhà bán hàng/nhà cung cấp dịch vụ liên quan và nhà cung cấp dịch vụ vận chuyển/hậu cần. Bất kỳ nhà bán hàng /nhà cung cấp dịch vụ nào liên quan trực tiếp đến chuỗi cung ứng của công ty và/hoặc xử lý thông tin/thiết bị nhạy cảm cũng được đưa vào danh sách được sàng lọc; điều này bao gồm các nhà môi giới hoặc nhà cung cấp CNTT theo hợp đồng. Sàng lọc sâu đến đâu phụ thuộc vào mức độ rủi ro trong chuỗi cung ứng.	Phải
3.4	Quá trình sàng lọc đối tác kinh doanh phải tính đến việc đối tác là Thành viên CTPAT hay thành viên trong chương trình Nhà điều hành kinh tế ủy quyền (AEO) đã được phê duyệt qua Thỏa thuận công nhận lẫn nhau (MRA) với Hoa Kỳ (hoặc MRA đã được phê duyệt). Chứng nhận trong CTPAT hoặc AEO được phê duyệt là bằng chứng chấp nhận được coi như đáp ứng các yêu cầu chương trình cho các đối tác kinh doanh và Thành viên phải có được bằng chứng chứng nhận và tiếp tục theo dõi các đối tác kinh doanh này để đảm bảo họ duy trì chứng nhận.	Chứng nhận CTPAT của đối tác kinh doanh có thể được xác minh thông qua hệ thống Giao diện Xác minh Trạng thái của Cổng thông tin CTPAT. Nếu chứng nhận đối tác kinh doanh là từ chương trình AEO nước ngoài theo một MRA với Hoa Kỳ, chứng nhận AEO nước ngoài sẽ bao gồm thành phần phần bảo mật. Các thành viên có thể truy cập vào trang web của cơ quan Hải quan nước ngoài, nơi có liệt kê tên của các AEO của cơ quan Hải quan đó, hoặc yêu cầu chứng nhận trực tiếp từ các đối tác kinh doanh. Các MRA hiện tại của Hoa Kỳ bao gồm: New Zealand, Canada, Jordan, Nhật Bản, Hàn Quốc, Liên minh châu Âu (28 nước thành viên), Đài Loan, Israel, Mexico, Singapore, Cộng hòa Dominica và Peru.	Phải
3.5	Khi Thành viên CTPAT thuê ngoài hoặc gọi thầu phụ các thành tố trong chuỗi cung ứng của mình, Thành viên phải	Các nhà nhập khẩu và xuất khẩu có xu hướng thuê ngoài một phần lớn các hoạt động trong chuỗi cung ứng của họ. Các nhà nhập khẩu (và một	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
	thực hiện thẩm định (thông qua các chuyến thăm, bảng câu hỏi, v.v.) để đảm bảo các đối tác kinh doanh này có các biện pháp bảo mật đáp ứng hoặc vượt quá Tiêu chí Bảo mật Tối thiểu (MSC) của CTPAT.	số nhà xuất khẩu) là các bên trong các giao dịch này thường có tầm ảnh hưởng lên các đối tác kinh doanh của họ và có thể yêu cầu thực hiện các biện pháp bảo mật trong toàn bộ chuỗi cung ứng của họ, như được bảo đảm. Đối với những đối tác kinh doanh không phải là thành viên CTPAT hoặc thành viên MRA được chấp nhận, Thành viên CTPAT sẽ thực hiện thẩm định để đảm bảo (khi có tầm ảnh hưởng để làm như vậy) các đối tác kinh doanh này đáp ứng các tiêu chí bảo mật thích ứng của chương trình. Để xác minh sự tuân thủ các yêu cầu bảo mật, các nhà nhập khẩu tiến hành đánh giá bảo mật với các đối tác kinh doanh của họ. Quá trình xác định cần thu thập bao nhiêu thông tin liên quan đến chương trình bảo mật của đối tác kinh doanh dựa vào đánh giá rủi ro của Thành viên, và nếu có nhiều chuỗi cung ứng, cần ưu tiên các lĩnh vực có nguy cơ cao. Xác định xem một đối tác kinh doanh có tuân thủ MSC hay không có thể được thực hiện theo nhiều cách. Dựa trên rủi ro, công ty có thể thực hiện kiểm toán thực địa tại cơ sở, thuê nhà thầu/nhà cung cấp dịch vụ để thực hiện kiểm toán tại chỗ, hoặc sử dụng bảng câu hỏi bảo mật. Nếu sử dụng bảng câu hỏi bảo mật, mức độ rủi ro sẽ xác định mức độ chi tiết hoặc bằng chứng cần thu thập. Có thể yêu cầu thêm chi tiết từ các công ty nằm ở các vùng rủi ro cao. Nếu Thành viên gửi bảng câu hỏi bảo mật cho các đối tác kinh doanh của mình, hãy cân nhắc yêu cầu các mục sau đây: • Tên và chức danh của (những) người trả lời bảng câu hỏi; • Ngày hoàn thành; • Chữ ký của (các) cá nhân trả lời bảng câu hỏi; • * Chữ ký của một quan chức cấp cao của công ty, giám sát viên an ninh hoặc đại diện công ty được ủy quyền để chứng thực tính chính xác của bảng câu hỏi; • Cung cấp đủ chi tiết trong các câu trả lời để xác định sự tuân thủ; và • Dựa trên rủi ro và nếu giao thức bảo mật địa phương cho phép, bổ sung bằng chứng bằng hình ảnh, bản sao chính sách/thủ tục và bản sao các biểu mẫu đã điền như danh mục kiểm tra các Thiết bị Vận chuyển Quốc tế và/hoặc sổ bảo vệ. * Chữ ký có thể là điện tử. Nếu khó lấy/xác minh chữ ký, người trả lời có thể chứng thực tính hợp lệ của câu hỏi qua email và xác nhận các câu trả	

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
		lời và bất kỳ bằng chứng củng cố nào kèm theo đã được người giám sát/người quản lý phê duyệt (cần có tên và chức vụ).	
3.6	Nếu xác định các điểm yếu trong khi các đánh giá bảo mật đối tác kinh doanh, chúng phải được xử lý càng sớm càng tốt và việc khắc phục phải được thực hiện kịp thời. Thành viên phải xác nhận rằng những thiếu sót đã được giảm nhẹ thông qua các bằng chứng ở dạng tài liệu.	CTPAT thừa nhận sẽ có các mốc thời gian khác nhau để thực hiện chỉnh sửa dựa trên những gì cần thiết cho việc chỉnh sửa. Cài đặt thiết bị phần cứng thường mất nhiều thời gian hơn thay đổi thủ tục, nhưng lỗ hổng bảo mật phải được giải quyết khi phát hiện ra. Ví dụ: Nếu vấn đề là thay thế hàng rào bị hư hỏng, quá trình mua hàng rào mới cần bắt đầu ngay lập tức (giải quyết sự thiếu sót) và lắp đặt hàng rào mới (hành động khắc phục) cần phải diễn ra ngay khi có thể. Dựa trên mức độ rủi ro liên quan và tầm quan trọng của điểm yếu được tìm thấy, một số vấn đề có thể cần được chú ý ngay lập tức. Ví dụ, nếu đó là một thiếu sót có thể gây nguy hiểm cho an ninh của một container, cần được giải quyết càng sớm càng tốt. Một số ví dụ về bằng chứng ở dạng tài liệu có thể bao gồm bản sao các hợp đồng cho các nhân viên bảo vệ bổ sung, ảnh chụp một camera an ninh hoặc báo động xâm nhập mới được cài đặt hoặc bản sao danh mục kiểm tra, v.v.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
3.7	Để đảm bảo các đối tác kinh doanh tiếp tục tuân thủ các tiêu chí bảo mật của CTPAT, Thành viên nên cập nhật các đánh giá bảo mật đối với các đối tác kinh doanh một cách thường xuyên hoặc khi hoàn cảnh/rủi ro đặt ra yêu cầu.	Định kỳ xem xét đánh giá bảo mật của các đối tác kinh doanh là điều rất quan trọng để đảm bảo rằng một chương trình bảo mật mạnh mẽ vẫn được áp dụng và hoạt động chính xác. Nếu một thành viên không bao giờ yêu cầu cập nhật đánh giá về chương trình bảo mật của đối tác kinh doanh, Thành viên sẽ không biết rằng chương trình từng rất hiệu quả nay không còn hiệu quả, do đó gây nguy hiểm cho chuỗi cung ứng của thành viên. Quyết định tần suất xem xét đánh giá bảo mật của đối tác dựa vào quy trình đánh giá rủi ro của Thành viên. Chuỗi cung ứng rủi ro cao hơn yêu cầu có đánh giá thường xuyên hơn so với chuỗi rủi ro thấp. Nếu Thành viên đánh giá bảo mật của đối tác kinh doanh bằng cách trực tiếp thăm quan, có thể nên xem xét tận dụng các loại kiểm tra khác. Ví dụ, đào tạo chéo nhân viên kiểm tra việc kiểm soát chất lượng cũng để tiến hành xác minh bảo mật. Các trường hợp có thể yêu cầu cập nhật thường xuyên hơn việc tự đánh giá bao gồm mức độ đe dọa gia tăng từ nước cung cấp, thay đổi vị trí cung cấp, đối tác kinh doanh quan trọng mới (những người thực sự xử lý hàng hóa, cung cấp bảo vệ cho cơ sở, v.v.).	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
3.8	Đối với các chuyến hàng đến Hoa Kỳ, nếu Thành viên ký hợp đồng dịch vụ vận chuyển với một hãng vận tải đường bộ khác, Thành viên phải sử dụng hãng vận chuyển đường bộ được CTPAT chứng nhận hoặc hãng vận chuyển đường bộ làm việc trực tiếp cho Thành viên như vạch ra qua một hợp đồng bằng văn bản. Hợp đồng phải quy định việc tuân thủ tất cả các yêu cầu về tiêu chí bảo mật tối thiểu (MSC).	Hãng vận chuyển phải cung cấp danh sách các hãng vận tải và tài xế được ký hợp đồng phụ tới các cơ sở nơi nhận và giao hàng. Mọi thay đổi trong danh sách nhà thầu phụ cần được chuyển ngay lập tức đến các đối tác liên quan. Khi xem xét các nhà cung cấp dịch vụ về sự tuân thủ, Thành viên cần xác minh rằng công ty được ký hợp đồng phụ thực sự là công ty vận chuyển hàng và không tiếp tục ký hợp đồng phụ chở hàng mà không được phê duyệt. Thành viên nên hạn chế gọi nhà thầu phụ dịch vụ vận chuyển xuống một cấp thôi. Nếu cho phép các trường hợp ngoại lệ được phép gọi thầu phụ thêm cấp nữa, Thành viên CTPAT và bên chuyển hàng phải được thông báo rằng hàng được ký hợp đồng phụ thêm một cấp nữa.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải/ Nên
3.9	Các thành viên CTPAT phải có sẵn một chương trình tuân thủ xã hội được lập thành tài liệu để, ít nhất, cũng giải quyết cách thức công ty đảm bảo hàng hóa nhập khẩu vào Hoa Kỳ không được khai thác, sản xuất hoặc chế tạo, toàn bộ hoặc một phần, bằng các hình thức lao động bị cấm, tức là lao động cưỡng bức, bị cầm tù, bị chuyển giao, hoặc lao động trẻ em bị chuyển giao.	Những nỗ lực của lĩnh vực tư nhân để bảo vệ quyền của người lao động trong hoạt động và chuỗi cung ứng có thể thúc đẩy sự hiểu biết nhiều hơn về luật và tiêu chuẩn lao động và giảm thiểu các hình thức lao động xấu. Những nỗ lực này cũng tạo ra một môi trường tốt hơn cho mối quan hệ giữa người lao động và người sử dụng lao động và cải thiện lợi nhuận của công ty. Mục 307 của Đạo luật Thuế quan năm 1930 (19 USC § 1307) nghiêm cấm nhập khẩu hàng hóa khai thác, sản xuất hoặc chế tạo, toàn bộ hoặc một phần, ở bất kỳ nước ngoài nào bằng lao động trẻ em bị cưỡng bức hoặc bị chuyển giao - kể cả lao động trẻ em bị ép buộc. Lao động cưỡng bức được xác định theo Công ước số 29 của Tổ chức Lao động Quốc tế chỉ mọi công việc hoặc dịch vụ mà một người bị ép buộc phải làm dưới sự đe dọa của một hình phạt nào đó và bản thân người đó không tự nguyện làm. Chương trình tuân thủ xã hội là một tập hợp các chính sách và thực tiễn mà qua đó một công ty tìm cách đảm bảo tuân thủ tối đa các yếu tố của bộ quy tắc ứng xử, bao gồm các vấn đề xã hội và lao động. Tuân thủ xã hội đề cập đến cách doanh nghiệp giải quyết trách nhiệm của mình trong việc bảo vệ môi trường, cũng như sức khỏe, an toàn và các quyền của nhân viên, cộng đồng nơi họ hoạt động và cuộc sống và cộng đồng của người lao động trong chuỗi cung ứng.	Phải

4. **<u>An ninh mạng</u>** – Trong thế giới kỹ thuật số ngày nay, an ninh mạng là chìa khóa để bảo vệ những tài sản quý giá nhất của công ty - tài sản trí tuệ, thông tin khách hàng, dữ liệu tài chính và thương mại, và hồ sơ nhân viên và nhiều thứ khác. Đi kèm với sự kết nối với internet ngày càng tăng là nguy cơ hệ thống thông tin của công ty bị xâm phạm. Mối đe dọa này liên quan đến các doanh nghiệp thuộc mọi loại hình và quy mô. Các biện pháp bảo mật công nghệ thông tin (CNTT) của công ty và dữ liệu là điều rất quan trọng và các tiêu chí được liệt kê cung cấp nền tảng cho một chương trình an ninh mạng tổng thể cho các Thành viên.

   Định nghĩa chính: An ninh mạng – An ninh mạng là hoạt động hoặc quy trình tập trung vào việc bảo vệ máy tính, mạng, chương trình và dữ liệu khỏi sự truy cập, thay đổi hoặc phá hủy ngoài ý muốn hoặc trái phép. Đó là quá trình xác định, phân tích, đánh giá và truyền đạt rủi ro liên quan đến mạng và chấp nhận, tránh, chuyển hoặc giảm thiểu rủi ro đến mức chấp nhận được, có cân nhắc chi phí và lợi ích.

   Công nghệ thông tin (CNTT) – CNTT bao gồm máy tính, lưu trữ, kết nối mạng và các thiết bị cụ thể khác, cơ sở hạ tầng và quy trình để tạo, xử lý, lưu trữ, bảo mật và trao đổi tất cả các dạng dữ liệu điện tử.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.1	Thành viên CTPAT phải có các chính sách và/hoặc thủ tục an ninh mạng toàn diện bằng văn bản để bảo vệ các hệ thống công nghệ thông tin (CNTT). Chính sách CNTT bằng văn bản, ở mức tối thiểu, phải bao gồm tất cả các tiêu chí An ninh mạng riêng lẻ.	Các thành viên được khuyến khích tuân theo các giao thức an ninh mạng dựa trên các tiêu chuẩn/khung công nghiệp được công nhận. * Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) là một tổ chức như vậy, cung cấp Khung Bảo mật An ninh mạng (https://www.nist.gov/cyberframework) cung cấp hướng dẫn tự nguyện dựa trên các tiêu chuẩn, hướng dẫn và thực hành hiện có để giúp quản lý và giảm rủi ro an ninh mạng cả bên trong và bên ngoài. Nó có thể được sử dụng để giúp xác định và ưu tiên các hành động để giảm rủi ro an ninh mạng và là một công cụ để điều chỉnh chính sách, kinh doanh và phương các cách tiếp cận công nghệ để quản lý rủi ro đó. Khung Bảo mật bổ sung cho quy trình quản lý rủi ro và chương trình an ninh mạng của một tổ chức. Ngoài ra, một tổ chức hiện không có chương trình an ninh mạng có thể sử dụng Khung Bảo mật làm tham chiếu để thiết lập một chương trình. * NIST là một cơ quan liên bang không có chức năng quản lý thuộc Bộ Thương mại nhằm thúc đẩy và duy trì các tiêu chuẩn đo lường, và đây là cơ quan xây dựng tiêu chuẩn công nghệ cho chính phủ liên bang.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.2	Để bảo vệ các hệ thống Công nghệ Thông tin (CNTT) trước các mối đe dọa an ninh mạng phổ biến, công ty phải cài đặt đầy đủ phương thức bảo vệ phần mềm/phần cứng khỏi phần mềm độc hại (virus, phần mềm gián điệp, sâu, Trojans, v.v.) và xâm nhập bên trong/bên ngoài (tường lửa) trong hệ thống máy tính của Thành viên. Thành viên phải đảm bảo rằng phần mềm bảo mật của họ là mới nhất và nhận được cập nhật bảo mật thường xuyên. Thành viên phải có chính sách và thủ tục để ngăn chặn các cuộc tấn công thông qua lừa đảo trên mạng. Nếu xảy ra xâm phạm dữ liệu hoặc có một sự kiện bất ngờ khác dẫn đến việc mất dữ liệu và/hoặc thiết bị thì thủ tục phải bao gồm việc phục hồi (hoặc thay thế) hệ thống CNTT và/hoặc dữ liệu.		Phải
4.3	Thành viên CTPAT sử dụng hệ thống mạng phải thường xuyên kiểm tra tính bảo mật của cơ sở hạ tầng CNTT. Nếu phát hiện các lỗ hổng, phải thực hiện các hành động khắc phục ngay khi có thể.	Một mạng máy tính an toàn có tầm quan trọng lớn đối với doanh nghiệp và việc đảm bảo rằng nó được bảo vệ cần phải được kiểm tra một cách thường xuyên. Điều này có thể được thực hiện bằng cách lên lịch rà soát lỗ hổng. Giống như nhân viên bảo vệ kiểm tra các cửa ra vào và cửa sổ tại một doanh nghiệp, rà soát lỗ hổng (VS) xác định các lỗ hổng trên máy tính của quý vị (cổng mở và địa chỉ IP), hệ điều hành và phần mềm mà tin tặc có thể truy cập vào hệ thống CNTT của công ty. VS thực hiện điều này bằng cách so sánh kết quả rà soát của nó với cơ sở dữ liệu về các lỗ hổng đã biết và tạo ra một báo cáo can thiệp để doanh nghiệp hành động. Có nhiều phiên bản miễn phí và thương mại đối với chương trình rà soát lỗ hổng. Tần suất của việc kiểm tra phụ thuộc vào các yếu tố khác nhau như mô hình kinh doanh và mức độ rủi ro của công ty. Ví dụ, công ty nên tiến hành kiểm tra bất cứ khi nào có thay đổi đối với cơ sở hạ tầng mạng của doanh nghiệp. Tuy nhiên, các cuộc tấn công mạng đang gia tăng với mọi mô hình doanh nghiệp và cần xem xét điều này khi thiết kế một kế hoạch kiểm tra.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.4	Chính sách an ninh mạng nên giải quyết cách thức Thành viên chia sẻ thông tin về các mối đe dọa an ninh mạng với chính phủ và các đối tác kinh doanh khác.	Các thành viên được khuyến khích chia sẻ thông tin về các mối đe dọa an ninh mạng với chính phủ và các đối tác kinh doanh trong chuỗi cung ứng. Chia sẻ thông tin là một phần quan trọng trong sứ mệnh của Bộ An ninh Nội địa nhằm tạo ra nhận thức tình huống chung về hoạt động mạng độc hại. Thành viên CTPAT có thể tham gia Trung tâm Tích hợp Truyền thông và An ninh mạng Quốc gia (NCCIC - https://www.us-cert.gov/nccic). NCCIC chia sẻ thông tin giữa các đối tác lĩnh vực công và tư nhân để xây dựng nhận thức về các lỗ hổng, sự cố và giảm nhẹ. Người dùng hệ thống kiểm soát công nghiệp và mạng có thể đăng ký các sản phẩm thông tin, nguồn cấp dữ liệu và dịch vụ một cách miễn phí.	Nên
4.5	Phải có một hệ thống để xác định truy cập trái phép hệ thống/dữ liệu CNTT hoặc lạm dụng các chính sách và quy trình bao gồm việc nhân viên hoặc nhà thầu truy cập không đúng hệ thống nội bộ hoặc trang web bên ngoài và giả mạo hoặc thay đổi dữ liệu kinh doanh. Tất cả những người vi phạm phải chịu các hình thức kỷ luật thích hợp.		Phải
4.6	Các chính sách và thủ tục an ninh mạng phải được xem xét hàng năm, hoặc thường xuyên hơn, tùy tình hình rủi ro hoặc hoàn cảnh yêu cầu. Sau khi xem xét, các chính sách và thủ tục phải được cập nhật nếu cần thiết.	Một ví dụ về tình huống đòi hỏi cập nhật chính sách sớm hơn hàng năm là một cuộc tấn công mạng. Sử dụng những bài học rút ra từ cuộc tấn công sẽ giúp củng cố chính sách an ninh mạng của Thành viên.	Phải
4.7	Quyền truy cập của người dùng phải được hạn chế dựa trên mô tả công việc hoặc nhiệm vụ được giao. Việc cấp quyền truy cập phải được xem xét thường xuyên để đảm bảo quyền truy cập vào các hệ thống nhạy cảm là dựa trên yêu cầu công việc. Phải chấm dứt truy cập máy tính và mạng khi nhân viên nghỉ việc.		Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.8	Các cá nhân có quyền truy cập vào hệ thống Công nghệ Thông tin (CNTT) phải sử dụng các tài khoản được thiết lập riêng. Phải bảo đảm quyền truy cập vào hệ thống CNTT không bị xâm nhập bằng việc sử dụng mật khẩu khó đoán, cụm mật khẩu hoặc các hình thức xác thực khác và quyền truy cập của người dùng vào hệ thống CNTT phải được bảo vệ. Phải thay đổi mật khẩu và/hoặc cụm mật khẩu càng sớm càng tốt nếu có bằng chứng về sự xâm nhập hoặc có nghi ngờ hợp lý về sự xâm nhập.	Để bảo vệ hệ thống CNTT chống lại sự xâm nhập, quyền truy cập của người dùng phải được bảo vệ bằng cách trải qua quy trình xác thực. Mật khẩu hay cụm mật khẩu đăng nhập phức tạp, công nghệ sinh trắc học và thẻ ID điện tử là ba loại quy trình xác thực khác nhau. Các quy trình sử dụng nhiều hơn một biện pháp được ưu tiên. Chúng được gọi là xác thực hai yếu tố (2FA) hoặc xác thực đa yếu tố (MFA). MFA là an toàn nhất vì nó yêu cầu người dùng đưa ra hai hoặc nhiều bằng chứng (thông tin xác thực) để xác thực danh tính của người đó trong quá trình đăng nhập. MFA có thể hỗ trợ ngăn chặn các cuộc xâm nhập mạng nhờ khai thác mật khẩu yếu hoặc thông tin bị đánh cắp. MFA có thể hỗ trợ ngăn chặn các cuộc tấn công này bằng cách yêu cầu các cá nhân bổ sung mật khẩu hoặc cụm mật khẩu (thứ bạn biết) bằng thứ gì đó bạn có, như một token hoặc một trong các tính năng thể chất của bạn - sinh trắc học. Nếu sử dụng mật khẩu, chúng cần phải phức tạp. Ấn bản đặc biệt NIST 800-63B của Viện Tiêu chuẩn và Công nghệ (NIST): Nguyên tắc Nhận dạng Kỹ thuật số, bao gồm hướng dẫn tạo mật khẩu (https://pages.nist.gov/800-63-3/sp800-63b.html). Tài liệu khuyến nghị sử dụng các cụm mật khẩu dài, dễ nhớ thay vì các từ có ký tự đặc biệt. Các cụm mật khẩu dài này (NIST khuyên nên cho phép dài tối đa 64 ký tự) được coi là khó bẻ khóa hơn nhiều vì chúng được tạo thành từ một câu hoặc cụm từ dễ nhớ.	Phải
4.9	Thành viên cho phép người dùng của họ kết nối mạng từ xa phải sử dụng các công nghệ bảo mật, chẳng hạn như mạng riêng ảo (VPN), để cho phép nhân viên truy cập mạng nội bộ của công ty một cách an toàn khi ở bên ngoài văn phòng. Thành viên cũng phải có các quy trình được thiết kế để ngăn chặn người dùng trái phép truy cập từ xa.	VPN không phải là lựa chọn duy nhất để bảo vệ quyền truy cập từ xa vào mạng. Xác thực đa yếu tố (MFA) là một phương pháp khác. Một ví dụ về xác thực đa yếu tố là một token có mã bảo mật động mà nhân viên phải gõ vào để truy cập mạng.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.10	Nếu Thành viên cho phép nhân viên sử dụng các thiết bị cá nhân để thực hiện công việc của công ty, tất cả các thiết bị đó phải tuân thủ các chính sách và quy trình an ninh mạng của công ty như cập nhật bảo mật thường xuyên và phương pháp truy cập an toàn vào mạng của công ty.	Các thiết bị cá nhân bao gồm phương tiện lưu trữ như CD, DVD và ổ USB. Phải cẩn thận nếu nhân viên được phép kết nối phương tiện cá nhân của họ với các hệ thống riêng lẻ vì các thiết bị lưu trữ dữ liệu này có thể bị nhiễm phần mềm độc hại rồi có thể lan truyền qua mạng của công ty.	Phải
4.11	Các chính sách và thủ tục an ninh mạng nên bao gồm các biện pháp để ngăn chặn việc sử dụng các sản phẩm công nghệ giả hoặc được cấp phép không đúng cách.	Phần mềm máy tính là tài sản trí tuệ (IP) thuộc sở hữu của nơi đã tạo ra nó. Nếu không có sự cho phép rõ ràng của nhà sản xuất hoặc nhà xuất bản, việc cài đặt phần mềm là bất hợp pháp, bất kể nó được mua như thế nào. Sự cho phép đó hầu như luôn có dạng một giấy phép từ nhà xuất bản, đi kèm với các bản sao chính thức của phần mềm. Phần mềm không được cấp phép có nhiều khả năng bị lỗi do không thể cập nhật. Nó dễ bị chứa phần mềm độc hại, khiến máy tính và thông tin của chúng trở nên vô dụng. Không thể trông chờ việc bảo hành hoặc hỗ trợ cho phần mềm không có giấy phép, nên công ty phải tự mình xử lý các thất bại. Cũng có những hậu quả pháp lý đối với phần mềm không được cấp phép, bao gồm cả hình phạt dân sự nghiêm khắc và truy tố hình sự. Ăn cắp phần mềm tăng chi phí cho người dùng phần mềm hợp pháp, chính thức và giảm vốn dành cho đầu tư vào nghiên cứu và phát triển phần mềm mới. Thành viên nên có chính sách yêu cầu lưu trữ nhãn mã số sản phẩm và giấy chứng nhận quyền sở hữu khi mua. CD, DVD và ổ USB bao gồm các tính năng bảo mật ba chiều để giúp đảm bảo quý vị nhận được các sản phẩm thật và để bảo vệ chống hàng giả.	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
4.12	Dữ liệu nên được sao lưu mỗi tuần một lần hoặc khi thích hợp. Tất cả dữ liệu nhạy cảm và riêng tư nên được lưu trữ ở định dạng được mã hóa.	Nên sao lưu dữ liệu vì mất dữ liệu có thể ảnh hưởng một cách khác nhau đến các cá nhân trong một tổ chức. Sao lưu hàng ngày cũng được khuyến nghị trong trường hợp máy chủ dùng chung hay sản xuất bị xâm nhập/mất dữ liệu. Các hệ thống riêng lẻ có thể yêu cầu sao lưu ít thường xuyên hơn, tùy thuộc vào loại thông tin có liên quan. Phương tiện được sử dụng để lưu trữ các bản sao lưu tốt nhất nên được lưu trữ tại một cơ sở bên ngoài. Các thiết bị được sử dụng để sao lưu dữ liệu không nên nằm trên cùng một mạng với thiết bị được sử dụng cho công việc sản xuất. Sao lưu dữ liệu lên một đám mây có thể được chấp nhận như là một cơ sở bên ngoài.	Nên
4.13	Tất cả phương tiện, phần cứng hoặc thiết bị CNTT khác có chứa thông tin nhạy cảm liên quan đến quá trình xuất/nhập khẩu phải được kiểm đếm thông qua kiểm tra kho thường kỳ. Khi thanh lý, chúng phải được tẩy trùng đúng cách và/hoặc tiêu hủy theo Hướng dẫn của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) về cách tẩy trùng phương tiện lưu trữ hoặc các hướng dẫn phù hợp khác của ngành.	Một số loại phương tiện máy tính là ổ cứng, ổ di động, đĩa CD-ROM hoặc CD-R, DVD hoặc ổ USB. Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đã phát triển các tiêu chuẩn phá hủy phương tiện truyền thông dữ liệu của chính phủ. Thành viên nên tham khảo các tiêu chuẩn của NIST về tẩy trùng và phá hủy thiết bị và phương tiện CNTT. Tẩy trùng phương tiện lưu trữ: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	Phải

Lĩnh vực Trọng tâm Thứ hai: An ninh Vận tải

5. **<u>Bảo mật cho Phương tiện vận chuyển và Công cụ Vận tải Quốc tế</u>** – Các mánh khóe buôn lậu thường liên quan đến việc sửa đổi các phương tiện vận chuyển và Công cụ Vận tải Quốc tế (IIT) hoặc che giấu hàng lậu trong IIT. Danh mục tiêu chí này bao gồm các biện pháp bảo mật được thiết kế để ngăn chặn, phát hiện và/hoặc ngăn chặn sự thay đổi cấu trúc IIT hoặc lén lút xâm nhập vào chúng, qua đó có thể vận chuyển hàng hay người trái phép.

   Tại điểm đóng hàng/đóng gói, cần có quy trình kiểm tra IIT và niêm phong chúng đúng cách. Hàng hóa quá cảnh hoặc "nằm yên" ít bị kiểm soát hơn và do đó dễ bị xâm nhập hơn, đó là lý do tại sao kiểm soát niêm phong và phương pháp theo dõi hàng hóa đang quá cảnh là tiêu chí bảo mật chính yếu.

   Các cuộc xâm nhập vào chuỗi cung ứng thường xảy ra nhất trong quá trình vận chuyển; do đó, Thành viên phải cảnh giác rằng các tiêu chí hàng hóa chính yếu này được bảo đảm trong toàn chuỗi cung ứng.

   Định nghĩa chính: Công cụ Vận tải Quốc tế (IIT) – ITT bao gồm container, xe kéo container, thiết bị tải hàng (ULD), xe tải nâng, xe tải chở hàng, thùng vận chuyển, thùng, khung, pallet, khung gỗ, lõi cho vải dệt, hoặc các container chuyên dụng khác (có hàng hoặc rỗng), đang sử dụng hoặc sẽ được sử dụng trong việc vận chuyển hàng hóa trong thương mại quốc tế.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
5.1	Phương tiện vận chuyển và Công cụ Vận tải Quốc tế (IIT) phải được cất giữ trong khu vực an toàn để ngăn chặn việc tiếp cận trái phép, mà có thể dẫn đến thay đổi cấu trúc của Công cụ Vận tải Quốc tế hoặc (tùy thực tế) dẫn tới việc xâm phạm niêm phong/cửa.	Việc lưu trữ an toàn các phương tiện vận chuyển và Công cụ Vận tải Quốc tế (cả rỗng và đầy hàng) rất quan trọng để chống lại việc tiếp cận trái phép.	Phải
5.2	Quy trình kiểm tra CTPAT phải có thủ tục bằng văn bản cho cả kiểm tra an ninh và kiểm tra nông nghiệp.	Với sự phổ biến của các mánh khóe buôn lậu liên quan đến việc sửa đổi phương tiện vận chuyển hoặc Công cụ Vận tải Quốc tế, điều bắt buộc là Thành viên phải tiến hành kiểm tra phương tiện vận chuyển và Công cụ Vận tải Quốc tế để tìm kiếm sâu bệnh có thể nhìn thấy và những khiếm khuyết cấu trúc nghiêm trọng. Tương tự như vậy, việc ngăn ngừa ô nhiễm dịch hại thông qua phương tiện vận chuyển và IIT là mối quan tâm hàng đầu, vì vậy một thành phần nông nghiệp đã được thêm vào quy trình kiểm tra an ninh.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
		Ô nhiễm sâu bệnh được định nghĩa là các dạng động vật, côn trùng hoặc động vật không xương sống khác (sống hoặc chết, trong bất kỳ giai đoạn vòng đời nào, bao gồm vỏ trứng hoặc ấu trùng), hoặc bất kỳ vật chất hữu cơ nào có nguồn gốc động vật (bao gồm máu, xương, lông, thịt, dịch tiết, bài tiết); thực vật có thể nảy mầm hoặc không thể nảy mầm hoặc các sản phẩm thực vật (bao gồm trái cây, hạt, lá, cành, rễ, vỏ cây); hoặc vật chất hữu cơ khác, bao gồm cả nấm; hoặc đất, hoặc nước; trong đó các sản phẩm đó không phải là hàng hóa đăng ký trong các Công cụ Vận tải Quốc tế (ví dụ như container, thiết bị tải hàng, v.v.).	
5.3	Thành viên CTPAT phải đảm bảo có tiến hành các cuộc kiểm tra nông nghiệp và an ninh CTPAT mang tính hệ thống sau đây. Các yêu cầu đối với các đợt kiểm tra này sẽ khác nhau tùy thuộc vào việc chuỗi cung ứng có nguồn gốc từ đất liền (Canada hoặc Mexico) hoặc nếu chuỗi cung ứng có nguồn gốc ở nước ngoài (đường biển và đường hàng không). Trước khi đóng hàng/đóng gói, mọi Công cụ Vận tải Quốc tế (IIT) rỗng phải được kiểm tra và phương tiện vận chuyển cũng phải được kiểm tra khi chúng đi qua biên giới đất liền vào Hoa Kỳ. <u>Yêu cầu kiểm tra đối với các lô hàng CTPAT qua đường biển, đường hàng không và đường bộ (tùy thực tế) bằng đường sắt hoặc vận tải hàng hóa đa phương thức:</u> Phải tiến hành kiểm tra bảy điểm với mọi container rỗng và các thiết bị tải hàng (ULD); và phải tiến hành kiểm tra tám điểm với mọi container và ULD đông lạnh rỗng: 1. Tường trước; 2. Bên trái; 3. Bên phải; 4. Sàn; 5. Trần/Mái; 6. Cửa bên trong/bên ngoài, bao gồm độ tin cậy của cơ chế khóa cửa; 7. Bên ngoài/Bên dưới; và 8. Khung quạt trên container đông lạnh.	Kiểm tra an ninh và nông nghiệp được thực hiện trên các Công cụ Vận tải Quốc tế (IIT) và phương tiện vận chuyển để đảm bảo cấu trúc của chúng không bị sửa đổi để che giấu hàng lậu hoặc đã bị nhiễm sâu bệnh nông nghiệp. Các chuỗi cung ứng ở nước ngoài được yêu cầu kiểm tra tất cả các công cụ IIT tại điểm đóng hàng/đóng gói. Tuy nhiên, nếu chuỗi cung ứng đường biển/đường hàng không có rủi ro cao hơn, có thể cần bao gồm các quy trình kiểm tra mở rộng hơn để bao gồm phương tiện vận chuyển và/hoặc kiểm tra tại các cảng biển hoặc các cơ sở hậu cần hàng không. Thông thường, các lô hàng có đường biên giới đất liền có mức độ rủi ro cao hơn, đó là lý do tại sao cả phương tiện vận chuyển lẫn IIT phải trải qua nhiều đợt kiểm tra. Một số ví dụ về IIT cho các phương thức khác nhau là container đại dương, container/rơ moóc đông lạnh, rơ moóc trên đường, rơ moóc phẳng, thùng chứa, đường ray/thùng, phễu và thiết bị tải hàng (ULD). Mục Thư viện Công cộng của Cổng thông tin CTPAT có đăng tải tài liệu đào tạo về kiểm tra an ninh và phương tiện vận chuyển nông nghiệp/Công cụ Vận tải Quốc tế.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	<u>Yêu cầu kiểm tra bổ sung đối với cửa khẩu biên giới đất liền thông qua các hãng vận tải đường bộ:</u> Việc kiểm tra phương tiện vận chuyển và IIT phải được tiến hành tại các bãi phương tiện vận chuyển/bãi chứa IIT. Nếu khả thi, việc kiểm tra phải được tiến hành khi vào và ra khỏi bãi chứa và tại điểm đóng hàng/đóng gói. Các kiểm tra có hệ thống này phải bao gồm kiểm tra 17 điểm: **<u>Máy kéo:</u>** 1. Cản/lốp/vành; 2. Cửa, khoang dụng cụ và cơ cấu khóa; 3. Hộp bình điện; 4. Máy hút khí; 5. Bình nhiên liệu; 6. Khoang nội thất/buồng ngủ; và 7. Khung/mái. **<u>Rơ moóc</u>**: 1. Khu vực bánh xe thứ năm - kiểm tra ngăn/tấm trượt; 2. Ngoại thất - mặt trước/mặt bên; 3. Phía sau - cản/cửa; 4. Tường trước; 5. Bên trái; 6. Bên phải; 7. Sàn; 8. Trần/mái; 9. Cửa bên trong/bên ngoài và cơ chế khóa; và 10. Bên ngoài/Bên dưới.		
5.4	Phương tiện vận chuyển và Công cụ Vận tải Quốc tế (tùy tình hình) phải được trang bị phần cứng bên ngoài có thể chịu được một cách hợp lý các nỗ lực để loại bỏ nó. Cửa, tay cầm, thanh, chốt, đinh tán,	Cân nhắc sử dụng các thùng chứa/rơ mooc có bản lề chống can thiệp. Thành viên cũng có thể đặt các tấm hoặc ghim bảo vệ trên	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	giá đỡ và tất cả các bộ phận khác của cơ chế khóa của thùng container phải được kiểm tra đầy đủ để phát hiện sự can thiệp và mọi sự không nhất quán về phần cứng trước khi gắn thiết bị niêm phong.	ít nhất hai bản lề của cửa và/hoặc đặt keo/băng dính trên ít nhất một bản lề ở mỗi bên.	
5.5	Việc kiểm tra mọi phương tiện vận chuyển và các Công cụ Vận tải Quốc tế rỗng nên được ghi lại trong danh mục kiểm tra. Các yếu tố sau phải được ghi lại trong danh mục kiểm tra: • Số Container/Rơ mooc /Công cụ Vận tải Quốc tế; • Ngày kiểm tra; • Thời gian kiểm tra; • Tên nhân viên tiến hành kiểm tra; và • Các khu vực cụ thể của Công cụ Vận tải Quốc tế đã được kiểm tra. Nếu việc kiểm tra được giám sát, giám sát viên cũng nên ký vào danh mục kiểm tra. Biên bản kiểm tra Container/Công cụ Vận tải Quốc tế phải là một phần của gói tài liệu vận tải. Người nhận hàng phải nhận được gói tài liệu vận chuyển hoàn chỉnh trước khi nhận hàng.		Nên
5.6	Mọi cuộc kiểm tra an ninh nên được thực hiện trong một khu vực có kiểm soát ra vào và, nếu có, được giám sát thông qua hệ thống camera quan sát.		Nên
5.7	Nếu phát hiện ô nhiễm dịch hại khi kiểm tra phương tiện vận chuyển/Công cụ Vận tải Quốc tế, phải tiến hành rửa/hút bụi để loại bỏ ô nhiễm đó. Hồ sơ phải được giữ lại trong một năm để chứng minh sự tuân thủ các yêu cầu kiểm tra này.	Lưu giữ hồ sơ về các loại gây ô nhiễm được tìm thấy, nơi chúng được tìm thấy (vị trí phương tiện vận chuyển) và cách loại bỏ dịch hại, là những hành động hữu ích có thể hỗ trợ Thành viên trong việc ngăn ngừa ô nhiễm dịch hại trong tương lai.	Phải
5.8	Dựa trên rủi ro, nhân viên quản lý nên tiến hành lục soát ngẫu nhiên các phương tiện vận chuyển sau khi nhân viên vận chuyển đã tiến hành kiểm tra phương tiện vận chuyển/Công cụ Vận tải Quốc tế. Việc lục soát phương tiện vận chuyển nên được thực hiện định kỳ, với tần suất cao hơn dựa trên rủi ro. Việc lục soát nên được tiến hành ngẫu nhiên mà không có cảnh báo, để không thể dự đoán trước được.	Tiến hành lục soát mang tính giám sát đối với phương tiện vận chuyển nhằm chống lại các âm mưu nội bộ. Như một cách thực hành tốt nhất, người giám sát có thể giấu một vật phẩm (như đồ chơi hoặc hộp màu) trên phương tiện vận chuyển để xác định xem người kiểm tra sàng lọc hiện trường/người vận hành phương tiện vận chuyển có tìm thấy nó	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	Việc kiểm tra cần được tiến hành tại nhiều địa điểm khác nhau, nơi phương tiện vận chuyển dễ bị ảnh hưởng: sân vận chuyển, sau khi xe tải đã được chất hàng, và trên đường đến biên giới Hoa Kỳ.	không. Nhân viên giám sát có thể là người quản lý an ninh, chịu trách nhiệm trước quản lý cấp cao về an ninh hoặc nhân viên quản lý được chỉ định khác.	
5.14	Thành viên CTPAT nên làm việc với các nhà cung cấp dịch vụ vận tải của mình để theo dõi phương tiện vận chuyển từ điểm xuất phát đến điểm đến cuối cùng. Các yêu cầu cụ thể về theo dõi, báo cáo và chia sẻ dữ liệu nên được đưa vào trong các điều khoản của thỏa thuận dịch vụ với các nhà cung cấp dịch vụ.		Nên
5.15	Chủ hàng nên có quyền truy cập vào hệ thống giám sát GPS của hãng vận chuyển, để họ có thể theo dõi đường đi của lô hàng.		Nên
5.16	Đối với các lô hàng biên giới trên đất liền gần biên giới Hoa Kỳ, nên thực hiện chính sách “không dừng” đối với việc dừng không theo lịch.	Hàng hóa nằm yên một chỗ là hàng hóa có nguy cơ. Chính sách này không cần bao quát các điểm dừng theo lịch nhưng chúng phải được xem xét trong một quy trình theo dõi và giám sát tổng thể.	Nên
5.24	Trong các khu vực có rủi ro cao và ngay trước khi đến cửa khẩu biên giới, các Thành viên CTPAT nên kết hợp quy trình xác minh "cơ hội cuối cùng" với các lô hàng nhập vào Hoa Kỳ để kiểm tra phương tiện vận chuyển/ Công cụ Vận tải Quốc tế để nhận biết các dấu hiệu can thiệp bao gồm kiểm tra trực quan phương tiện vận chuyển và quá trình xác minh niêm phong VVTT. Các cá nhân được đào tạo đúng cách nên tiến hành kiểm tra. V – (View) Xem xét niêm phong và cơ chế khóa container; đảm bảo chúng bình thường; V – (Verify) Đối chiếu lại số niêm phong với các tài liệu vận chuyển cho chính xác; T – (Tug) Kéo thử niêm phong để đảm bảo nó được gắn đúng cách; T – (Twist and Turn) Vặn và xoay niêm phong bu lông để đảm bảo các bộ phận của nó không bị tháo ra, tách rời khỏi nhau hoặc bất kỳ phần nào của niêm phong bị lỏng.		Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
5.29	Nếu phát hiện một mối đe dọa đáng tin cậy (hoặc được tìm thấy) đối với an ninh của lô hàng hoặc phương tiện vận chuyển, Thành viên phải cảnh báo (càng sớm càng tốt) cho các đối tác kinh doanh trong chuỗi cung ứng có thể bị ảnh hưởng và các cơ quan thực thi pháp luật phù hợp.		Phải

6. **<u>Bảo vệ Niêm phong</u> –** Việc niêm phong rơ moóc và container, bao gồm tính toàn vẹn niêm phong, tiếp tục là một yếu tố quan trọng của chuỗi cung ứng an toàn. Bảo vệ niêm phong bao gồm chính sách niêm phong toàn diện bằng văn bản nhằm xử lý tất cả các khía cạnh của việc bảo vệ niêm phong; sử dụng các niêm phong đúng đắn theo yêu cầu CTPAT; gắn niêm phong đúng cách trên IIT và xác minh rằng niêm phong đã được gắn đúng cách.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
6.1	Thành viên CTPAT phải có quy trình niêm phong bảo mật cao, chi tiết, bằng văn bản mô tả cách thức niêm phong được phát hành và kiểm soát tại cơ sở và trong quá trình vận chuyển. Quy trình phải cung cấp các bước cần thực hiện nếu niêm phong bị thay đổi, can thiệp, hoặc có số niêm phong không đúng, bao gồm ghi hồ sơ cho sự việc, các giao thức truyền thông cho các đối tác, và điều tra vụ việc. Những phát hiện từ cuộc điều tra phải được ghi lại và bất kỳ hành động khắc phục nào cũng phải được thực hiện nhanh nhất có thể. Quy trình bằng văn bản này phải được duy trì ở cấp điều hành địa phương để có thể dễ dàng tiếp cận. Quy trình phải được xem xét ít nhất một lần một năm và được cập nhật khi cần thiết. Kiểm soát niêm phong bằng văn bản phải bao gồm các yếu tố sau: **Kiểm soát tiếp cận niêm phong**: • Hạn chế việc quản lý niêm phong chỉ giới hạn trong số nhân viên được ủy quyền. • Lưu trữ an toàn. **Niêm phong trong kho, Phân phối và Theo dõi (Sổ niêm phong):** • Ghi lại việc nhận niêm phong mới. • Ghi lại việc phát hành niêm phong trong sổ trực. • Theo dõi niêm phong thông qua sổ trực. • Chỉ những nhân viên được đào tạo, có thẩm quyền mới có thể gắn niêm phong lên Công cụ Vận tải Quốc tế (IIT).		Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	Kiểm soát niêm phong trong quá trình vận chuyển : • Khi nhận IIT có niêm phong (hoặc sau khi dừng), xác minh niêm phong còn nguyên vẹn không có dấu hiệu bị can thiệp. • Xác nhận số niêm phong khớp với những gì được ghi chú trên chứng từ vận chuyển. **Niêm phong bị hỏng trong khi vận chuyển:** • Nếu kiểm tra hàng, ghi lại số niêm phong thay thế. • Người lái xe phải thông báo ngay cho nhóm điều phối khi niêm phong bị hỏng, cho biết ai đã phá vỡ niêm phong và cung cấp số niêm phong mới. • Hãng vận chuyển phải thông báo ngay cho người gửi, người môi giới và nhà nhập khẩu về việc thay đổi niêm phong và số niêm phong thay thế. • Người gửi hàng phải ghi số niêm phong thay thế vào sổ ghi niêm phong. **Niêm phong không khớp:** • Giữ lại niêm phong bị sửa đổi hoặc bị can thiệp để hỗ trợ điều tra. • Điều tra sự khác biệt; theo dõi bằng các biện pháp khắc phục (nếu cần). • Nếu phù hợp, báo cáo các niêm phong bị xâm phạm cho CBP và chính phủ nước ngoài phù hợp để hỗ trợ điều tra.		
6.2	Tất cả các lô hàng CTPAT có thể được niêm phong phải được bảo vệ ngay sau khi đóng hàng/tải hàng/đóng gói bởi các bên có trách nhiệm (ví dụ như người gửi hàng hoặc bên đóng gói đại diện cho người gửi hàng) bằng một niêm phong bảo mật cao, đáp ứng hoặc vượt quá tiêu chuẩn 17712 mới nhất của Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) đối với niêm phong bảo mật cao. Mọi niêm phong được sử dụng phải được gắn an toàn và đúng cách vào Công cụ Vận tải Quốc tế đang vận chuyển hàng hóa của Thành viên CTPAT đến/đi từ Hoa Kỳ.	Niêm phong bảo mật cao được sử dụng phải được gắn vào vị trí chốt khóa, nếu có, thay vì tay nắm cửa bên phải. Niêm phong phải được đặt ở dưới cùng của thanh dọc nằm chính giữa của cửa container bên phải. Ngoài ra, cũng có thể gắn niêm phong trên tay khóa bên trái nằm chính giữa trên cửa container bên phải nếu không có vị trí chốt khóa. Nếu sử dụng niêm phong bu lông, nên gắn niêm phong bu lông với phần nòng hoặc chèn mặt hướng lên trên với phần nòng phía trên bệ.	Phải
6.5	Thành viên CTPAT (quản lý niêm phong trong kho) phải có thể chứng minh rằng các niêm phong bảo mật cao mà họ sử dụng đáp ứng hoặc vượt quá tiêu chuẩn ISO 17712 mới nhất.	Bằng chứng tuân thủ chấp nhận được là một bản sao giấy chứng nhận thử nghiệm trong phòng thí nghiệm cho thấy có tuân thủ tiêu chuẩn niêm phong bảo mật cao của ISO. Thành viên CTPAT cần nhận thức được đặc điểm cho thấy có sự can thiệp vào niêm phong họ mua.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
6.6	Nếu Thành viên quản lý niêm phong trong kho, ban quản trị công ty hoặc giám sát viên an ninh phải tiến hành kiểm toán niêm phong bao gồm kiểm kê định kỳ các niêm phong được lưu kho và đối chiếu với sổ kiểm kê niêm phong và chứng từ vận chuyển. Tất cả các cuộc kiểm toán phải được ghi hồ sơ. Là một phần của quy trình kiểm toán niêm phong tổng thể, người giám sát bến tàu và/hoặc người quản lý kho phải định kỳ xác minh số niêm phong được sử dụng trên phương tiện vận chuyển và Công cụ Vận tải Quốc tế.		Phải
6.7	Phải tuân thủ quy trình xác minh niêm phong của CTPAT để đảm bảo tất cả các niêm phong bảo mật cao (bu-lông/cáp) đã được gắn đúng cách vào Công cụ Vận tải Quốc tế và đang vận hành như thiết kế. Quy trình này được gọi là quy trình VVTT: V – (View) Xem xét niêm phong và cơ chế khóa container; đảm bảo chúng bình thường; V – (Verify) Đối chiếu lại số niêm phong với các tài liệu vận chuyển cho chính xác; T – (Tug) Kéo thử niêm phong để đảm bảo nó được gắn đúng cách; T – (Twist and Turn) Vặn và xoay niêm phong bu lông để đảm bảo các bộ phận của nó không bị long ra, tách rời khỏi nhau hoặc bất kỳ phần nào của niêm phong bị lỏng.	Khi gắn niêm phong cáp, chúng cần bao bọc phần đáy hình chữ nhật của các thanh dọc để loại bỏ bất kỳ chuyển động lên hoặc xuống của niêm phong. Một khi đã gắn niêm phong, đảm bảo rằng cả hai phía của cáp không còn độ chùng nào. Quá trình VVTT với niêm phong cáp cần phải đảm bảo cáp được căng. Khi nó đã được gắn đúng cách, kéo và căng cáp để xác định xem cáp có trượt trong thân khóa không.	Phải

7. **<u>Bảo mật theo Thủ tục</u> –** Bảo mật theo Thủ tục bao gồm nhiều khía cạnh của quy trình xuất nhập khẩu, ghi hồ sơ và các yêu cầu lưu trữ và xử lý hàng hóa. Các tiêu chí thủ tục quan trọng khác liên quan đến báo cáo sự cố và thông báo cho cơ quan thực thi pháp luật thích hợp. Ngoài ra, CTPAT thường yêu cầu các quy trình được viết ra vì nó giúp duy trì quy trình thống nhất theo thời gian. Tuy nhiên, số lượng chi tiết cần thiết cho các thủ tục bằng văn bản này sẽ phụ thuộc vào các yếu tố khác nhau, chẳng hạn như mô hình kinh doanh của công ty hoặc những gì được quy trình này đề cập.

   CTPAT nhận thức rằng công nghệ được sử dụng trong chuỗi cung ứng tiếp tục thay đổi. Thuật ngữ được sử dụng trong các tiêu chí tham chiếu đến các thủ tục bằng văn bản, tài liệu và biểu mẫu, nhưng điều này không có nghĩa là chúng phải viết ra trên giấy. Tài liệu, chữ ký điện tử và các công nghệ kỹ thuật số khác được chấp nhận để đáp ứng các biện pháp này.

   Chương trình không được thiết kế để trở thành một mô hình với "một kích thước phù hợp với tất cả"; mỗi công ty phải quyết định (dựa trên đánh giá rủi ro của mình) cách thực hiện và duy trì các thủ tục. Tuy nhiên, sẽ hiệu quả hơn khi kết hợp các quy trình bảo mật vào các quy trình hiện có, thay vì tạo một hướng dẫn riêng cho các giao thức bảo mật. Điều này tạo ra một cấu trúc bền vững hơn và giúp nhấn mạnh rằng bảo mật chuỗi cung ứng là trách nhiệm của mọi người.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
7.1	Khi hàng hóa được sắp xếp qua đêm, hoặc trong một thời gian dài, phải có biện pháp để bảo đảm hàng hóa khỏi sự tiếp cận trái phép.		Phải
7.2	Các khu vực sắp xếp hàng hóa, và các khu vực lân cận, phải được kiểm tra thường xuyên để đảm bảo các khu vực này duy trì việc không có ô nhiễm dịch hại mà có thể nhìn thấy.	Các biện pháp phòng ngừa như sử dụng mồi, bẫy, hoặc các rào cản khác có thể được sử dụng khi cần thiết. Loại bỏ cỏ dại hoặc giảm thực vật phát triển quá mức có thể giúp loại bỏ môi trường sống dịch hại trong khu vực sắp xếp hàng.	Phải
7.4	Việc chất/đóng gói hàng hóa vào container/IIT cần được giám sát bởi nhân viên an ninh/quản lý hoặc nhân viên được chỉ định khác.		Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
7.5	Để làm bằng chứng được ghi nhận rằng niêm phong được gắn đúng cách, nên chụp hình ảnh kỹ thuật số tại điểm đóng hàng. Trong phạm vi khả thi, những hình ảnh này phải được chuyển tiếp điện tử cho điểm đến vì mục đích xác minh.	Bằng chứng hình ảnh có thể bao gồm các hình ảnh được chụp tại điểm đóng hàng để ghi lại bằng chứng về nhãn hàng hóa, quá trình đóng hàng, vị trí gắn niêm phong và niêm phong được gắn đúng cách.	Nên
7.6	Phải có sẵn các quy trình để đảm bảo mọi thông tin được sử dụng trong việc thông quan hàng hóa/vật phẩm là rõ ràng; hoàn chỉnh; chính xác; bảo vệ chống lại trao đổi, mất mát hoặc tạo ra thông tin sai lệch; và báo cáo đúng hạn.		Phải
7.7	Nếu sử dụng tài liệu giấy, các biểu mẫu và tài liệu khác liên quan đến xuất/nhập phải được bảo mật để ngăn chặn việc sử dụng trái phép.	Có thể thực hiện các biện pháp, như sử dụng tủ hồ sơ có khóa, để bảo mật việc lưu trữ các biểu mẫu chưa sử dụng, bao gồm các tờ khai, để ngăn chặn việc sử dụng trái phép tài liệu đó.	Nên
7.8	Người gửi hàng hoặc đại lý của mình phải đảm bảo rằng vận đơn (BOL) và/hoặc tờ khai phản ánh chính xác thông tin được cung cấp cho hãng vận chuyển và hãng vận chuyển phải thực hiện thẩm định để đảm bảo các tài liệu này là chính xác. BOL và tờ khai phải được nộp cho Cơ quan Hải quan và Bảo vệ Biên giới Hoa Kỳ (CBP) một cách kịp thời. Thông tin BOL nộp cho CBP phải cho thấy địa điểm/cơ sở nước ngoài đầu tiên nơi hãng vận chuyển tiếp nhận hàng hóa sẽ vận chuyển đến Hoa Kỳ. Trọng lượng và số lượng phải chính xác.	Khi nhận Công cụ Vận tải Quốc tế được niêm phong, hãng vận chuyển có thể dựa vào thông tin được cung cấp trong hướng dẫn vận chuyển của người gửi. Yêu cầu số niêm phong phải được in điện tử trên vận đơn (BOL) hoặc các tài liệu xuất khẩu khác giúp bảo vệ chống thay đổi niêm phong và thay đổi (các) tài liệu thích hợp để khớp với số niêm phong mới. Tuy nhiên, đối với một số chuỗi cung ứng nhất định, hàng hóa có thể được kiểm tra trong vận chuyển, bởi cơ quan Hải quan nước ngoài hoặc bởi CBP. Sau khi niêm phong bị phá vỡ bởi cơ quan chính phủ, cần phải có một quy trình để ghi lại số niêm phong mới gắn lên IIT sau khi kiểm tra. Trong một số trường hợp, có thể được viết tay.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
7.23	Thành viên CTPAT phải có các quy trình bằng văn bản để báo cáo sự cố, bao gồm mô tả về quy trình gia tăng cấp độ trong nội bộ của cơ sở. Phải có sẵn giao thức thông báo để báo cáo bất kỳ hoạt động đáng ngờ hoặc sự cố bảo mật nào (chẳng hạn như bắt giữ ma túy, phát hiện người trốn trong hàng, v.v.) diễn ra ở bất cứ đâu trên thế giới và ảnh hưởng đến an ninh của chuỗi cung ứng của thành viên. Khi có thể, Thành viên phải báo cáo bất kỳ sự cố toàn cầu nào cho Chuyên gia bảo mật chuỗi cung ứng của mình, cảng gần nhất, bất kỳ cơ quan thực thi pháp luật thích hợp nào và các đối tác kinh doanh có thể là một phần của chuỗi cung ứng bị ảnh hưởng. Thông báo cho CBP phải được thực hiện càng sớm càng tốt và trước khi có bất kỳ phương tiện vận chuyển hoặc IIT nào vượt qua biên giới. Thủ tục thông báo phải bao gồm thông tin liên lạc chính xác, liệt kê tên và số điện thoại của nhân viên cần thông báo, cũng như cho các cơ quan thực thi pháp luật. Các thủ tục phải được xem xét định kỳ để đảm bảo thông tin liên lạc là chính xác.	Ví dụ về các sự cố cần thông báo cho cơ quan Hải quan và Bảo vệ Biên giới Hoa Kỳ bao gồm (nhưng không giới hạn ở) những điều sau đây: • Phát hiện có can thiệp vào container/IIT hoặc niêm phong bảo mật cao; • Khám phá một khoang ẩn trong phương tiện vận chuyển hoặc IIT; • Một niêm phong mới chưa được ghi nhận được gắn lên IIT; • Buôn lậu hàng lậu , kể cả người; người trốn theo hàng; • Nhập trái phép vào phương tiện vận chuyển, đầu máy xe lửa, tàu hoặc tàu sân bay; • Tống tiền, trả tiền để được bảo vệ, đe dọa và/hoặc dọa nạt; • Sử dụng trái phép số nhận dạng doanh nghiệp (ví dụ: số Nhà nhập khẩu đã đăng ký (IOR), mã Alpha Hãng vận chuyển (SCAC), v.v.).	Phải
7.24	Phải có sẵn các thủ tục để xác định, truy vấn và giải quyết những người không được ủy quyền/không xác định. Nhân viên phải biết giao thức để truy vấn một người chưa biết/không được phép, cách ứng phó với tình huống và làm quen với quy trình đưa một cá nhân trái phép ra khỏi cơ sở.		Phải
7.25	Thành viên CTPAT nên thiết lập một cơ chế để báo cáo ẩn danh các vấn đề liên quan đến bảo mật. Một khi nhận được một cáo buộc, cần phải điều tra và nếu có thể, cần thực hiện các hành động khắc phục.	Các vấn đề nội bộ như trộm cắp, gian lận và âm mưu nội bộ có thể được báo cáo dễ dàng hơn nếu bên báo cáo biết vấn đề có thể được báo cáo ẩn danh. Thành viên có thể thiết lập một chương trình đường dây nóng hoặc cơ chế tương tự cho phép mọi người ẩn danh nếu họ sợ bị trả thù vì hành động của họ. Chúng tôi đề nghị rằng mọi báo cáo phải được	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
		giữ làm bằng chứng để chứng minh rằng mỗi sự việc báo cáo đã được điều tra và các hành động khắc phục đã được thực hiện.	
7.27	Tất cả sự thiếu hụt, quá tải và những khác biệt hoặc bất thường quan trọng khác phải được điều tra và giải quyết, khi thích hợp.		Phải
7.28	Hàng hóa đến nên được đối chiếu với thông tin trên bảng kê khai hàng hóa. Hàng gửi đi nên được xác minh đối chiếu với các đơn đặt hàng hoặc giao hàng.		Nên
7.29	Số niêm phong được chỉ định cho các lô hàng cụ thể nên được truyền đến người nhận hàng trước khi khởi hành.		Nên
7.30	Số niêm phong nên được in điện tử trên vận đơn hoặc chứng từ vận chuyển khác.		Nên
7.37	Sau một sự cố an ninh nghiêm trọng, các Thành viên phải khởi xướng một cuộc phân tích hậu sự cố ngay sau khi biết được sự cố, nhằm xác định nơi chuỗi cung ứng có thể bị xâm phạm. Phân tích này không được cản trở/can thiệp vào bất kỳ cuộc điều tra nào được thực hiện bởi cơ quan thực thi pháp luật. Kết quả phân tích hậu sự cố của công ty phải được ghi lại, hoàn tất sớm nhất theo khả năng có thể, và, nếu được cơ quan thực thi pháp luật cho phép, cung cấp cho các Chuyên gia An ninh Chuỗi cung ứng (SCSS) theo yêu cầu.	Một sự cố bảo mật được định nghĩa là một sự xâm phạm, trong đó các biện pháp an ninh đã bị phá vỡ, tránh né hoặc vi phạm, và đã hoặc sẽ dẫn đến một hành vi tội phạm. Các sự cố bảo mật bao gồm các hành vi khủng bố, buôn lậu (ma túy, người, v.v.) và có người đi lậu trên tàu.	Phải

8. **<u>An ninh Nông nghiệp</u> –** Nông nghiệp là ngành tạo việc làm lớn nhất ở Mỹ. Đây cũng là ngành bị đe dọa bởi sự ô nhiễm của động vật và thực vật đưa từ nước ngoài vào như đất, phân, hạt giống và vật chất động, thực vật có thể gây hại, dung dưỡng sâu bệnh xâm nhập và phá hoại. Loại bỏ chất gây ô nhiễm trong tất cả các phương tiện vận chuyển và trong tất cả các loại hàng hóa có thể làm giảm thời gian lưu hàng ở CBP, giảm chậm trễ, giảm lượng hàng hóa trả về hoặc phải xử lý. Đảm bảo tuân thủ các yêu cầu nông nghiệp của CTPAT cũng sẽ giúp bảo vệ một ngành kinh tế chính yếu của Hoa Kỳ và nguồn cung thực phẩm toàn cầu nói chung.

Định nghĩa Chính: Ô nhiễm dịch hại – Tổ chức Hàng hải Quốc tế định nghĩa ô nhiễm dịch hại là các dạng động vật, côn trùng hoặc động vật không xương sống khác (còn sống hoặc đã chết, trong bất kỳ giai đoạn vòng đời nào, bao gồm vỏ trứng hoặc ấu trùng) hoặc bất kỳ vật chất hữu cơ nào có nguồn gốc động vật (bao gồm cả máu, xương, lông, thịt, dịch tiết, bài tiết); thực vật có thể nẩy mầm hoặc không thể nẩy mầm hoặc các sản phẩm thực vật (bao gồm trái cây, hạt, lá, cành, rễ, vỏ cây); hoặc vật chất hữu cơ khác, bao gồm cả nấm; hoặc đất, hoặc nước; ở đó các sản phẩm này không phải là hàng hóa được liệt kê trong các Công cụ Vận tải Quốc tế (ví dụ như container, thiết bị tải hàng, v.v.).

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
8.1	Các Thành viên CTPAT, theo đúng mô hình kinh doanh của họ, phải có các quy trình bằng văn bản được thiết kế để ngăn ngừa ô nhiễm dịch hại có thể nhìn thấy, bao gồm việc tuân thủ các quy định về vật liệu đóng hàng bằng gỗ (WPM). Các biện pháp phòng trừ dịch hại hữu hình phải được tuân thủ trong toàn bộ chuỗi cung ứng. Các biện pháp liên quan đến WPM phải đáp ứng Tiêu chuẩn quốc tế đối với các biện pháp kiểm dịch thực vật số 15 (ISPM 15) của Công	WPM được định nghĩa là gỗ hoặc sản phẩm gỗ (không bao gồm các sản phẩm giấy) được sử dụng để hỗ trợ, bảo vệ hoặc vận chuyển hàng hóa. WPM bao gồm các mặt hàng như pallet, thùng, hộp, cuộn và chèn lót. Thông thường, các mặt hàng này được làm bằng gỗ thô có thể chưa trải qua quá trình xử lý hoặc xử lý chưa đủ để loại bỏ hoặc tiêu diệt sâu bệnh, và do đó vẫn là một phương tiện cho sâu bệnh xâm nhập và lây lan. Vật chèn lót nói riêng đã được chứng minh là có nguy cơ cao để sâu bệnh xâm nhập và lây lan. IPPC là một hiệp ước đa phương được giám sát bởi Tổ chức Lương thực và Nông nghiệp của Liên Hợp Quốc nhằm bảo đảm sự phối hợp, hành động hiệu quả để ngăn chặn và kiểm soát việc xâm nhập và lây lan các loài gây hại và ô nhiễm. ISPM 15 bao gồm các biện pháp được quốc tế chấp nhận có thể được áp dụng cho WPM để giảm đáng kể nguy cơ xâm nhập và lây lan của hầu hết các loài gây hại có liên quan đến WPM. ISPM 15 ảnh hưởng đến tất cả các vật liệu đóng hàng bằng gỗ, yêu cầu chúng phải được cạo sạch vỏ và sau đó được xử lý nhiệt hoặc khử trùng bằng methyl bromide và được đóng dấu hoặc gắn nhãn hiệu tuân thủ IPPC. Dấu hiệu tuân thủ này được gọi không chính thức là "tem lúa mì". Các sản phẩm được miễn trừ ISPM 15 được làm từ các vật liệu thay thế, như các sản phẩm giấy, kim loại, nhựa hoặc ván gỗ (ví dụ: ván sợi định hướng, ván cứng và ván ép).	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	ước bảo vệ thực vật quốc tế (IPPC).		

Lĩnh vực Tập trung Thứ ba: An ninh Thực thể và Con người

9. <u>An ninh Thực thể</u> – Cơ sở lưu trữ và xử lý hàng hóa, nơi lưu giữ Công cụ Vận tải Quốc tế và các cơ sở nơi chuẩn bị tài liệu xuất nhập khẩu ở các địa điểm trong và ngoài nước phải có hàng rào chắn và các biện pháp ngăn chặn việc tiếp cận trái phép.

Một trong những nền tảng của CTPAT là tính linh hoạt và các chương trình bảo mật nên được điều chỉnh để phù hợp với hoàn cảnh của mỗi công ty. Nhu cầu an ninh thực thể có thể thay đổi rất đa dạng dựa trên vai trò của Thành viên trong chuỗi cung ứng, mô hình kinh doanh và mức độ rủi ro. Các tiêu chí an ninh thực thể cung cấp một số biện pháp ngăn chặn/chướng ngại sẽ giúp ngăn chặn việc tiếp cận không được phép với hàng hóa, thiết bị nhạy cảm và/hoặc thông tin, và Thành viên nên sử dụng các biện pháp bảo mật này trong toàn chuỗi cung ứng của mình.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
9.1	Tất cả các cơ sở xử lý và lưu trữ hàng hóa, bao gồm bãi xe kéo và văn phòng phải có hàng rào chắn và/hoặc các biện pháp ngăn chặn tiếp cận trái phép.		Phải
9.2	Hàng rào chu vi nên bao bọc các khu vực xung quanh các cơ sở xử lý và lưu trữ hàng hóa. Nếu một cơ sở dùng để xử lý hàng hóa, nên có thêm hàng rào bên trong để bảo vệ hàng hóa và khu vực xử lý hàng hóa. Dựa trên rủi ro, hàng rào bổ sung bên trong nên tách biệt các loại hàng hóa khác nhau như hàng trong nước, quốc tế, giá trị cao và/hay hàng nguy hiểm. Hàng rào nên được nhân viên được chỉ định kiểm tra thường xuyên về tính toàn vẹn cũng như việc hư hại. Nếu phát hiện hư hại trên hàng rào, nên tiến hành sửa chữa càng sớm càng tốt.	Các rào cản chấp nhận được khác có thể được sử dụng thay cho hàng rào, chẳng hạn như tường ngăn cách hoặc các phần mang tính tự nhiên không thể thâm nhập hoặc cản trở việc xâm nhập như vách đá dốc hoặc cây cối dày đặc.	Nên
9.4	Cổng có phương tiện và/hoặc nhân viên đi vào hoặc ra (cũng như các điểm vào ra khác) phải có người trông coi hoặc được giám sát. Cá nhân và phương tiện có thể bị lục soát theo luật địa phương và luật lao động.	Số lượng cổng nên được giữ ở mức tối thiểu chỉ khi cần vào, ra phù hợp và an toàn. Các điểm vào ra khác là lối vào cơ sở không có cổng.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
9.5	Xe chở khách tư nhân nên bị cấm đậu trong hoặc liền kề với khu vực xử lý và lưu trữ hàng hóa, và phương tiện vận chuyển.	Ấn định khu vực đỗ xe bên ngoài khu vực có hàng rào và/hoặc khu vực hoạt động - hoặc ít nhất có khoảng cách đáng kể từ khu vực xử lý và lưu trữ hàng hóa.	Nên
9.6	Ánh sáng đầy đủ phải được cung cấp bên trong và bên ngoài cơ sở, bao gồm, tùy tình hình, các khu vực sau: lối vào và lối ra, khu vực lưu trữ và xử lý hàng hóa, hàng rào và khu vực đỗ xe.	Bộ hẹn giờ tự động hoặc cảm biến ánh sáng tự động bật đèn an ninh thích hợp là những bổ sung hữu ích cho hệ thống chiếu sáng.	Phải
9.7	Công nghệ bảo mật nên được sử dụng để giám sát các cơ sở và ngăn chặn tiếp cận trái phép các khu vực nhạy cảm.	Công nghệ bảo mật điện tử được sử dụng để bảo vệ/giám sát các khu vực nhạy cảm và các điểm tiếp cận bao gồm: hệ thống báo động trộm (hàng rào và bên trong), còn được gọi là Hệ thống Phát hiện Xâm nhập (IDS); thiết bị kiểm soát truy cập; và hệ thống giám sát video (VSS) - bao gồm Camera Quan sát Mạch kín (CCTV). Một hệ thống CCTV/VSS có thể bao gồm các thành phần như camera thường (dùng cáp), camera dựa trên giao thức Internet (IP) (dùng mạng), các thiết bị ghi âm, và phần mềm quản lý video. Các khu vực được bảo vệ/nhạy cảm, cần được giám sát video, có thể bao gồm: khu vực lưu trữ và xử lý hàng hóa, khu vực vận chuyển/nhận hàng, nơi lưu giữ tài liệu nhập khẩu , máy chủ CNTT, khu vực sân bãi và kho lưu trữ cho các Công cụ Vận tải Quốc tế (IIT), khu vực IIT được kiểm tra, và các khu vực lưu trữ niêm phong.	Nên
9.8	Các thành viên dựa vào công nghệ bảo mật để bảo vệ thực thể phải có các chính sách và quy trình bằng văn bản điều chỉnh việc sử dụng, bảo trì và bảo vệ công nghệ này. Tối thiểu, các chính sách và thủ tục này phải quy định: • Việc vào ra các địa điểm nơi công nghệ này được kiểm soát hoặc quản lý chỉ giới hạn ở nhân viên được ủy quyền; • Các quy trình đã được thực hiện để kiểm tra/giám sát công nghệ một cách thường xuyên;	Công nghệ bảo mật cần phải được kiểm tra một cách thường xuyên để đảm bảo nó hoạt động tốt. Có các hướng dẫn chung để tuân theo: • Kiểm tra hệ thống bảo mật sau khi thực hiện bất kỳ công việc bảo trì nào; trong và sau khi sửa chữa lớn, chỉnh sửa hoặc xây thêm cho tòa nhà hoặc cơ sở. Các thành phần của một hệ thống có thể đã bị xâm phạm, cố ý hoặc vô ý. • Kiểm tra hệ thống bảo mật sau khi có bất kỳ thay đổi lớn nào đối với dịch vụ điện thoại hoặc internet. Bất cứ điều gì có thể ảnh hưởng đến khả năng giao tiếp của hệ thống với trung tâm giám sát đều phải được kiểm tra lại. • Đảm bảo các cài đặt video như ghi hình khi có chuyển động kích	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
	• Việc kiểm tra bao gồm xác minh rằng tất cả các thiết bị đều hoạt động tốt và tùy trường hợp, thiết bị được đặt đúng vị trí; • Kết quả kiểm tra và kiểm tra hiệu suất được ghi hồ sơ; • Nếu cần có hành động khắc phục, cần được thực hiện càng sớm càng tốt và các biện pháp khắc phục được ghi hồ sơ; • Các kết quả được ghi hồ sơ từ các cuộc kiểm tra phải được lưu giữ trong một thời gian đủ cho mục đích kiểm toán. Nếu sử dụng trạm giám sát trung tâm của bên thứ ba (bên ngoài cơ cở), Thành viên CTPAT phải có các quy trình bằng văn bản quy định các chức năng hệ thống chính yếu và các giao thức xác thực như (nhưng không giới hạn đối với) thay đổi mã bảo mật, thêm hoặc bớt nhân viên được ủy quyền, sửa đổi mật khẩu, và truy cập hoặc từ chối cho vào hệ thống. Các chính sách và quy trình công nghệ bảo mật phải được xem xét và cập nhật hàng năm, hoặc thường xuyên hơn, tùy mức độ rủi ro hoặc hoàn cảnh.	hoạt hệ thống; cảnh báo phát hiện chuyển động; hình ảnh mỗi giây (IPS) và mức chất lượng, đã được thiết lập đúng đắn. • Đảm bảo ống kính camera (hoặc vòm bảo vệ camera) sạch sẽ và ống kính đúng tiêu cự. Tầm nhìn không để bị giới hạn bởi chướng ngại vật hoặc ánh đèn sáng chói. • Kiểm tra để đảm bảo camera an ninh được đặt đúng vị trí và giữ đúng vị trí (camera có thể đã bị cố ý hoặc vô tình di chuyển).	
9.9	Thành viên CTPAT nên sử dụng các nguồn lực có giấy phép/được chứng nhận khi cân nhắc thiết kế và cài đặt công nghệ bảo mật.	Công nghệ bảo mật ngày nay rất phức tạp và phát triển nhanh chóng. Thông thường các công ty mua công nghệ bảo mật sai, hoạt động không hiệu quả khi cần và/hoặc trả tiền nhiều hơn mức cần thiết. Tìm kiếm hướng dẫn có chất lượng sẽ giúp người mua chọn các tùy chọn công nghệ phù hợp với nhu cầu và ngân sách của họ. Theo Hiệp hội các nhà thầu điện tử quốc gia (NECA), tại Hoa Kỳ 33 tiểu bang hiện đòi hỏi giấy phép hành nghề cho các chuyên gia tham gia lắp đặt hệ thống an ninh và báo động.	Nên
9.10	Tất cả các cơ sở hạ tầng công nghệ bảo mật phải được bảo mật về mặt vật lý khỏi sự tiếp cận trái phép.	Cơ sở hạ tầng công nghệ bảo mật bao gồm máy tính, phần mềm bảo mật, bảng điều khiển điện tử, video giám sát hoặc camera ghi hình	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
		mạch kín, các bộ phận nguồn và ổ cứng cho camera, cũng như ghi âm.	
9.11	Các hệ thống công nghệ bảo mật nên được lắp đặt với một nguồn năng lượng thay thế, cho phép hệ thống tiếp tục hoạt động trong trường hợp bất ngờ mất điện trực tiếp.	Tội phạm tìm cách xâm nhập hệ thống an ninh có thể cố gắng vô hiệu hóa nguồn điện cho hệ thống bảo mật để thực hiện ý đồ. Do đó, điều quan trọng là phải có một nguồn năng lượng thay thế cho hệ thống bảo mật. Nguồn điện thay thế có thể là nguồn phát điện phụ hoặc pin dự phòng. Máy phát điện dự phòng cũng có thể được sử dụng cho các hệ thống quan trọng khác như chiếu sáng.	Nên
9.12	Nếu hệ thống camera được triển khai, camera phải giám sát các cơ sở và khu vực nhạy cảm để ngăn chặn tiếp cận trái phép. Nên sử dụng báo động để cảnh báo cho công ty việc tiếp cận trái phép các khu vực nhạy cảm.	Các khu vực nhạy cảm, tùy tình hình, có thể bao gồm khu vực lưu trữ và xử lý hàng hóa, khu vực vận chuyển/nhận hàng, nơi lưu giữ chứng từ nhập khẩu, máy chủ CNTT, sân bãi và khu vực lưu trữ Công cụ Vận tải Quốc tế (IIT), khu vực kiểm tra IIT và khu vực lưu trữ niêm phong.	Nên
9.13	Nếu hệ thống camera được triển khai, camera phải được định vị để bao quát các khu vực chính của các cơ sở liên quan đến quá trình nhập/xuất khẩu. Camera nên được lập trình để ghi hình với chất lượng hình ảnh cao nhất ở mức có sẵn và được cài đặt để ghi hình 24/7.	Định vị chính xác các camera là rất quan trọng để cho phép các camera ghi lại càng nhiều càng tốt các giai đoạn giao nhận thực tế trong phạm vi kiểm soát của cơ sở. Dựa trên rủi ro, các khu vực hoặc quy trình chính có thể bao gồm khu vực xử lý và lưu trữ hàng hóa; vận chuyển/nhận hàng; quá trình đóng hàng; quá trình niêm phong; phương tiện vận chuyển đến/đi; máy chủ CNTT; kiểm tra container (an ninh và nông nghiệp); lưu trữ niêm phong; và bất kỳ lĩnh vực nào khác liên quan đến việc đảm bảo các lô hàng quốc tế.	Phải
9.14	Nếu các hệ thống camera được triển khai, các camera nên có tính năng báo động/thông báo, sẽ báo hiệu sự cố "không hoạt động/ghi hình".	Hệ thống giám sát video ngưng hoạt động có thể là kết quả của việc ai đó vô hiệu hóa hệ thống để xâm phạm chuỗi cung ứng mà không để lại bằng chứng video về tội phạm. Chức năng không hoạt động có thể tạo ra một thông báo điện tử được gửi đến (các) nhân sự được chỉ định trước thông báo cho họ rằng thiết bị cần được sửa chữa ngay lập tức.	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
9.15	Nếu hệ thống camera được triển khai, phải tiến hành xem ngẫu nhiên, một cách định kỳ, các cảnh quay camera (bởi ban quản lý, an ninh hoặc nhân viên được chỉ định khác) để xác minh rằng các quy trình an ninh hàng hóa đang được tuân thủ đúng theo quy định của pháp luật. Kết quả của các lần xem video phải được tóm tắt bằng văn bản để bao gồm mọi hành động khắc phục được thực hiện. Các kết quả phải được lưu trữ trong một thời gian đủ dài cho mục đích kiểm toán.	Nếu cảnh quay camera chỉ được xem khi có sự cố (như một phần của cuộc điều tra sau khi vi phạm an ninh, v.v.), thì không phát huy được toàn bộ lợi ích của việc gắn camera. Camera không chỉ là công cụ điều tra. Nếu sử dụng một cách chủ động, chúng có thể giúp ngăn chặn vi phạm an ninh xảy ra ngay từ đầu. Tập trung xem ngẫu nhiên các cảnh quay giao nhận thực tế để đảm bảo lô hàng được an toàn và tất cả các giao thức bảo mật được tuân thủ. Một số ví dụ về các quy trình có thể được xem xét như sau: • Hoạt động xử lý hàng hóa; • Kiểm tra container; • Quá trình đóng hàng; • Quy trình niêm phong; • Phương tiện vận chuyển đến/đi; và • Hàng khởi hành, v.v. **Mục đích của việc xem video:** Việc xem video là nhằm để đánh giá sự tuân thủ và hiệu quả chung của các quy trình bảo mật được thiết lập, xác định lỗ hổng hoặc yếu kém đã nhận ra, và đưa ra hành động khắc phục để hỗ trợ cải thiện các quy trình an ninh. Dựa trên rủi ro (sự cố trước đây hoặc báo cáo ẩn danh về nhân viên không tuân theo các giao thức bảo mật tại bến đóng hàng, v.v.), Thành viên có thể nhắm đến mục tiêu xem định kỳ. **Các mục cần bao gồm trong bản tóm tắt bằng văn bản**: • Ngày xem; • Ngày của đoạn phim được xem; • Camera/khu vực nào được ghi hình; • Mô tả ngắn gọn về bất kỳ phát hiện nào; và • Hành động khắc phục, nếu cần thiết.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
9.16	Nếu sử dụng camera, các bản ghi cảnh quay các quá trình xuất/nhập khẩu chính đối với các lô hàng được giám sát phải được lưu giữ trong một thời gian đủ để cho phép một cuộc điều tra được hoàn thành.	Nếu xảy ra sự cố xâm phạm, cần tiến hành một cuộc điều tra và việc lưu giữ các cảnh quay camera bao quát việc đóng hàng (để xuất khẩu) và quá trình đóng hàng/niêm phong sẽ rất quan trọng trong việc khám phá khâu nào trong chuỗi cung ứng có thể bị can thiệp. Đối với giám sát, chương trình CTPAT khuyến nghị cho phép ít nhất là 14 ngày sau khi một lô hàng đã về đến điểm đầu tiên của quá trình phân phối. Đây là nơi container được mở đầu tiên sau khi làm thủ tục hải quan.	Nên

10. <u>Kiểm soát tiếp cận vật chất</u> – Kiểm soát tiếp cận ngăn chặn tiếp cận trái phép vào các cơ sở/khu vực, giúp duy trì quyền kiểm soát nhân viên và khách và bảo vệ tài sản của công ty. Kiểm soát tiếp cận bao gồm nhận dạng tất cả nhân viên, khách, nhà cung cấp dịch vụ và nhà bán hàng tại tất cả các điểm đi vào.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
10.1	Thành viên CTPAT phải có các quy trình bằng văn bản về cách các thẻ nhận dạng và thiết bị tiếp cận được cấp, thay đổi và xóa. Khi thích hợp, phải có sẵn một hệ thống nhận dạng nhân sự cho các mục đích nhận dạng và kiểm soát tiếp cận. Tiếp cận vào các khu vực nhạy cảm phải được hạn chế dựa trên mô tả công việc hoặc nhiệm vụ được giao. Việc loại bỏ các thiết bị tiếp cận phải diễn ra khi các nhân viên rời bỏ công ty.	Các thiết bị tiếp cận bao gồm thẻ nhận dạng nhân viên, thẻ tạm thời của khách và nhà bán hàng, hệ thống nhận dạng sinh trắc học, thẻ khóa gần, mã và khóa. Khi nhân viên nghỉ việc ở công ty, việc sử dụng danh sách kiểm tra khi ra giúp đảm bảo rằng tất cả các thiết bị tiếp cận đã được trả lại và/hoặc bị vô hiệu hóa. Đối với các công ty nhỏ hơn, nơi nhân sự biết nhau, không cần hệ thống nhận dạng. Nói chung, đối với một công ty có hơn 50 nhân viên, cần có một hệ thống nhận dạng.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
10.2	Khách, nhà bán hàng và nhà cung cấp dịch vụ phải xuất trình giấy tờ tùy thân có ảnh khi đến và phải có sổ trực để ghi lại các chi tiết của chuyến thăm. Tất cả khách nên có người đi kèm. Ngoài ra, tất cả khách và nhà cung cấp dịch vụ nên được cấp giấy tờ nhận dạng tạm thời. Nếu nhận dạng tạm thời được sử dụng, nó phải được hiển thị rõ ràng mọi lúc trong chuyến thăm. Sổ đăng ký phải bao gồm các mục sau: • Ngày thăm; • Tên của khách; • Xác minh giấy tờ nhận dạng có ảnh (loại được xác minh như giấy phép lái xe hoặc thẻ căn cước quốc gia). Khách tiếp cận thường xuyên, đã biết như nhà bán hàng thường xuyên có thể bỏ qua kiểm tra giấy tờ nhận dạng có ảnh, nhưng vẫn phải đăng ký vào và ra khỏi cơ sở; • Thời điểm đến; • Người liên lạc của công ty; và • Thời điểm ra về.		Phải
10.3	Người lái xe giao hoặc nhận hàng phải được xác minh trước khi nhận hoặc trả hàng. Các tài xế phải xuất trình giấy tờ tùy thân có ảnh do chính phủ cấp cho nhân viên của cơ sở cấp quyền tiếp cận để xác minh danh tính của họ. Nếu việc xuất trình giấy tờ tùy thân có ảnh do chính phủ cấp là không khả thi, nhân viên của cơ sở có thể chấp nhận một hình thức nhận dạng ảnh có thể nhận ra được do công ty vận tải đường bộ nơi tuyển dụng tài xế phát hành.		Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
10.4	Phải có một sổ nhận hàng hóa để đăng ký lái xe và ghi lại các chi tiết về phương tiện vận chuyển của họ khi lấy hàng. Khi lái xe đến nhận hàng tại một cơ sở, nhân viên của cơ sở phải ghi nhận trong sổ trực nhận hàng. Khi ra về, lái xe phải được đăng xuất. Sổ hàng hóa phải được giữ an toàn và lái xe không được phép tiếp cận nó. Sổ nhận hàng cần ghi lại các mục sau: • Tên tài xế; • Ngày và giờ đến; • Chủ lao động; • Số xe tải; • Số xe kéo; • Thời điểm ra về; • Số niêm phong được gắn vào lô hàng tại thời điểm khởi hành.	Có thể sử dụng sổ ghi nhận khách làm sổ hàng hóa miễn là có ghi thông tin bổ sung vào sổ.	Phải
10.7	Trước khi đến, hãng vận chuyển cần thông báo cho cơ sở về thời gian dự kiến đến nhận hàng theo lịch trình, tên của tài xế và số xe tải. Khi khả thi về mặt thực hiện, Thành viên CTPAT chỉ nên cho phép giao hàng và nhận hàng theo lịch hẹn.	Tiêu chí này sẽ giúp chủ hàng và hãng vận chuyển tránh những lần nhận hàng không có thật. Nhận hàng không có thật là mánh lới tội phạm dẫn đến hành vi trộm cắp hàng hóa bằng cách lừa đảo bao gồm các tài xế xe tải sử dụng căn cước giả và/hoặc các doanh nghiệp ma được lập nên cho mục đích trộm cắp hàng hóa. Khi một hãng vận chuyển có tài xế thường xuyên nhận hàng từ một cơ sở nhất định, cách tốt là cơ sở đó sẽ duy trì một danh sách các tài xế có hình ảnh của họ. Do đó, nếu không thể cho công ty biết tài xế nào sẽ đến, công ty vẫn có thể xác minh rằng tài xế được chấp thuận nhận hàng từ cơ sở.	Nên
10.8	Các bưu kiện và thư đến nên được kiểm tra định kỳ về chuyện hàng lậu trước khi nhận.	Ví dụ về hàng lậu như vậy bao gồm, nhưng không giới hạn đối với chất nổ, ma túy bất hợp pháp và tiền mặt.	Nên

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
10.10	Nếu có sử dụng nhân viên bảo vệ, hướng dẫn làm việc cho nhân viên bảo vệ phải được đưa vào các chính sách và quy trình bằng văn bản. Ban quản lý phải định kỳ xác minh sự tuân thủ và sự thích hợp của các thủ tục này thông qua kiểm toán và đánh giá chính sách.	Mặc dù nhân viên bảo vệ có thể được tuyển vào bất kỳ cơ sở nào, nhưng họ thường được tuyển dụng cho các địa điểm sản xuất, cảng biển, trung tâm phân phối, kho lưu trữ cho các Công cụ Vận tải Quốc tế, các điểm hoạt động của bên gom hàng và bên giao nhận.	Phải

11. <u>An ninh Nhân sự</u> – Lực lượng nhân sự của một công ty là một trong những tài sản quan trọng nhất, nhưng đây cũng có thể là một trong những khâu bảo mật yếu nhất. Các tiêu chí trong danh mục này tập trung vào các vấn đề như sàng lọc nhân viên và xác minh trước khi tuyển dụng. Nhiều vi phạm an ninh được gây ra bởi các âm mưu nội bộ, đó là nơi một hoặc nhiều nhân viên thông đồng để phá vỡ các thủ tục bảo mật nhằm cho phép xâm nhập vào chuỗi cung ứng. Do đó, Thành viên phải thực hiện thẩm định để xác minh rằng nhân viên đảm nhiệm các vị trí nhạy cảm là đáng tin cậy. Vị trí nhạy cảm bao gồm nhân viên làm việc trực tiếp với hàng hóa hay hồ sơ hàng hóa, cũng như nhân viên liên quan đến việc kiểm soát tiếp cận vào các khu vực hoặc thiết bị nhạy cảm. Những vị trí này bao gồm, nhưng không giới hạn đối với việc vận chuyển, tiếp nhận, nhân viên phòng văn thư, tài xế, liên lạc viên, nhân viên bảo vệ, bất kỳ cá nhân nào liên quan đến việc đóng hàng, theo dõi phương tiện vận chuyển và/hoặc kiểm soát niêm phong.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
11.1	Phải có sẵn các quy trình bằng văn bản để sàng lọc các nhân viên tương lai và kiểm tra định kỳ các nhân viên hiện tại. Thông tin xin việc, như lịch sử việc làm và người giới thiệu, phải được xác minh trước khi tuyển dụng, trong phạm vi có thể và được cho phép theo luật.	CTPAT nhận thức được rằng luật lao động và quyền riêng tư ở một số quốc gia nhất định có thể không cho phép tất cả các thông tin xin việc được xác minh. Tuy nhiên, cần thẩm định để xác minh thông tin xin việc khi được phép.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
11.2	Thể theo các giới hạn pháp lý thích hợp và sự sẵn có của cơ sở dữ liệu hồ sơ tội phạm, nên tiến hành kiểm tra lý lịch nhân viên. Dựa trên độ nhạy cảm của vị trí, các yêu cầu kiểm tra nhân viên nên mở rộng cho lực lượng lao động và nhà thầu tạm thời. Sau khi được tuyển dụng, việc tái thẩm tra định kỳ nên được thực hiện dựa trên vụ việc và/hoặc độ nhạy cảm của vị trí nhân viên. Rà soát lý lịch nhân viên nên bao gồm xác minh nhận dạng của người lao động và tiền sử tội phạm, bao quát các cơ sở dữ liệu của thành phố, tiểu bang, tỉnh, và cả nước. Thành viên CTPAT và các đối tác kinh doanh của họ nên lưu ý kết quả kiểm tra lý lịch, như được cho phép bởi các đạo luật địa phương, khi đưa ra quyết định tuyển dụng. Kiểm tra lý lịch không giới hạn vào việc xác minh nhận dạng và tiền sử tội phạm. Trong các lĩnh vực có rủi ro lớn hơn, có thể cần điều tra sâu hơn.		Nên
11.5	Thành viên CTPAT phải có Bộ Quy tắc ứng xử của nhân viên bao gồm các kỳ vọng và xác định các hành vi được chấp nhận. Hình phạt và quy trình kỷ luật phải được đưa vào Bộ Quy tắc ứng xử. Nhân viên/nhà thầu phải xác nhận rằng họ đã đọc và hiểu Bộ Quy tắc ứng xử bằng cách ký tên, và xác nhận này phải được lưu trong hồ sơ của nhân viên để làm tài liệu.	Bộ Quy tắc ứng xử giúp bảo vệ doanh nghiệp và thông báo cho nhân viên về những kỳ vọng. Mục đích của nó là phát triển và duy trì một tiêu chuẩn ứng xử được công ty chấp nhận. Nó giúp công ty phát triển một hình ảnh chuyên nghiệp và thiết lập một văn hóa đạo đức mạnh mẽ. Ngay cả một công ty nhỏ cũng cần phải có Bộ Quy tắc ứng xử; tuy nhiên, không cần phải được thiết kế tỉ mỉ hoặc chứa thông tin phức tạp.	Phải

12. <u>Giáo dục, Đào tạo và Nhận thức</u> – Tiêu chí bảo mật của CTPAT được thiết kế để làm cơ sở cho hệ thống bảo mật nhiều lớp. Nếu một lớp bảo mật bị vượt qua, một lớp khác sẽ ngăn chặn vi phạm bảo mật hoặc cảnh báo cho công ty về vi phạm. Việc thực hiện và duy trì một chương trình bảo mật nhiều lớp cần có sự tham gia và hỗ trợ tích cực của một số phòng ban và nhiều nhân sự khác nhau. Một trong những khía cạnh quan trọng để duy trì một chương trình bảo mật là đào tạo. Giáo dục nhân viên về các mối đe dọa là gì và vai trò của họ là quan trọng như thế nào trong việc bảo vệ chuỗi cung ứng của công ty là một khía cạnh quan trọng đối với sự thành công và sự bền vững của chương trình bảo mật chuỗi cung ứng. Hơn nữa, khi nhân viên hiểu tại sao các quy trình bảo mật được áp dụng, họ có thể sẽ tuân thủ chúng hơn.

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
12.1	Các thành viên phải thiết lập và duy trì chương trình đào tạo và nhận thức về an ninh để nhận ra và bồi dưỡng nhận thức về các lỗ hổng an ninh đối với các cơ sở, phương tiện vận chuyển và hàng hóa tại mỗi điểm trong chuỗi cung ứng, mà có thể bị những kẻ khủng bố hoặc buôn lậu khai thác. Chương trình đào tạo phải toàn diện và đáp ứng tất cả các yêu cầu bảo mật của CTPAT. Nhân viên ở các vị trí nhạy cảm phải được đào tạo chuyên môn bổ sung, hướng đến các trách nhiệm mà vị trí đó nắm giữ. Một trong những khía cạnh quan trọng của chương trình bảo mật là đào tạo. Nhân viên hiểu tại sao phải đưa ra các biện pháp an ninh thì có nhiều khả năng họ tuân thủ chúng hơn. Đào tạo an ninh phải được cung cấp cho nhân viên, theo yêu cầu, dựa trên chức năng và vị trí của họ một cách thường xuyên, và nhân viên mới được tuyển dụng phải được đào tạo như một phần của đào tạo kỹ năng công việc/định hướng cho họ. Thành viên phải giữ lại bằng chứng về đào tạo như nhật ký đào tạo, sổ đăng nhập (bảng điểm danh) hoặc hồ sơ đào tạo điện tử. Hồ sơ đào tạo nên bao gồm ngày đào tạo, tên của người tham dự và các chủ đề của khóa đào tạo.	Các chủ đề đào tạo có thể bao gồm bảo vệ kiểm soát tiếp cận, nhận ra âm mưu nội bộ và quy trình báo cáo cho các hoạt động đáng ngờ và sự cố bảo mật. Khi có thể, đào tạo chuyên ngành nên bao gồm một cuộc trình diễn thực hành. Nếu tiến hành trình diễn thực hành, người hướng dẫn nên dành thời gian cho học viên để trình diễn quy trình. Cho mục đích của CTPAT, các vị trí nhạy cảm bao gồm nhân viên làm việc trực tiếp với hàng hóa xuất/nhập khẩu hoặc tài liệu hàng hóa, cũng như nhân viên liên quan đến việc kiểm soát việc tiếp cận các khu vực hoặc thiết bị nhạy cảm. Những vị trí này bao gồm, nhưng không giới hạn đối với việc vận chuyển, tiếp nhận, nhân viên phòng văn thư, tài xế, nhân viên liên lạc, nhân viên bảo vệ, bất kỳ cá nhân nào liên quan đến việc đóng hàng, theo dõi phương tiện vận chuyển và/hoặc kiểm soát niêm phong.	Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
12.2	Các tài xế và nhân viên khác thực hiện kiểm tra an ninh và nông nghiệp đối với phương tiện vận chuyển và Công cụ Vận tải Quốc tế (IIT) rỗng phải được đào tạo để kiểm tra phương tiện vận chuyển/IIT cho cả mục đích an ninh và nông nghiệp. Đào tạo cập nhật phải được tiến hành định kỳ, khi cần thiết, sau khi xảy ra sự cố hoặc vi phạm an ninh, hoặc khi có thay đổi về thủ tục của công ty. Đào tạo kiểm tra phải bao gồm các chủ đề sau: • Dấu hiệu của các ngăn ẩn; • Che giấu hàng lậu trong các ngăn xuất hiện tự nhiên; và • Dấu hiệu ô nhiễm dịch hại.		Phải
12.4	Thành viên CTPAT cần có các biện pháp để xác minh rằng việc đào tạo được cung cấp đáp ứng tất cả các mục tiêu đào tạo.	Hiểu được đào tạo và có thể sử dụng đào tạo đó ở vị trí của một người (đối với nhân viên nhạy cảm) là điều tối quan trọng. Bài kiểm tra hoặc câu hỏi, bài tập mô phỏng/diễn tập, hoặc kiểm tra thường xuyên các thủ tục, v.v. là một số biện pháp mà Thành viên có thể thực hiện để xác định hiệu quả của việc đào tạo.	Nên
12.8	Tùy tình hình, dựa trên chức năng và/hoặc vị trí của họ, nhân viên phải được đào tạo về các chính sách và quy trình an ninh mạng của công ty. Điều này phải bao gồm nhu cầu nhân viên bảo vệ mật khẩu/cụm mật khẩu và truy cập máy tính.	Đào tạo chất lượng là rất quan trọng để giảm bớt lỗ hổng cho các cuộc tấn công mạng. Một chương trình đào tạo an ninh mạng mạnh mẽ thường là một chương trình được cung cấp cho nhân viên phù hợp trong một môi trường chính thức thay vì chỉ đơn giản thông qua email hoặc bản ghi nhớ.	Phải
12.9	Nhân sự vận hành và quản lý các hệ thống công nghệ an ninh phải được đào tạo về vận hành và bảo dưỡng trong các lĩnh vực cụ thể của họ. Kinh nghiệm trước đó với các hệ thống tương tự là chấp nhận được. Tự đào tạo thông qua các sách hướng dẫn vận hành và các phương pháp khác là điều chấp nhận được		Phải

ID	Tiêu chí	Hướng dẫn thực hiện	Phải / Nên
12.10	Nhân viên phải được đào tạo về cách báo cáo sự cố an ninh và các hoạt động đáng ngờ.	Các thủ tục để báo cáo sự cố bảo mật hoặc hoạt động đáng ngờ là các khía cạnh cực kỳ quan trọng của một chương trình bảo mật. Đào tạo về cách báo cáo sự cố có thể được bao gồm trong đào tạo an ninh tổng thể. Các mô-đun đào tạo chuyên ngành (dựa trên nhiệm vụ công việc) có thể có các đào tạo chi tiết hơn về thủ tục báo cáo, bao gồm chi tiết cụ thể về quy trình, chẳng hạn như, cần báo cáo những điều gì, cho ai, làm thế nào để báo cáo sự cố, và phải làm gì sau khi báo cáo được hoàn thành.	Phải

Số xuất bản: 1076-0420