Critères minimaux de sécurité – transporteurs routiers

Mars 2020

Remarque: Il est possible que les identifiants critères ne soient pas des nombres consécutifs. Les identifiants qui n'apparaissent pas dans ce document ne s'appliquent pas aux transporteurs routiers.

Premier domaine d'intérêt: La sécurité dans l'entreprise

1. **Vision en matière de sécurité, responsabilité –** Pour que le programme de sécurité de la chaîne d'approvisionnement d'un membre du CTPAT soit efficace et le reste, il doit bénéficier du soutien de la direction générale. Faire de la sécurité une partie intégrante de la culture d'entreprise et veiller à ce qu'elle soit une priorité globale pour cette dernière est, en grande partie, la responsabilité des cadres dirigeants.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
1.1	Dans leurs efforts de promotion d'une culture de sécurité, les membres du CTPAT devraient manifester leur engagement en faveur de la sécurité de la chaîne d'approvisionnement et du programme CTPAT par le biais d'une déclaration de soutien. Cette déclaration devrait porter la signature d'un haut dirigeant de l'entreprise et être affichée dans les endroits appropriés.	La déclaration de soutien devrait souligner l'importance de la protection de la chaîne d'approvisionnement contre les activités criminelles comme le trafic de drogues, le terrorisme, la traite des personnes et la contrebande illicite. Les hauts dirigeants de l'entreprise qui devraient soutenir et signer la déclaration sont, entre autres, le président, le PDG, le secrétaire-gérant ou le directeur de la sécurité. Il convient de poster la déclaration de soutien, entre autres, sur le site internet de l'entreprise et dans les zones clés (accueil, zones d'emballage, entrepôts, etc.), et/ou de l'aborder pendant les séminaires d'entreprise portant sur la sécurité.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
1.2	Pour élaborer un solide programme de sécurité de la chaîne d'approvisionnement, une entreprise devrait disposer d'une équipe multidisciplinaire constituée des représentants de toutes les divisions concernées. Ces nouvelles mesures de sécurité doivent être incorporées aux procédures actuelles de l'entreprise, ce qui favorisera une structure plus durable et soulignera le fait que la sécurité de la chaîne d'approvisionnement est la responsabilité de chacun.	La sécurité de la chaîne d'approvisionnement a une portée beaucoup plus large que les programmes de sécurité traditionnels. Elle est étroitement liée à de nombreuses divisions de l'entreprise, outre la sécurité, comme les ressources humaines, l'informatique et les services d'importation et d'exportation. Les programmes de sécurité de la chaîne d'approvisionnement fondés sur des modèles plus traditionnels et axés sur un service de sécurité risquent d'être moins viables à long terme: la responsabilité d'appliquer les mesures de sécurité se concentrant sur un nombre restreint d'employés, l'entreprise peut être affectée en cas de perte de personnel clé.	Recommandé
1.3	Le programme de sécurité de la chaîne d'approvisionnement doit être conçu, appuyé et mis en œuvre par une composante d'examen écrit appropriée. L'objet de cette composante d'examen est de documenter l'existence d'un système en vertu duquel le personnel est tenu responsable de ses tâches et où toutes les procédures décrites dans le programme de sécurité sont appliquées comme il se doit. Le plan d'examen doit être mis à jour au besoin, en fonction des modifications pertinentes apportées aux activités de l'entreprise et au niveau du risque.	Aux fins d'observation du CTPAT, cet examen a pour objet de s'assurer que les employés d'une entreprise respectent les procédures de sécurité. Le processus d'examen n'a pas nécessairement besoin d'être complexe. Le membre décide de la portée et de la profondeur des examens en fonction de son rôle dans la chaîne d'approvisionnement, de son modèle commercial, du niveau de risque et des variations entre certains sites/emplacements particuliers. Les petites entreprises peuvent créer une méthodologie d'examen très simple, tandis que les multinationales devront peut-être instaurer un processus plus vaste et prendre en compte divers facteurs comme les exigences égales locales, etc. Certaines grandes entreprises disposent déjà d'une équipe de vérificateurs à laquelle faire appel pour faciliter les examens de sécurité. Un membre peut choisir de recourir à des examens plus ciblés visant des procédures spécifiques. Les domaines spécialisés essentiels à la sécurité de la chaîne d'approvisionnement, comme les inspections et les contrôles	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
		des scellés, peuvent faire l'objet d'examens particuliers. Toutefois, il convient de procéder périodiquement à un examen général afin de s'assurer que tous les éléments du programme de sécurité fonctionnent comme prévu. Si un membre effectue déjà des examens dans le cadre de son examen annuel, cela pourrait suffire à satisfaire à ce critère. Les membres dont la chaîne d'approvisionnement est à risque élevé (d'après leur évaluation du risque) peuvent intégrer à ce programme d'examen des exercices de simulation pour s'assurer que le personnel sait comment réagir en cas de véritable incident de sécurité.	
1.4	Le ou les point(s) de contact de l'entreprise auprès du CTPAT doivent posséder de solides connaissances sur les exigences du programme CTPAT. Ces personnes doivent régulièrement informer la direction générale des questions relatives au programme, notamment de l'avancement ou des résultats d'un audit, des exercices portant sur la sécurité et des validations CTPAT.	Le CTPAT attend du point de contact désigné qu'il soit proactif et qu'il communique régulièrement avec son spécialiste de sécurité de la chaîne d'approvisionnement, en s'assurant d'être à son écoute. Les membres peuvent identifier d'autres interlocuteurs qui contribueront à cette fonction et les inscrire comme contacts sur le portail du CTPAT.	Obligatoire

2. **<u>L'évaluation du risque</u> –** La menace persistante des groupes terroristes et organisations criminelles ciblant les chaînes d'approvisionnement impose aux membres la nécessité d'évaluer la mesure dans laquelle ils sont réellement et potentiellement exposés à ces menaces en perpétuelle évolution. Le CTPAT comprend que lorsqu'une entreprise dispose de plusieurs chaînes d'approvisionnement faisant intervenir de nombreux partenaires commerciaux, elle doit faire face à une complexité accrue pour les sécuriser. Une entreprise qui gère de nombreuses chaînes d'approvisionnement devrait concentrer son attention sur celles qui sont implantées dans des zones géographiques à risque plus élevé.

   Lors de la détermination du risque au sein de leurs chaînes d'approvisionnement, les membres doivent prendre en compte divers facteurs propres à la chaîne d'approvisionnement en question: le modèle commercial, l'emplacement géographique des fournisseurs, etc.

   Définition importante: Risque – Mesure d'un préjudice potentiel, provoqué par un événement indésirable, qui prend en compte les menaces, les vulnérabilités et les conséquences. Le niveau d'un risque est déterminé en fonction de la probabilité de la menace. Un évènement à probabilité élevé équivaut généralement à un niveau de risque élevé. Il n'est pas toujours possible d'éliminer un risque, mais on peut l'atténuer en le gérant, c'est à dire, en parant aux vulnérabilités ou en réduisant l'impact global du risque en question sur l'entreprise.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
2.1	Les membres du CTPAT doivent gérer et documenter le niveau de risque dans leurs chaînes d'approvisionnement. Ils doivent mener une évaluation globale du risque pour identifier les éventuelles vulnérabilités de sécurité. L'évaluation globale du risque doit identifier les menaces, évaluer les risques et incorporer des mesures durables pour atténuer les vulnérabilités. Le membre doit prendre en compte les	L'évaluation globale du risque se compose de deux parties essentielles. La première est une auto-évaluation des pratiques, procédures et règlements de sécurité de la chaîne d'approvisionnement du membre – au sein des locaux qu'il administre – pour vérifier sa conformité aux critères de sécurité minimale du CTPAT, et un examen global de la gestion pour déterminer comment est contrôlé le risque. La deuxième partie de l'évaluation globale est une évaluation du risque à l'échelle internationale. Cette partie consiste à identifier la ou les potentielles menaces géographiques en fonction du modèle commercial du membre et de son rôle dans la chaine d'approvisionnement. Lorsqu'il examine l'impact éventuel de chaque menace sur la sécurité de sa chaîne d'approvisionnement, le membre doit utiliser une méthode qui lui permet d'évaluer ou de différencier les niveaux de risque. La méthode simple consiste à attribuer les niveaux de risque faible, moyen et élevé.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
	exigences CTPAT spécifiques à son rôle dans la chaîne d'approvisionnement.	Le CTPAT a élaboré son « Guide d'évaluation du risque en 5 étapes » pour aider les membres à mener la partie internationale de leur évaluation globale du risque; il est disponible sur le site internet du Service des douanes et de la protection des frontières des États-Unis (U.S. Customs and Border Protection): https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. Les membres dont les chaînes d'approvisionnement sont vastes devraient se concentrer principalement sur les domaines à risque élevé.	
2.3	Les évaluations du risque doivent être réexaminées chaque année, voire plus fréquemment en fonction des facteurs de risque.	Dans certaines circonstances, il peut être nécessaire de réexaminer les évaluations du risque plusieurs fois par an, notamment en cas d'augmentation du niveau de menace dans un pays donné, de périodes d'alerte plus élevée, d'atteintes à la sécurité ou d'incidents connexes, de changement de partenaire commercial et/ou de modification de la structure/propriété de l'entreprise (fusions ou acquisitions), etc.	Obligatoire
2.4	Les membres du CTPAT devraient disposer de procédures écrites abordant la gestion des crises, la continuité des opérations, les plans de rétablissement de la sécurité et la reprise des activités.	On peut qualifier de « crise » la perturbation de la circulation des données commerciales en cas de cyberattaque, d'incendie ou de détournement d'un transporteur par des individus armés. En fonction du risque et de l'endroit où le membre s'approvisionne ou exerce ses activités, un plan d'urgence peut comporter des notifications supplémentaires ou une assistance complémentaire en matière de sécurité, et expliquer comment récupérer ce qui a été détruit ou volé et rétablir des conditions de fonctionnement normales.	Recommandé

3. **<u>Les partenaires commerciaux</u> –** Les membres du CTPAT traitent avec toutes sortes de partenaires commerciaux, à la fois aux niveaux national et international. Concernant les partenaires commerciaux qui s'occupent directement des documents relatifs au fret et/ou à l'importation/exportation, il est essentiel que les membres veillent à ce que ces partenaires appliquent des mesures de sécurité adéquates pour sécuriser la marchandise sur l'ensemble de la chaîne d'approvisionnement internationale. Un partenaire qui sous-traite certains services représente un facteur de complexité supplémentaire qui doit être pris en compte lors de l'analyse des risques d'une chaîne d'approvisionnement.

Définition importante: Partenaire commercial – Toute personne ou entreprise dont les pratiques peuvent affecter la chaîne de possession des marchandises importées ou exportées des États-Unis via la chaîne d'approvisionnement d'un membre du CTPAT. Toute partie fournissant un service pour répondre à un besoin de la chaîne d'approvisionnement internationale d'une entreprise peut être qualifiée de « partenaire commercial ». Notamment, les parties (à la fois directes et indirectes) impliquées dans l'achat, la préparation des documents, la facilitation, la manutention, le stockage et/ou le mouvement des cargaisons, pour le compte d'un importateur ou exportateur membre du CTPAT. Les transporteurs en sous-traitance et les entrepôts de groupage à l'étranger coordonnées par un agent/fournisseur logistique sont deux exemples de partenaires indirects.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
3.1	Les membres du CTPAT doivent disposer d'un processus écrit, basé sur les risques, en ce qui concerne la sélection de nouveaux partenaires commerciaux et la surveillance de leurs partenaires actuels. Contrôler les activités liées au blanchiment de capitaux et au financement du terrorisme est un élément que les membres devraient inclure dans ce processus. À cet effet, veuillez consulter les Indices d'avertissement du CTPAT relatifs aux activités de blanchiment de capitaux et de financement du terrorisme par le commerce.	Voici quelques exemples d'éléments de vérification permettant de déterminer la légitimité d'une entreprise: • Vérifier l'adresse commerciale de l'entreprise et depuis combien de temps elle est enregistrée à cette adresse; • Effectuer des recherches sur internet sur l'entreprise et ses dirigeants; • Contrôler ses références commerciales; • Demander un rapport de crédit. Les partenaires commerciaux qui doivent faire l'objet d'une vérification préalable sont les partenaires directs, comme les fabricants, les fournisseurs de produits, les distributeurs/prestataires de services pertinents ainsi que les fournisseurs de logistique et de services de transport. Les distributeurs/prestataires de services directement impliqués dans la chaîne d'approvisionnement de l'entreprise, et/ou qui gèrent ses informations/équipements sensibles, doivent également figurer sur la liste de vérification préalable, y compris les courtiers et prestataires informatiques.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
		L'exhaustivité de la vérification préalable est fonction du niveau de risque présent dans la chaîne d'approvisionnement.	
3.3	Les procédures écrites de vérification doivent comprendre des indicateurs pour identifier les expéditions ou clients susceptibles d'être illégitimes. Si, lors de la vérification d'une expédition ou d'un client, un facteur de risque accru est détecté, le transporteur devra effectuer un examen approfondi. Si la vérification met en évidence un doute considérable quant à l'authenticité d'une expédition ou d'un client, le transporteur doit faire part de ses soupçons au Service des douanes et de la protection des frontières des États-Unis.	Si, entre autres, l'entité concernée est disposée à payer un montant supérieur à la norme en espèces, dispose de peu d'informations sur la marchandise à transporter, est peu enclin à répondre aux questions, dispose de coordonnées limitées (numéro de téléphone portable, boîte postale), ou s'il s'agit d'une nouvelle entreprise ou d'une entreprise sans historique d'activités, il peut s'agir d'un signal d'alarme.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
3.4	La procédure de vérification préalable d'un partenaire commercial doit prendre en compte si celui-ci est membre du CTPAT ou du programme d'un opérateur économique agréé (OEA) bénéficiant d'un accord de reconnaissance mutuelle (MRA) avec les États-Unis (ou une administration MRA agréée). Si un partenaire commercial est titulaire de l'autorisation OEA ou de la certification CTPAT ceci constitue une preuve acceptable du fait qu'il satisfait aux exigences de programme; les membres doivent demander une preuve de ladite certification et continuer de surveiller ces partenaires pour s'assurer que ces certifications sont tenues à jour.	On peut vérifier si un partenaire commercial détient la certification CTPAT par le biais du système de vérification de statut du portail CTPAT. Si un partenaire commercial est détenteur d'une autorisation OEA octroyée par une administration étrangère reconnue par les États-Unis, l'autorisation OEA de ladite administration comportera la composante sécurité. Les membres peuvent se rendre sur le site internet des autorités douanières étrangères en question où ils trouveront le nom des titulaires d'autorisations OEA; ils peuvent également demander directement à leurs partenaires commerciaux une copie de leur autorisation. Les États-Unis disposent actuellement d'un accord de reconnaissance mutuelle (MRA) avec les pays suivants: La Nouvelle Zélande, le Canada, la Jordanie, le Japon, la Corée du Sud, l'Union Européenne (28 États membres), Taïwan, Israël, le Mexique, Singapour, la République dominicaine et le Pérou.	Obligatoire
3.5	Les membres CTPAT qui sous-traitent certains éléments de leur chaîne d'approvisionnement devraient exercer une diligence raisonnable (par le biais de visites, de questionnaires, etc.) pour s'assurer que ces partenaires commerciaux emploient des mesures qui satisfont ou surpassent les critères minimaux du CTPAT en matière de sécurité.	Les importateurs et exportateurs ont tendance à sous-traiter une grande partie des activités de leur chaîne d'approvisionnement. Dans ces transactions, les importateurs (et certains exportateurs) sont les parties qui disposent généralement d'un pouvoir d'influence sur leurs partenaires commerciaux et peuvent exiger la mise en œuvre de mesures de sécurité sur l'ensemble de la chaîne d'approvisionnement, selon qu'il convient Lorsque ces partenaires commerciaux ne sont ni titulaires de la certification CTPAT ni membres d'un programme MRA autorisé, le membre du CTPAT doit exercer une diligence raisonnable afin de veiller (quand il dispose de l'influence nécessaire) à ce que ces partenaires satisfassent aux critères de sécurité applicables du programme. Afin de s'assurer que les exigences de sécurité sont respectées, les importateurs procèdent à l'évaluation des mesures de sécurité de leurs partenaires commerciaux. Le processus permettant de déterminer la quantité d'informations à collecter au sujet du programme de sécurité d'un partenaire commercial repose sur l'évaluation du risque du membre concerné; si ce dernier gère plusieurs chaînes	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
		d'approvisionnement, les zones à risque élevé sont prioritaires. On peut déterminer si un partenaire satisfait aux critères minimaux de sécurité de plusieurs manières. En fonction du risque, l'entreprise pourra – directement ou en engageant un entrepreneur/prestataire de services – mener un audit des installations, ou faire appel à un questionnaire de sécurité. Si l'on utilise un questionnaire de sécurité, le niveau de risque déterminera la quantité nécessaire de détails ou de preuves à collecter. Il faut parfois demander plus de détails à une entreprise implantée dans une zone à risque élevé. Si un membre envoie un questionnaire de sécurité à ses partenaires commerciaux, il conviendra de demander les informations suivantes: •Le nom et le titre des personnes qui y répondent; •La date à laquelle il y a été rempli; •La signature des personnes qui y répondent; •*La signature d'un haut dirigeant de l'entreprise, du responsable de la sécurité, ou du représentant autorisé de l'entreprise qui se porte garant de l'exactitude du questionnaire; •Des réponses suffisamment détaillées pour déterminer le niveau de conformité; •En fonction du risque, et selon que les protocoles de sécurité locaux l'autorisent, des preuves photographiques, des copies des règlements et procédures ainsi que des copies des formulaires remplis, comme la liste d'inspection des « instruments de trafic international », et/ou les registres des gardiens. *Les signatures peuvent être électroniques. Si une signature est difficile à obtenir ou à confirmer, l'interlocuteur peut attester de la validité du questionnaire par courrier électronique et certifier que les réponses et les preuves fournies ont été approuvées par un superviseur/responsable (nom et titre requis).	

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
3.7	Pour s'assurer que leurs partenaires commerciaux continuent de respecter les critères de sécurité du CTPAT, les membres doivent régulièrement, ou lorsque les circonstances/risques l'imposent, mettre à jour les évaluations de sécurité de leurs partenaires commerciaux.	Il est important d'examiner périodiquement les évaluations de sécurité des partenaires commerciaux pour garantir qu'un solide programme de sécurité est toujours en place et fonctionne correctement. Si un membre ne réévaluait jamais le programme de sécurité de ses partenaires commerciaux, il ne pourrait pas savoir qu'un programme autrefois viable n'est plus efficace et il exposerait ainsi sa chaîne d'approvisionnement à des risques. C'est en fonction de son propre processus d'évaluation du risque qu'un membre détermine à quelle fréquence réexaminer l'évaluation de sécurité d'un partenaire. Les chaînes d'approvisionnement exposées à un risque élevé devraient faire l'objet d'examens plus fréquents que celles à faible risque. Un membre qui évalue les pratiques de sécurité d'un partenaire commercial en effectuant des visites sur son site pourrait tirer profit d'autres types de visites obligatoires. Il pourrait, par exemple, former le personnel chargé des tests de contrôle de la qualité à effectuer également des vérifications de sécurité. Les circonstances pouvant nécessiter des réévaluations plus fréquentes sont les suivantes: augmentation du niveau de menace d'un pays d'approvisionnement, changement d'une source d'approvisionnement, nouveaux partenaires commerciaux essentiels (ceux qui manient réellement les cargaisons, assurent la sécurité d'une installation, etc.).	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
3.8	Pour les expéditions à destination des États-Unis, si un membre sous-traite le service de transport à un autre transporteur routier, le membre doit avoir recours à un transporteur certifié CTPAT, ou à un transporteur qui travaille directement pour le membre en vertu d'un contrat écrit. Le contrat doit stipuler le respect de toutes les exigences des critères de sécurité minimum (MSC).	Le transporteur doit fournir une liste de ses transporteurs et chauffeurs sous-traitants au lieu de chargement et de déchargement. Toute modification apportée à la liste des fournisseurs doit être transmise immédiatement aux partenaires concernés. Lors de l'examen de la conformité de ses prestataires, le membre doit vérifier que le sous-traitant transporte lui-même les marchandises au lieu de le sous-traiter à son tour sans autorisation. Les membres doivent limiter la sous-traitance des services de transport à un seul niveau. Si, exceptionnellement, un niveau de sous-traitance supplémentaire est autorisé, le membre du CTPAT et le transporteur doivent en être dûment informés.	Obligatoire

4. **<u>La cybersécurité</u>** – À l'ère numérique actuelle, la cybersécurité est un élément clé de la protection des actifs les plus importants d'une entreprise: propriété intellectuelle, informations sur les clients, données financières et commerciales, dossiers du personnel, etc. Plus une entreprise est connectée à internet, plus ses systèmes informatiques courent le risque d'une intrusion. Cette menace concerne les entreprises de tout type et de toute taille. Les mesures visant à sécuriser les technologies de l'information (TI) et les données d'une entreprise sont d'une importance capitale. À cet égard, les critères énumérés ci-dessous constituent, pour les membres, la base d'un programme de cybersécurité qui se veut global.

   Définitions importantes: Cybersécurité – Activité ou processus visant à protéger les ordinateurs, les réseaux, les programmes et les données contre tout accès, modification ou destruction accidentel ou non autorisé. C'est le processus qui consiste à identifier, analyser, évaluer et communiquer un risque lié à internet, et à l'accepter, l'éviter, le transférer ou l'atténuer, en tenant compte des coûts et des avantages.

   Technologies de l'information (TI) – Ordinateurs, dispositifs de stockage et de mise en réseau (et autres appareils physiques), infrastructures et processus permettant de créer, de traiter, de stocker, de sécuriser et d'échanger toutes les formes de données électroniques.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.1	Les membres du CTPAT doivent disposer de politiques et/ou de procédures écrites complètes en matière de cybersécurité, afin de protéger les systèmes de technologies de l'information (TI). La politique TI écrite doit, au minimum, couvrir tous les critères individuels de cybersécurité.	Les membres sont encouragés à suivre des protocoles de cybersécurité s'appuyant sur des cadres/normes industriels reconnus. L'Institut national des normes et de la technologie (National Institute of Standards and Technology - NIST) des États-Unis fait partie des organisations qui fournissent un cadre de cybersécurité (https://www.nist.gov/cyberframework) proposant des conseils basés sur les normes, les directives et les pratiques existantes, pour une meilleure gestion ainsi qu'une réduction des risques en matière de cybersécurité en interne et à l'externe. Cet outil peut servir à identifier et hiérarchiser les mesures d'atténuation des risques liés à la cybersécurité et il permet d'aligner les approches politiques, commerciales et technologiques concernant la gestion de ces risques. Ce cadre vient compléter le processus de gestion des risques et le programme de cybersécurité d'une organisation. Inversement, une organisation qui ne dispose pas d'un programme de cybersécurité peut s'appuyer sur ce cadre pour en établir un. *Le NIST est un organisme fédéral sans pouvoir réglementaire qui relève du département du Commerce et promeut et maintient des normes de mesure. Il est officiellement chargé d'élaborer des normes technologiques pour le gouvernement fédéral.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.2	Pour se prémunir des menaces à la cybersécurité les plus fréquentes, les membres doivent équiper leurs systèmes informatiques (TI) d'une protection logicielle/matérielle contre les logiciels malveillants (virus, logiciels espions, vers, chevaux de Troie, etc.) et les intrusions internes/externes (pares-feux). Les membres doivent s'assurent que leur logiciel de sécurité est actualisé et qu'il exécute régulièrement des mises à jour. Les membres doivent disposer de politiques et de procédures pour prévenir les attaques par ingénierie sociale. En cas d'atteinte à la protection des données ou d'un autre incident inaperçu qui occasionne la perte de données et/ou de matériel, les procédures doivent aborder la récupération (ou le remplacement) des systèmes TI et/ou des données.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.3	Les membres CTPAT utilisant des systèmes de réseaux doivent régulièrement tester la sécurité de leur infrastructure informatique. Si des vulnérabilités sont détectées, des actions correctives doivent être mises en place dans les plus brefs délais.	Un réseau informatique sécurisé est d'une importance capitale pour une entreprise: il doit être régulièrement testé pour s'assurer qu'il est adéquatement protégé. Pour ce faire, on peut programmer des analyses des vulnérabilités. De la même manière qu'un vigile s'assure que les portes et fenêtres d'une entreprise sont bien fermées, une analyse des vulnérabilités identifie la présence d'ouvertures sur les ordinateurs (ports et adresses IP ouverts), les systèmes d'exploitation et les logiciels, par le biais desquelles un cyberpirate peut accéder au système informatique de l'entreprise. À ces fins, l'analyse des vulnérabilités compare les résultats de son examen à une base de données de vulnérabilités connues et produit un rapport de correction indiquant les mesures que devrait prendre l'entreprise. Il existe de nombreuses versions gratuites et commerciales de logiciels de détection des vulnérabilités. La fréquence des analyses dépend de plusieurs facteurs, notamment du modèle commercial de l'entreprise et de son niveau de risque. Par exemple, il convient de lancer une analyse lorsque l'infrastructure réseau de l'entreprise a été modifiée. Cependant, les cyberattaques frappent de plus en plus les entreprises de toute taille – une réalité qui doit être prise en compte lors de la conception d'un plan d'analyse.	Obligatoire
4.4	Les politiques d'un membre en matière de cybersécurité devraient indiquer de quelle manière il doit communiquer au gouvernement et à d'autres partenaires commerciaux les informations concernant les menaces à la cybersécurité.	Les membres sont encouragés à communiquer au gouvernement et aux partenaires commerciaux de leur chaîne d'approvisionnement toute information relative à des menaces à la cybersécurité. Le partage de l'information est un élément clé de la mission du département de la Sécurité intérieure en vue de favoriser une connaissance partagée de la situation en matière de cyberactivité malveillante. Les membres du CTPAT peuvent se joindre au Centre national d'intégration de la cybersécurité et des communications (NCCI - https://www.us-cert.gov/nccic). Le NCCIC partage ses informations avec ses partenaires des secteurs public et privé afin de les sensibiliser aux vulnérabilités, incidents et solutions. Les utilisateurs de systèmes de contrôle électroniques et industriels peuvent s'abonner gratuitement aux produits d'information, actualités et services.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.5	Les membres doivent disposer d'un système pour identifier les accès non autorisés aux systèmes/données informatiques et les infractions aux politiques et procédures, notamment l'accès inapproprié aux systèmes internes ou à des sites internet externes, et la falsification ou la modification des données de l'entreprise par les employés ou les sous-traitants. Tous les auteurs d'infractions doivent faire l'objet de sanctions adéquates.		Obligatoire
4.6	Les politiques et procédures en matière de cybersécurité doivent être réexaminées une fois par an, voire plus fréquemment en fonction des circonstances et des facteurs de risque. À la suite de ce réexamen, les politiques et procédures doivent être mises à jour, le cas échéant.	Une cyberattaque constitue une situation exigeant la mise à jour d'une politique avant l'échéance du délai d'un an. Un membre qui tirerait profit des leçons d'une cyberattaque contribuerait à renforcer sa politique en matière de cybersécurité.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.7	L'accès des utilisateurs est limité en fonction de la description de leur poste ou des tâches qui leur sont assignées. Les autorisations d'accès doivent être régulièrement réexaminées pour veiller à ce que l'accès aux systèmes sensibles soit basé sur les exigences de poste. L'autorisation d'accès d'un employé aux ordinateurs et réseaux doit être supprimée lors du départ de celui-ci.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.8	Toute personne ayant accès aux systèmes informatiques doit utiliser le compte qui lui a été attribué individuellement. L'accès aux systèmes informatiques doit être protégé des infiltrations par le biais de mots de passe et de phrases passe sûrs (ou autres formes d'authentification), et l'accès des utilisateurs aux systèmes informatiques doit être sécurisé. Les mots de passe et phrases passe doivent être changés dès que possible s'il est établi ou fortement soupçonné que ceux-ci ont été compromis.	Pour se prémunir des infiltrations, les utilisateurs doivent passer par une procédure d'authentification pour accéder aux systèmes informatiques. Les mots de passe (ou phrases passe) complexes, les technologies biométriques ainsi que les cartes d'identité électroniques sont trois facteurs d'authentification différents. Les procédures d'authentification qui font appel à plusieurs facteurs sont à privilégier. On les appelle authentification à deux facteurs (2FA) et authentification multifacteur (MFA). La MFA est l'authentification la plus sécurisée car l'utilisateur doit présenter pas moins de deux éléments de preuve (identifiants) pour confirmer son identité pendant le processus de connexion. Les MFA peuvent contribuer à bloquer de potentielles intrusions généralement facilitées par des mots de passe faibles ou des identifiants volés. Les MFA peuvent contribuer à neutraliser ces vecteurs d'attaque en exigeant des utilisateurs qu'ils complètent leurs mots de passe ou phrases passe (quelque chose qu'ils savent) par quelque chose qu'ils possèdent (comme un jeton) ou l'une de leurs caractéristiques physiques (une donnée biométrique). Si vous utilisez des mots de passe, ils doivent être complexes. La publication spéciale NIST 800-63B de l'Institut national des normes et de la technologie, intitulée « Digital Identity Guidelines [Lignes directrices relatives à l'identité numérique] » offre des recommandations en matière de mots de passe (https://pages.nist.gov/800-63-3/sp800-63b.html). Elle recommande l'utilisation de phrases passe longues, faciles à mémoriser plutôt que des mots accompagnés de caractères spéciaux. Faciles à mémoriser, ces longues phrases passe (le NIST recommande d'autoriser une longueur maximale de 64 caractères) sont considérées comme étant beaucoup plus difficiles à pirater.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.9	Les membres qui permettent à leurs utilisateurs de se connecter à distance doivent utiliser des technologies sécurisées, comme par exemple les réseaux privés virtuels (VPN), pour permettre aux employés d'accéder de manière sécurisée à l'intranet de l'entreprise quand ils ne sont pas aux bureaux. Les membres doivent également disposer de procédures conçues pour empêcher l'accès à distance de tout utilisateur non autorisé.	Les VPN ne sont pas la seule option pour sécuriser l'accès distant à un réseau. L'authentification multifacteur (MFA) en est une autre. Exemple d'authentification multifacteur: un jeton doté d'un code de sécurité dynamique que l'employé doit saisir pour accéder au réseau.	Obligatoire
4.10	Si un membre autorise ses employés à utiliser leurs appareils personnels pour remplir leurs fonctions professionnelles, lesdits appareils doivent être conformes aux politiques et procédures de l'entreprise en matière de cybersécurité, notamment en veillant à ce que les mises à jour de sécurité soient régulièrement effectuées et à ce que la méthode d'accès au réseau de l'entreprise soit sécurisée.	Les supports d'enregistrement (CD, DVD, clés USB, etc.) sont également des appareils personnels. Il convient de prendre certaines précautions si les employés sont autorisés à connecter leurs supports personnels à des systèmes individuels. En effet, ces dispositifs de stockage des données pourraient être infectés par des logiciels malveillants susceptibles de se propager via le réseau de l'entreprise.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.11	Les politiques et procédures de cybersécurité devraient comprendre des mesures visant à empêcher l'utilisation de produits technologiques contrefaits ou sans licence valable.	Un logiciel informatique est la propriété intellectuelle de l'entité qui l'a créé. Sans l'autorisation expresse du fabricant ou de l'éditeur, il est illégal d'installer un logiciel, quelle que soit la manière dont il a été acquis. Les versions logicielles autorisées sont généralement accompagnées d'une licence accordée par l'éditeur. Les logiciels sans licence sont plus susceptibles de tomber en panne en raison de leur incapacité à se mettre à jour. Ils sont plus vulnérables aux logiciels malveillants, rendant les ordinateurs et leurs informations inutiles. Vous ne bénéficierez ni d'une garantie ni d'une assistance pour les logiciels sans licence, laissant votre entreprise seule responsable de gérer les pannes. Utiliser un logiciel sans licence implique également des conséquences juridiques, notamment des sanctions sévères au civil et des poursuites au pénal. Le piratage de logiciel provoque l'augmentation des coûts pour les utilisateurs de logiciels sous licence et réduit le capital disponible pour la recherche et le développement de nouveaux logiciels. Il peut être judicieux pour les membres d'instaurer une politique exigeant que les étiquettes de clé de produit et les certificats d'authenticité soient conservés lors de l'achat d'un nouveau support. Les CD, DVD et supports USB sont équipés d'étiquettes holographiques permettant de déterminer l'authenticité des produits et de se protéger de la contrefaçon.	Recommandé
4.12	Les données devraient être sauvegardées une fois par semaine, voire plus fréquemment selon les cas. Toutes les données sensibles et confidentielles devraient être stockées dans un format crypté.	Parce qu'une perte de données peut être plus ou moins grave pour certains individus au sein d'une même organisation, il convient d'effectuer des sauvegardes de données fréquentes. Si la production ou les serveurs partagés sont susceptibles d'être compromis ou perdus, une sauvegarde quotidienne est recommandée. Selon le type d'informations qu'ils hébergent, les systèmes individuels peuvent nécessiter des sauvegardes moins fréquentes. Dans l'idéal, les supports utilisés pour stocker les sauvegardes devraient être conservés hors site. Les périphériques utilisés pour la sauvegarde des données ne devraient pas être connectés au même réseau que celui servant au travail de production. Sauvegarder les données dans le Cloud constitue une méthode de stockage hors site acceptable.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
4.13	Tous les supports, matériels ou autres équipements informatiques contenant des informations sensibles sur les procédures d'importation/exportation doivent être régulièrement inventoriés. Pour s'en débarrasser, il faut correctement les nettoyer et/ou les détruire conformément aux directives en matière de désinfection des périphériques de l'Institut national des normes et de la technologie (NIST), et autres directives connexes.	Exemples de supports informatiques: disques durs (y compris externes), CD-ROM ou CD-R, DVD, clés USB, etc. Le NIST a élaboré les normes de destruction des supports informatiques appliquées par le gouvernement. Il peut être utile pour les membres de consulter les normes NIST relatives à la désinfection et à la destruction du matériel informatique. Désinfection des supports: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	Obligatoire

Deuxième domaine d'intérêt: Sécurité des transports

5. **<u>La sécurité des moyens de transport et des instruments de trafic international</u>** – Les opérations de contrebande impliquent souvent de modifier les moyens de transport et instruments de trafic international (IIT), ou d'y dissimuler des articles de contrebande à l'intérieur. La présente catégorie de critères aborde les mesures de sécurité conçues pour empêcher, détecter et/ou dissuader toute modification ou effraction clandestine des structures IIT visant à y introduire des personnes ou matériaux non autorisés.

   Les membres devraient appliquer, au point d'empotage/de chargement, des procédures pour l'inspection et le scellement des IIT. Les marchandises en transit ou « immobilisées » sont moins contrôlées et sont donc plus vulnérables aux infiltrations. C'est pourquoi le contrôles des scellés et les méthodes de suivi des marchandises/moyens de transport en transit constituent des critères de sécurité essentiels.

   Les atteintes à la chaîne d'approvisionnement surviennent généralement pendant le transport. Par conséquent, les membres doivent veiller à ce que ces critères essentiels relatifs au fret soient respectés tout au long de leur chaîne d'approvisionnement.

   Définition importante: Instruments de trafic international (IIT) – Conteneurs, plateaux, unités de chargement (UC), fourgons élévateurs, fourgons utilitaires, citernes d'expédition, caisses, palettes, plaques de presse, tubes d'enroulement pour tissus et autres conteneurs spécialisés arrivant (chargés ou vides), qui sont ou seront utilisés pour l'expédition de marchandises à l'international.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.1	Les moyens de transports et instruments de trafic international (IIT) doivent être entreposés dans une zone sécurisée afin d'empêcher tout accès non autorisé qui pourrait occasionner une modification de la structure d'un instrument de trafic international ou, le cas échéant, une atteinte aux scellés ou aux portes.	Il est important de sécuriser les zones d'entreposage des moyens de transport et instruments de trafic international (qu'ils soient vides et pleins) pour prévenir tout accès non autorisé.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.2	Le processus d'inspection du CTPAT doit intégrer des procédures écrites pour les inspections de sécurité et les inspections de produits agricoles.	Compte tenu de la prévalence des opérations de contrebande impliquant la modification des moyens de transport ou des instruments de trafic international, ces derniers doivent impérativement être inspectés par les membres afin de détecter tout signe visible d'organismes nuisibles et toute faiblesse structurelle. De la même manière, prévenir la contamination des moyens de transport et IIT par des organismes nuisibles est primordial; c'est pourquoi la composante agricole a été ajoutée au processus d'inspection de sécurité. La contamination par des organismes nuisibles se définit par la présence visible d'animaux, d'insectes ou d'autres invertébrés (vivants, morts – ou à toute autre étape de leur cycle de vie, oothèques et coques compris), de matières organiques d'origine animale (sang, os, poils, chair, sécrétions, excrétions, etc.), de plantes ou produits végétaux viables ou non viables (fruits, graines, feuilles, brindilles, racines, écorce, etc.), d'autres matières organiques (ex. champignons) et de terre ou d'eau, lorsque ces produits ne figurent pas sur le manifeste de marchandises d'un instrument de trafic international (conteneur, unité de chargement, etc.).	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.3	Les membres du CTPAT doivent s'assurer l'inspection de sécurité et agricole suivante, agréée par le CTPAT, ait lieu. Les exigences de ces inspections dépendent du moyen de transport de la chaîne d'approvisionnement: terrestre (Canada ou Mexique) ou maritime et aérien (si elle ne provient pas du continent américain). Avant l'empotage/conditionnement, tous les instruments de trafic international (IIT) doivent être inspectés. Les moyens de transport doivent également être inspectés lorsqu'ils franchissent la frontière terrestre des États-Unis. <u>Les exigences relatives à l'inspection des expéditions CTPAT par voie maritime, aérienne, terrestre (le cas échéant), ferroviaire ou intermodale sont les suivantes:</u> Il convient de mener une inspection en sept points de tous les conteneurs vides et unités de chargement (UC) et une inspection en huit points de tous les conteneurs et UC frigorifiques vides: 1. Paroi avant; 2. Côté gauche; 3. Côté droit; 4. Plancher; 5. Plafond/le toit; 6. Portes intérieures/extérieures, y compris la fiabilité des mécanismes de verrouillage des portes; 7. Extérieur/train roulant; 8. Boîtier du ventilateur des conteneurs frigorifiques. <u>Exigences supplémentaires pour les transporteurs routiers qui franchissent la frontière terrestre:</u> L'inspection des moyens de transport et IIT doit être systématique et effectuée dans l'aire d'entreposage des moyens de transport et IIT.	Les instruments de trafic international (IIT) et les moyens de transports doivent faire l'objet d'une inspection agricole et de sécurité pour vérifier que leurs structures n'ont pas été modifiées afin d'y cacher de la marchandise de contrebande, ou contaminées par des nuisibles agricoles visibles. Pour les chaînes d'approvisionnement internationales, tous les IIT doivent être inspectés au point d'empotage/conditionnement. Si une chaîne d'approvisionnement aérienne/maritime affiche un risque élevé, des procédures d'inspection approfondies peuvent être nécessaires. Celles-ci peuvent comprendre une inspection des moyens de transport, des terminaux maritimes et des installations de logistique aérienne. Le niveau de risque est habituellement plus élevé pour les expéditions qui franchissent la frontière terrestre. C'est pourquoi, dans ce cas, le moyen de transport et l'IIT sont soumis à plusieurs inspections. Les conteneurs de transport maritime, les conteneurs/remorques réfrigérés, conteneurs routiers, remorques à plateau, conteneurs citernes, wagons de marchandises, chalands à clapets et unités de chargement (UC) sont quelques exemples d'IIT utilisés pour différents moyens de transport. Des outils de formation portant sur les inspections de sécurité et inspections agricoles des moyens de transport/instruments de trafic	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
	Dans la mesure du possible, des inspections doivent être menées à l'entrée et à la sortie des aires d'entreposage et au point de chargement/d'empotage. Doivent être inspectés systématiquement les 17 points suivants: **<u>Les tracteurs:</u>** 1. Pare-chocs/pneus/jantes; 2. Portes, compartiments à outils et mécanismes de verrouillage; 3. Compartiment de batterie; 4. Reniflard; 5. Réservoir d'essence; 6. Habitacle/couchette; 7. Carénage/toit. **<u>Remorques</u>**: 1. Zone de la sellette d'attelage – vérification de la nature d'origine des compartiments/la plaque de protection; 2. Extérieur – avant/côtés; 3. Arrière – pare-chocs/portes; 4. Paroi avant; 5. Côté gauche; 6. Côté droit; 7. Plancher; 8. Plafond/toit; 9. Portes intérieures/extérieures et mécanismes de verrouillage; 10. Extérieur/train roulant.	international sont disponibles dans la section Bibliothèque publique du portail CTPAT.	

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.4	Les moyens de transport et les instruments de trafic international (selon le cas) doivent être équipés de matériel externe pouvant raisonnablement résister aux tentatives d'effraction. La porte, les poignées, les tiges, les moraillons, les rivets, les supports et toutes les autres pièces du mécanisme de verrouillage du conteneur doivent être minutieusement inspectés afin de détecter toute effraction et incohérence matérielle avant de fixer les scellés.	Il est recommandé d'utiliser des conteneurs/remorques équipés de charnières inviolables. On peut également installer des plaques ou broches de protection sur au moins deux des charnières des portes, et/ou appliquer un scellé/ruban adhésif sur l'une (ou plusieurs) des charnières de chaque côté.	Obligatoire
5.5	L'inspection de tous les moyens de transport et des instruments de trafic international vides devrait être consignée sur une liste de contrôle. Les éléments suivants devraient apparaître sur la liste: • Le numéro de conteneur/remorque/instrument de trafic international; • La date d'inspection; • L'heure d'inspection; • Le nom de l'employé effectuant l'inspection; • Les parties spécifiques de l'instrument de trafic international ayant été inspectées. Si les inspections sont supervisées, le superviseur devrait également signer la liste de contrôle. La fiche d'inspection du conteneur/des instruments de trafic international dûment remplie devrait être annexée à la documentation d'expédition. Le destinataire devrait recevoir toute la documentation d'expédition avant de recevoir la marchandise.		Recommandé
5.6	Toutes les inspections de sécurité doivent avoir lieu dans une zone d'accès contrôlé et, si possible, être surveillées via un système de vidéosurveillance.		Recommandé
5.7	Si des nuisibles sont détectés pendant l'inspection des moyens de transport et instruments de trafic international, il convient de les laver et de passer l'aspirateur pour remédier à la contamination. Les documents qui justifient la conformité avec ces exigences d'inspection doivent être conservés pendant un an.	Les membres sont invités à conserver des données sur les types de contaminants détectés, leur emplacement (emplacement du moyen de transport) et leur mode d'élimination, pour éviter d'autres cas de contamination par des nuisibles.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.8	Selon les risques, le personnel de gestion devrait procéder à des fouilles aléatoires des moyens de transport une fois que le personnel des transports a terminé l'inspection des moyens de transport/instruments de trafic international. Les moyens de transport devraient être fouillés périodiquement et à une fréquence plus élevée si le niveau de risque le justifie. Les fouilles devraient être effectuées au hasard et sans avertissement, afin qu'elles ne deviennent pas prévisibles. Les inspections doivent avoir lieu à divers endroits, notamment là où le moyen de transport est le plus vulnérable: chez le transporteur, une fois le camion chargé et, en cours d'acheminement vers la frontière des États-Unis.	Ces fouilles de contrôle des moyens de transports sont nécessaires pour contrer les complots internes. À titre de bonne pratique, les superviseurs peuvent dissimuler un objet (un jouet ou une boîte colorée, par ex.) dans le moyen de transport pour déterminer si l'agent de contrôle ou le conducteur du moyen de transport le trouve. Le personnel de supervision peut être un responsable de la sécurité qui rend ses comptes à la direction générale de la sécurité, ou un autre membre de la direction désigné à cet effet.	Recommandé
5.11	Un registre de suivi et d'activité, ou autre technologie équivalente (par exemple, GPS), doit être utilisé pour suivre le moyen de transport en route vers les États-Unis. Si des carnets de bord chauffeur sont utilisés, le chauffeur doit y consigner chaque arrêt ainsi que les inspections du moyen de transport, des instruments de trafic international (IIT) et du scellé.	Les moyens de transport sont suivis pour éviter tout détournement destiné à altérer la marchandise ou la structure du moyen de transport/instrument de trafic international pour y introduire de la marchandise de contrebande. Selon les risques, les prestataires de transports peuvent être amenés à suivre en temps réel leurs moyens de transport/instruments de trafic international. De nombreux outils de suivi sont disponibles gratuitement sur smartphone. Les petites entreprises de transport peuvent utiliser des applications comme Life 360, Find Friends from Google ou WhatsApp pour suivre des personnes ou moyens de transport.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.14	Les membres du CTPAT devraient collaborer avec leurs fournisseurs de services de transport pour suivre les moyens de transport de leur point d'origine à leur destination finale. Les exigences relatives au suivi, à la création de rapports et au partage des données doivent être spécifiées dans les modalités du contrat conclu avec les fournisseurs de services.		Recommandé
5.16	En ce qui concerne les cargaisons transitant par les frontières terrestres à proximité de la frontière des États-Unis, une politique « escales interdites » devrait être mise en place pour les escales non programmées.	Une cargaison immobilisée est une cargaison en situation de risque. Les escales programmées ne seraient pas concernées par cette politique, mais elles devraient être prises en compte dans la procédure globale de suivi et de contrôle.	Recommandé
5.19	Si un système de suivi par GPS est utilisé, les transporteurs devraient également avoir recours au couplage de capteurs entre tracteur et remorque, des capteurs connectés ou autre technologie équivalente afin que la remorque puisse également être suivie.		Recommandé
5.20	Les transporteurs devraient disposer d'un registre électronique de répartition. Ces registres devraient être conservés à des fins de vérification.	Les registres électroniques de répartition sont un outil pratique pour vérifier la bonne gestion de l'entreprise et permettre le partage et/ou le recoupement d'informations avec d'autres données d'évaluation. Il est recommandé de conserver ces registres suffisamment longtemps pour qu'ils puissent contribuer à une vérification ou à une instruction en cas d'irrégularité constatée dans une chaîne d'approvisionnement.	Recommandé
5.21	Pour les expéditions transfrontalières, un itinéraire doit être défini au préalable. Celui-ci doit comprendre une estimation du temps de parcours entre les différents points de cheminement. Une fois les temps de parcours entre les points de cheminement déterminés, à la fois pour l'heure de pointe et les heures creuses, ils doivent être enregistrés et incorporés dans la procédure de suivi.	Les points de cheminement sont des emplacements géographiques définis par un ensemble de coordonnées (latitude et longitude) à des fins de navigation, y compris le calcul d'itinéraires de transport terrestre.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
	Si la technologie GPS est utilisée, le géorepérage (geofencing) doit être employé pour émettre une notification d'alarme si le transporteur s'écarte de l'itinéraire défini au préalable. Les paramètres de géorepérage doivent être réglés au niveau de tolérance minimum vis-à-vis des écarts à l'itinéraire défini au préalable.	Pour définir les points de cheminement, il est recommandé de prendre en compte le temps de trajet entre le dépôt, le lieu de chargement/retrait de la remorque, la frontière des États-Unis et les points de livraison. Si un arrêt est nécessaire pour récupérer les documents d'exportation ou contrôler les scellés, il peut également figurer comme point de cheminement.	
5.22	Les transporteurs doivent avoir des systèmes ou procédures écrites pour réagir en cas de déviation considérable ou d'arrivée tardive au lieu de chargement, aux points de transfert ou à la destination finale. Les chauffeurs doivent informer le répartiteur en cas de retard considérable dû aux conditions météorologiques, à la circulation ou à une déviation. Le répartiteur doit vérifier de son côté le motif du retard.		Obligatoire
5.23	Après un arrêt, les chauffeurs doivent contrôler les scellés ou mécanismes de verrouillage du moyen de transport pour y détecter d'éventuels signes d'effraction avant de reprendre la route. Ces contrôles doivent être documentés.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.24	Dans les zones à haut risque, immédiatement avant l'arrivée à la frontière, les membres du CTPAT doivent incorporer une procédure de vérification dite « dernière chance » pour les expéditions à destination des États-Unis afin de détecter sur les moyens de transports/instruments de trafic international d'éventuels signes d'effraction. Cela comprend notamment un contrôle visuel des moyens de transport et un contrôle du scellé par le biais de la méthode VVTT. Les inspections doivent être effectuées par des personnes dûment formées. V – Vérifier l'intégrité du scellé et des mécanismes de verrouillage du conteneur; V – Vérifier la correspondance entre le numéro de scellé et les documents de transport; T – Tirer sur le scellé pour vérifier qu'il est correctement attaché; T – Tordre et tourner le scellé boulon pour vérifier qu'aucune partie ne se dévisse, sépare ou desserre.		Recommandé
5.26	Les chauffeurs doivent signaler et enregistrer toute anomalie ou modification structurelle inhabituelle constatée sur le moyen de transport à la suite d'une inspection menée par le gouvernement.	Cela comprend les inspections effectuées par le département des transports des États-Unis (DOT) ou toute autre agence de réglementation. Les inspections menées au Mexique et au Canada sont également concernées.	Obligatoire
5.27	La direction doit effectuer des examens aléatoires fréquents des procédures de suivi et de contrôle. Les résultats de ces examens doivent être enregistrés. L'examen doit comprendre une comparaison entre l'historique de suivi, les documents horodatés et les systèmes internes. Les délais de transit inexpliqués doivent également y figurer. La direction doit effectuer périodiquement des vérifications aléatoires en route.	Les examens aléatoires doivent permettre de vérifier la bonne tenue des registres de suivi ainsi que le respect des procédures de suivi et de contrôle des moyens de transport. Les documents horodatés comprennent les reçus pour les achats de carburant, les documents de pesée, les reçus de péage, manifestes ACE, documents du SAT mexicain, documents de courtage, etc. Les vérifications en route doivent être effectuées dans les zones à haut risque pour vérifier en temps réel le respect des procédures.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
5.28	Les transporteurs routiers CTPAT doivent informer les parties concernées (par exemple, expéditeur, destinataire, importateur) de tout retard considérable, y compris s'il est dû à une panne mécanique pendant le transport.		Recommandé
5.29	Si une menace crédible (ou détectée) à la sécurité d'une cargaison ou d'un moyen de transport est découverte, le membre doit alerter (dès que possible) tous les partenaires commerciaux de la chaîne d'approvisionnement susceptibles d'être concernés ainsi que les forces de l'ordre, le cas échéant.		Obligatoire
5.30	Toute technologie, y compris les transpondeurs, fournie par le CBP au transporteur routier, doit être protéger contre toute utilisation malveillante, compromission, vol, effraction, altération ou duplication. Toute utilisation malveillante des transpondeurs, y compris leur mise à disposition à des transporteurs tiers, verra son auteur suspendu ou exclu du programme. En outre, pour raccourcir les temps d'attente, les transporteurs CTPAT doivent payer leurs frais d'utilisation annuels ou par passage avant leur arrivée au point d'entrée.	Le transpondeur, également appelé « frais d'utilisation », est un autocollant contenant une puce d'identification par radiofréquences (RFID) qui transmet des informations à propos du véhicule, y compris sa situation relative au paiement des frais d'utilisation. Le transpondeur est collé sur le pare-brise du véhicule commercial et doit y rester pendant toute la durée de vie du transpondeur (jusqu'à 10 ans), même si le véhicule est vendu. Pour en savoir plus sur les transpondeurs, consultez le Decal and Transportation Online Procurement System (DTOPS): https://dtops.cbp.dhs.gov En payant les frais d'utilisation annuels ou par passage avant votre arrivée à la frontière, vous réduisez votre consommation de carburant et votre temps d'attente. S'ils n'ont plus besoin d'encaisser les paiements en espèces ou par carte bancaire au cours de l'inspection primaire, les agents du CBP peuvent accélérer leur traitement des véhicules entrant, ce qui réduit les émissions de CO2 associées au trafic des poids lourds.	Obligatoire

6. **<u>La sécurité des scellés</u> –** Le scellement des remorques et des conteneurs et l'intégrité permanente des scellés, continuent d'être un élément crucial de la sécurité de la chaîne d'approvisionnement. La sécurité des scellés implique d'établir une politique écrite détaillée qui aborde tous les aspects de la sécurité des scellés, notamment utiliser les scellés conformes aux exigences CTPAT, poser correctement un scellé sur l'IIT et vérifier qu'il a été correctement posé.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
6.1	Les membres du CTPAT doivent disposer de procédures écrites détaillées relatives aux scellés haute sécurité, qui doivent décrire la manière dont les scellés sont délivrés et contrôlés à l'entrepôt et pendant le transit. Les procédures doivent indiquer quelles étapes suivre si un scellé est altéré ou détérioré, ou s'il porte le mauvais numéro, en mentionnant comment documenter les faits, comment les communiquer aux partenaires et comment enquêter sur l'incident. Les constatations de l'enquête doivent être documentées et les actions correctives nécessaires doivent être appliquées aussi rapidement que possible. Ces procédures écrites doivent être conservées au niveau opérationnel local afin d'être facilement consultables. Les procédures doivent être examinées au moins une fois par an et mises à jour si nécessaire. Les procédures de contrôle des scellés doivent comprendre les éléments suivants: **Contrôle de l'accès aux scellés**: • Gestion des scellés réservée au personnel autorisé; • Entreposage en lieu sûr. **Inventaire, distribution et suivi (registre des scellés):** • Enregistrement des scellés nouvellement reçus; • Inscription des scellés délivrés dans le registre; • Suivi des scellés via le registre; • Seul le personnel autorisé et dûment formé peut poser des scellés sur un instrument de trafic international (IIT).		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
	Contrôle des scellés pendant le transit: • Lorsqu'on récupère l'IIT (ou après une escale), inspecter le scellé pour confirmer qu'il est intact et ne présente aucun signe d'altération; • Vérifier que le numéro du scellé correspond au numéro inscrit dans la documentation d'expédition. **Rupture de scellés pendant le transit:** • Si la cargaison a été examinée, enregistrer le numéro du scellé de remplacement; • En cas de scellé rompu, le chauffeur doit immédiatement en informer son répartiteur, indiquer qui l'a rompu et lui fournir le nouveau numéro de scellé; • Le transporteur doit immédiatement informer l'expéditeur, le courtier et l'importateur du changement de scellé, en leur précisant le nouveau numéro; • L'expéditeur doit noter le numéro du scellé de remplacement dans le registre des scellés. **Divergences de scellés:** • Conserver les scellés altérés ou détériorés aux fins d'enquête; • Enquêter sur les divergences; appliquer les mesures correctives (le cas échéant); • Selon le cas, signaler les scellés altérés au Service des douanes et de la protection des frontières des États-Unis et au gouvernement étranger concerné, aux fins d'enquête.		

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
6.2	Toutes les cargaisons des membres du CTPAT sur lesquelles il est possible d'apposer un scellé doivent être sécurisées immédiatement après le chargement/l'empotage/l'emballage par la partie qui en est responsable (c'est à dire, l'expéditeur ou l'emballeur agissant pour le compte de l'expéditeur) avec un scellé haute sécurité qui satisfait ou surpassent aux exigences en matière de scellés haute sécurité de la norme ISO 17712 la plus récente. Les scellés-câbles et les scellés-boulons agréés sont acceptables. Tous les scellés utilisés doivent être correctement et solidement apposés sur les instruments de trafic international qui transportent la cargaison d'un membre du CTPAT en provenance/à destination des États-Unis.	Le scellé haute sécurité doit être placé à la position « Secure Cam », le cas échéant, plutôt que sur la poignée de la porte de droite. Le scellé doit être installé en bas de la barre verticale centrale la plus à gauche de la porte de droite du conteneur. On peut également installer le scellé sur la poignée de verrouillage la plus à gauche de la porte de droite du conteneur, si la position « Secure Cam » n'est pas une option. Si l'on utilise un scellé-boulon, il est recommandé de l'installer de manière à ce que la partie cylindrique ou l'insert soit orienté vers le haut en s'assurant que la partie cylindrique soit au-dessus du moraillon.	Obligatoire
6.3	Les transporteurs par chargement partiel (CP) doivent au moins utiliser un verrou haute sécurité lorsqu'ils chargent des marchandises locales dans un environnement CP international où les hubs de groupage ne sont pas utilisés. Au dernier point de chargement avant le passage de la frontière, le transporteur doit sécuriser le chargement à l'aide d'un scellé haute sécurité conforme à la norme ISO 17712. Les transporteurs par chargement partiel doivent disposer de contrôles stricts qui limitent l'accès aux verrous, aux clés ou aux codes de déverrouillage des verrous.		Obligatoire
6.5	Les membres du CTPAT (qui gèrent des inventaires de scellés) doivent pouvoir prouver, documents à l'appui, que les scellés haute sécurité qu'ils utilisent satisfont ou surpassent aux exigences de la norme ISO 17712 la plus récente.	La copie d'un certificat d'essai de laboratoire démontrant la conformité du scellé haute sécurité aux exigences de la norme ISO est une preuve de conformité acceptable. Pour chaque scellé qu'ils utilisent, les membres du CTPAT sont censés connaître les caractéristiques indiquant s'il y a eu altération.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
6.6	Si un membre tient un inventaire des scellés, la direction de l'entreprise (ou un responsable de la sécurité) doit mener des audits des scellés exigeant un inventaire périodique des scellés en stock et le rapprochement des registres d'inventaire avec les documents d'expédition. Tous les audits doivent être documentés. Dans le cadre de la procédure globale d'audit des scellés, les superviseurs de quai et/ou les responsables d'entrepôts doivent inspecter périodiquement les numéros de scellés utilisés sur les moyens de transport et les instruments de trafic international.		Obligatoire
6.7	Il faut suivre la procédure de vérification des scellés du CTPAT pour s'assurer que tous les scellés haute sécurité (boulon/câble) ont correctement été apposés sur les instruments de trafic international et qu'ils fonctionnent comme prévu. Cette procédure est connue sous le nom de méthode VVTT. V – Vérifier l'intégrité du scellé et des mécanismes de verrouillage du conteneur; V – Vérifier la correspondance entre le numéro de scellé et les documents de transport; T – Tirer sur le scellé pour vérifier qu'il est correctement attaché; T – Tordre et tourner le scellé boulon pour vérifier qu'aucune partie ne se dévisse, sépare ou desserre.	S'il s'agit d'un scellé-câble, il doit envelopper la base rectangulaire des barres verticales afin d'empêcher tout mouvement vertical vers le haut ou le bas de la part du scellé. Une fois le scellé installé, s'assurer que tout le mou a été éliminé des deux côtés du câble. Si l'on applique la méthode VVTT à des scellés-câbles, il faut s'assurer que les câbles sont tendus. Une fois qu'il a été correctement installé, tirez sur le câble afin de déterminer s'il glisse dans le corps de verrouillage.	Obligatoire

7. **La sécurité des procédures –** La sécurité des procédures concerne de nombreux aspects des exigences relatives au processus d'importation/d'exportation, à la documentation et, à l'entreposage et la manutention des cargaisons. D'autres critères procéduraux essentiels concernent le signalement des incidents et leur notification aux forces de l'ordre concernées. En outre, le CTPAT exige souvent des procédures qu'elles soient écrites car cela contribue à l'uniformité des procédures dans le temps. Néanmoins, la quantité de détails exigée pour ces procédures écrites dépendra de plusieurs facteurs comme, par exemple, le modèle commercial de l'entreprise ou les éléments spécifiquement concernés par la procédure.

   Le CTPAT comprend que les technologies utilisées dans les chaînes d'approvisionnement continuent d'évoluer. La terminologie relative aux présents critères fait référence à des documents, formulaires et procédures écrites, mais cela ne signifie pas pour autant que ceux-ci doivent être sous format papier. Les documents et signatures électroniques, ainsi que d'autres technologies numériques, sont des supports acceptables pour documenter le respect des procédures requises.

   Le programme CTPAT n'a pas été conçu pour être un modèle « format unique ». Chaque entreprise doit décider (en fonction de son évaluation du risque) comment elle appliquera et maintiendra ces procédures. Cependant, il est plus efficace d'incorporer les procédures de sécurité aux procédures existantes, plutôt que de créer un autre manuel pour les protocoles de sécurité. Cela favorise une structure plus durable et contribue à souligner que la sécurité de la chaîne d'approvisionnement est la responsabilité de tous.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.2	Il faut régulièrement inspecter les aires de rassemblement du fret et les zones alentours pour s'assurer qu'elles n'ont pas été contaminées par des organismes nuisibles.	Si nécessaire, on peut déployer des mesures préventives comme, par exemple, utiliser des appâts ou des pièges. Désherber et tailler la végétation envahissante peut contribuer à détruire l'habitat des organismes nuisibles dans les aires de rassemblement.	Obligatoire
7.6	Des procédures doivent être mises en place pour veiller à ce que toutes les informations servant au dédouanement des marchandises soient lisibles, complètes, exactes, qu'il soit impossible de les remplacer, de les perdre ou d'y introduire des erreurs, et qu'elles soient communiquées en temps opportun.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.7	Si l'on utilise des supports papier, les formulaires et autres documents relatifs à l'importation/l'exportation doivent être sécurisés pour empêcher toute utilisation non autorisée.	On peut prendre certaines mesures (utiliser un classeur à tiroir verrouillé, par ex.) pour sécuriser les formulaires non utilisés, y compris les manifestes, afin d'empêcher l'utilisation non autorisée de ces documents.	Recommandé
7.8	L'expéditeur ou son mandataire doit s'assurer que les connaissements et/ou les manifestes reflètent avec exactitude les informations fournies au transporteur. Le transporteur doit également exercer une diligence raisonnable pour s'assurer que ces documents sont exacts. Les connaissements et manifestes doivent être enregistrés auprès du Service des douanes et de la protection des frontières des États-Unis dans les délais convenus. Les informations figurant sur les connaissements enregistrés auprès du Service des douanes et de la protection des frontières doivent indiquer le nom du premier lieu étranger où le transporteur prend possession de la cargaison à destination des États-Unis. Les informations relatives au poids et au nombre de pièces doivent être exactes.	Lorsqu'ils récupèrent des instruments de trafic international scellés, les transporteurs peuvent se fier aux informations fournies dans les consignes d'expédition de l'expéditeur. Exiger que le numéro du scellé soit imprimé électroniquement sur le connaissement (ou sur d'autres documents d'exportation) permet d'empêcher le remplacement du scellé et la modification du ou des documents afin qu'ils correspondent au nouveau numéro de scellé. Pour certaines chaînes d'approvisionnement, il se peut toutefois que les marchandises soient examinées par une autorité douanière étrangère ou par le Service des douanes et de la protection des frontières des États-Unis, pendant qu'elles sont en transit. Pour les cas où le scellé d'origine a été rompu par les autorités, il faut disposer d'une procédure permettant d'enregistrer le nouveau numéro de scellé de l'IIT après son inspection. Dans certain cas, on peut le noter manuellement.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.10	Le personnel doit examiner les informations figurant sur les documents d'importation/d'exportation pour identifier ou reconnaître toute cargaison suspecte. Le personnel concerné doit avoir été formé pour identifier toute information figurant dans les documents d'expédition (les manifestes, par ex.), qui pourrait indiquer une cargaison suspecte. Selon leur niveau de risque, les membres du CTPAT devraient prendre en compte les signaux d'alarme clés du CTPAT – en matière d'activités de blanchiment de capitaux et de financement du terrorisme – qui correspondent le plus aux fonctions qu'eux-mêmes et/ou que leurs entités commerciales exécutent dans la chaîne logistique. Un document sur les signaux d'alarme clés est disponible sur le portail CTPAT (section bibliothèque publique). Le personnel des entreprises de transport routier doit avoir été formé à l'inspection des manifestes et autres documents, afin de savoir identifier ou reconnaître toute cargaison suspecte, par exemple: • Point d'origine ou destination finale inhabituels; • Cargaison dont le transport est réglé en espèces ou par chèque certifié; • Méthodes d'acheminement inhabituelles; • Pratiques d'expédition/de réception inhabituelles; • Informations vagues, trop générales ou incomplètes.		Obligatoire
7.12	Les chauffeurs doivent jeter leurs déchets avant de pénétrer sur le territoire des États-Unis. Dans le cas contraire, les déchets doivent être déclarés au Service des douanes et de la protection des frontières des États-Unis afin d'être éliminés correctement.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.13	Selon le risque, les transporteurs routiers doivent disposer de procédures afin d'atténuer le risque de complot entre employés, par exemple, entre le chauffeur et le répartiteur, de nature à contourner les mesures de sécurité.	Par exemple, un chauffeur et un répartiteur peuvent se mettre d'accord pour falsifier les temps de parcours pour se soustraire aux procédures de suivi et de contrôle. Pour éviter toute collusion, les procédures suivantes peuvent être envisagées: restriction de l'accès des chauffeurs au bureau des répartiteurs, salles de repos séparées pour les répartiteurs et les chauffeurs, positionnement des balises GPS en dehors de la vue des chauffeurs, audits réguliers et dûment documentés des registres des répartiteurs, analyse des tendances utilisant les données GPS pour comparer le temps de parcours moyen des chauffeurs et l'identité du répartiteur en service au même moment.	Obligatoire
7.14	Si la loi et les règles syndicales le permettent, les transporteurs doivent effectuer de manière aléatoire des vérifications des bagages et effets personnels des chauffeurs. Si une anomalie est détectée au cours de cette vérification, le transporteur doit la documenter et transmettre ses constatations au Service des douanes et de la protection des frontières des États-Unis.		Recommandé
7.15	Les transporteurs routiers CTPAT doivent garantir que leurs chauffeurs certifiés FAST respectent toutes les exigences du programme FAST lorsqu'ils empruntent la file dédiée. Notamment, toutes les personnes présentes à bord de l'habitacle doivent disposer de la certification FAST.		Obligatoire
7.16	Pour les expéditions à destination des États-Unis, le transporteur routier qui transporte la marchandise (y compris les transporteurs sous-traitants) doit utiliser son propre SCAC, qu'il emprunte ou non la file FAST.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.17	Conformément aux normes du département des transports des États-Unis, les transporteurs routiers CTPAT doivent disposer d'un programme d'entretien préventif exhaustif, et s'assurer que leurs chauffeurs effectuent les vérifications adéquates sur leurs véhicules. Les registres d'entretien doivent être conservés pendant un an minimum.	Une cargaison immobilisée est une cargaison en situation de risque. Un programme d'entretien exhaustif permet d'éviter les arrêts inopinés dus à des problèmes mécaniques.	Recommandé
7.18	Dans les zones à haut risque, si possible, le transporteur routier doit transporter les marchandises par convoi (c'est-à-dire, au moins deux camions circulant ensemble). Au sein du convoi, chaque camion doit avoir un moyen de communiquer avec les autres camions du convoi et avec les répartiteurs.		Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.23	Les membres du CTPAT doivent disposer de procédures écrites en matière de signalement des incidents, lesquelles doivent décrire la procédure de communication ascendante propre à leur entreprise. Un protocole de notification doit être en place pour signaler toute activité suspecte ou tout incident de sécurité (saisie de drogues, découverte de passagers clandestins, etc.) pouvant nuire à la sécurité de la chaîne d'approvisionnement du membre. Selon le cas, le membre doit signaler un incident au spécialiste de la sécurité de sa chaîne d'approvisionnement ainsi qu'au port d'entrée le plus proche, aux services de police pertinents et aux partenaires commerciaux susceptibles d'être impliqués dans la chaîne d'approvisionnement concernée. Il convient également de notifier le Service des douanes et de la protection des frontières des États-Unis dès que possible et avant que le moyen de transport ou IIT en question traverse la frontière. Les procédures de notification doivent indiquer les coordonnées exactes (notamment les noms et numéros de téléphone) des membres du personnel à notifier, ainsi que celles des autorités policières pertinentes. Les procédures doivent être régulièrement réexaminées pour s'assurer que les coordonnées sont à jour.	Voici quelques exemples d'incidents devant être notifiés au Service des douanes et de la protection des frontières des États-Unis: • Découverte d'un conteneur/IIT ou scellé présentant des marques d'altération/d'effraction; • Découverte d'un compartiment secret dans un moyen de transport ou IIT; • Scellé inconnu apposé sur un IIT; • Trafic d'articles de contrebande et passage de clandestins; • Entrée non autorisée dans un moyen de transport ou sur une locomotive, un navire ou un porte-avions; • Extorsion, paiements en échange d'une protection, menaces et/ou intimidation; • Utilisation non autorisée d'un numéro d'identification d'entreprise (no. d'importateur officiel, Standard Carrier Alpha Code (SCAC), etc.).	Obligatoire
7.24	Des procédures doivent être en place afin d'identifier, de mettre en cause et d'aborder des personnes non autorisées/non identifiées. Le personnel doit connaître le protocole permettant de demander à toute personne inconnue/non autorisée de s'identifier, savoir comment réagir à la situation, et être apte à faire sortir des locaux tout individu non autorisé.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.25	Les membres du CTPAT devraient mettre en place un mécanisme permettant de signaler anonymement les problèmes liés à la sécurité. Toute allégation devrait faire l'objet d'une enquête et de mesures correctives, le cas échéant.	Les problèmes internes comme le vol, la fraude et les complots internes sont plus susceptibles d'être signalés si la partie déclarante sait qu'elle peut le faire de manière anonyme. Les membres peuvent mettre en place un programme d'assistance téléphonique (ou autre mécanisme similaire) permettant aux personnes de garder l'anonymat si elles craignent des représailles. Il est recommandé de conserver tous les rapports afin de documenter que chaque incident signalé a fait l'objet d'une enquête et que des mesures correctives ont été prises.	Recommandé
7.30	Les numéros de scellés devraient être électroniquement imprimés sur le connaissement ou sur les autres documents d'expédition.		Recommandé
7.31	Les transporteurs routiers CTPAT (ou autre partie autorisée à transmettre des informations au nom du transporteur) doivent transmettre un manifeste électronique pour les tracteurs circulant sans remorque et les conteneurs/remorques vides. La transmission doit s'effectuer via le manifeste électronique pour les camions (e-Manifest) de l'environnement commercial automatisé (ACE) avant l'arrivée du moyen de transport au premier point de contrôle du Service des douanes et de la protection des frontières des États-Unis.	La loi commerciale de 2002 n'oblige pas les transporteurs routiers à transmettre au préalable des informations sur les conteneurs vides au Service des douanes et de la protection des frontières des États-Unis. Seuls les conteneurs chargés doivent être signalés. Le CTPAT, en revanche, exige que le transporteur transmette les informations relatives au moyen de transport et au chauffeur avant l'arrivée du camion au point de contrôle du Service des douanes et de la protection des frontières des États-Unis.	Obligatoire
7.33	Si des transpondeurs sont utilisés, les transporteurs routiers doivent disposer d'une procédure écrite pour gérer la commande, l'émission, l'activation et la désactivation des transpondeurs. Les transporteurs routiers CTPAT ne peuvent effectuer une demande de transpondeur pour une société de transport qui n'est pas détenue et contrôlée par le transporteur membre en question.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
7.37	En cas d'incident sérieux de sécurité, les membres doivent lancer une analyse post-incident dès qu'ils prennent connaissance de l'incident et pour déterminer l'emplacement où la chaîne d'approvisionnement pourrait avoir été compromise. Cette analyse ne doit interférer ou faire obstruction à toute enquête connue menée par les services de police d'un gouvernement. Les conclusions de l'analyse post-incident enquête interne doivent être documentées, menées à bon terme dès que possible, et, si les services de police l'autorisent, mises à la disposition du SCSS, si celui-ci en fait la demande.	Un incident de sécurité est une infraction par contournement, évitement ou violation de mesures de sécurité et dont le résultat est ou sera un acte criminel. Au nombre des incidents de sécurité figurent notamment les actes de terrorisme, la contrebande (de stupéfiants, d'êtres humains, etc.) et la présence de passages clandestins	Obligatoire

8. **La sécurité agricole –** Première industrie des États-Unis, le secteur agricole est aussi le premier employeur du pays. Cette industrie est menacée par l'introduction de contaminants étrangers provenant de la faune et de la flore, tels que la terre, le fumier, les semences et les substances végétales et animales susceptibles de contenir des maladies et organismes nuisibles et destructeurs. L'élimination des contaminants dans tous les moyens de transport et tous les types de fret peut réduire la fréquence des inspections du Service des douanes et de la protection des frontières ainsi que celle des retards, retours et traitements de marchandises. En outre, garantir la conformité aux exigences agricoles du CTPAT contribuera à protéger une industrie clé aux États-Unis et l'approvisionnement alimentaire mondial.

   Définition importante: Contamination par les nuisibles –Selon la définition de l'Organisation maritime internationale, présence visible d'animaux, d'insectes ou d'autres invertébrés (vivants, morts – ou à toute autre étape de leur cycle de vie, oothèques et coques compris), de matières organiques d'origine animale (sang, os, poils, chair, sécrétions, excrétions, etc.), de plantes ou produits végétaux viables ou non viables (fruits, graines, feuilles, brindilles, racines, écorce, etc.), d'autres matières organiques (ex. champignons) et de terre ou d'eau, lorsque ces produits ne figurent pas sur le manifeste de marchandises d'un instrument de trafic international (conteneur, unité de chargement, etc.).

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
8.1	Les membres du CTPAT doivent, conformément à leur modèle commercial, disposer de procédures écrites conçues pour empêcher la contamination visible par des organismes nuisibles, procédures qui aborderont notamment la conformité à la réglementation des matériaux d'emballage en bois. Les mesures de prévention en matière d'organismes nuisibles visibles doivent être respectées tout au long de la chaîne d'approvisionnement. Les mesures s'appliquant aux matériaux d'emballage en bois doivent être conformes à la norme internationale pour les mesures phytosanitaires n°15 (NIMP 15) de la Convention internationale pour la protection des végétaux (CIPV).	On qualifie de « matériau d'emballage en bois » le bois ou les produits de bois (à l'exception des produits de papier) qui servent à soutenir, à protéger ou à transporter des biens. Les matériaux d'emballage en bois sont, entre autres, les palettes, les caisses, les boîtes, les bobines et le bois de calage. Ces articles sont fréquemment fabriqués à partir de bois brut qui n'a peut-être pas fait l'objet d'un traitement (ou d'un traitement suffisant) pour éliminer ou tuer les organismes nuisibles, lesquels peuvent donc s'y introduire et se disséminer. Le bois de calage, en particulier, présente un risque élevé d'introduction et de dissémination d'organismes nuisibles. La CIPV est un traité multilatéral supervisé par l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO), qui vise à garantir une action coordonnée et efficace pour prévenir et contrôler l'introduction et la dissémination d'organismes nuisibles et de contaminants. La NIMP 15 comprend des mesures acceptées sur le plan international qui peuvent être appliquées aux matériaux d'emballage en bois afin de réduire considérablement le risque d'introduction et de dissémination de la plupart des organismes nuisibles pouvant être associés à ces matériaux. La NIMP 15 concerne tous les matériaux d'emballage en bois et exige qu'ils soient écorcés et qu'ils subissent un traitement thermique ou une fumigation au bromure de méthyle, puis qu'on leur appose le tampon indiquant leur conformité à la CIPV. On appelle familièrement cette marque de conformité « l'épi de blé » (ou « wheat stamp » en anglais). Les produits exemptés des dispositions de la NIMP 15 sont ceux constitués de matériaux comme le papier, le métal, le plastique ou les panneaux bois (OSB, agglomérés et contreplaqués, par exemple).	Obligatoire

Troisième domaine d'intérêt: La sécurité physique et la sécurité des personnes

9. **<u>La sécurité physique</u> –** Les installations de manutention et d'entreposage des cargaisons, les zones de stockage des instruments de trafic international et les locaux dans lesquels sont préparés les documents d'importation/d'exportation – à l'intérieur du pays comme à l'étranger – doivent être équipés de barrières physiques et de moyens de dissuasion empêchant tout accès non autorisé.

   L'une des pierres angulaires du CTPAT est la souplesse: les membres devraient personnaliser leur programme de sécurité afin qu'il soit adapté aux circonstances de leur entreprise. Les besoins d'un membre en termes de sécurité physique peuvent varier considérablement en fonction de son rôle dans la chaîne d'approvisionnement, de son modèle commercial et de son niveau de risque.

   Les critères en matière de sécurité physique prévoient un certain nombre d'éléments dissuasifs/obstacles qui contribueront à empêcher tout accès injustifié au fret, aux équipements et/ou aux informations sensibles. Les membres devraient appliquer ces mesures de sécurité sur l'ensemble de leur chaîne d'approvisionnement.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.1	Toutes les installations de manutention et d'entreposage de la marchandise (garages de remorques et bureaux compris) doivent être équipées de barrières physiques et/ou de moyens de dissuasion empêchant tout accès non autorisé.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.2	Des clôtures de périmètre devraient entièrement entourer les installations de manutention et d'entreposage de la marchandise. Toute installation de manutention de la marchandise devrait être équipée d'une clôture intérieure pour sécuriser les cargaisons et leurs zones de manutention. En fonction du niveau de risque, il convient d'installer des clôtures intérieures supplémentaires pour séparer les divers types de marchandises: nationales, internationales, de grande valeur et/ou dangereuses. Les clôtures devraient être régulièrement inspectées par le personnel désigné à cet effet pour s'assurer qu'elles ne sont pas endommagées. Si l'on constate qu'une clôture est endommagée, il faut la réparer le plus rapidement possible.	Il existe d'autres types de barrière pouvant se substituer aux clôtures, comme un mur de séparation ou une caractéristique naturelle qui rend les lieux impénétrables ou bloque l'accès (une falaise abrupte ou des bosquets denses).	Recommandé
9.4	Les portes d'entrée ou de sortie des véhicules et/ou du personnel (et autres points de sortie) doivent être gardées ou surveillées. Toute personne et véhicule peut faire l'objet d'une fouille, conformément à la législation locale et à la législation du travail.	Il est recommandé de limiter le nombre de barrières au minimum nécessaire pour permettre l'accès et garantir la sécurité. Les autres points de sortie sont les entrées sans barrière.	Obligatoire
9.5	Il devrait être interdit aux véhicules à passagers privés de stationner dans les zones de manutention et d'entreposage des cargaisons et moyens de transport, ou à proximité de celles-ci.	Il convient d'aménager les aires de stationnement en dehors des zones clôturées et/ou opérationnelles ou, tout du moins, à une bonne distance des zones de manutention et d'entreposage du fret.	Recommandé
9.6	L'intérieur et l'extérieur des installations doivent être adéquatement éclairés, notamment les zones suivantes: entrées et sorties, zones de manutention et d'entreposage de la cargaison, lignes de clôture et aires de stationnement.	Les minuteries ou détecteurs de mouvement qui allument automatiquement les lampes de sécurité sont des ajouts utiles aux appareils d'éclairage.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.7	Il convient d'installer des technologies de sécurité pour surveiller les locaux et empêcher tout accès non autorisé aux zones sensibles.	Les technologies de sécurité électronique utilisées pour sécuriser/surveiller les zones et points d'accès sensibles comprennent: les systèmes d'alarme anti-intrusion (périmètre et intérieur), également appelés systèmes de détection d'intrusion ou IDS, les dispositifs de contrôle d'accès et les systèmes de vidéosurveillance (VS), y compris les caméras de télévision en circuit fermé (CCTV). Un système de CCTV/VS peut être constitué, entre autres, de caméras analogiques (avec câble coaxial), de caméras IP (sur le réseau), de dispositifs d'enregistrement et de logiciels de gestion vidéo. Les zones sécurisées/sensibles pouvant bénéficier d'une vidéosurveillance sont, entre autres: les zones de manutention et d'entreposage de la marchandise, les zones d'expédition/de réception où sont conservés les documents d'importation, les serveurs informatiques, les parcs et aires d'entreposage des instruments de trafic international (IIT), les zones d'inspection des IIT et les zones d'entreposage des scellés.	Recommandé
9.8	Les membres utilisent des technologies de sécurité pour assurer la sécurité physique doivent disposer de politiques et de procédures écrites régissant l'utilisation, la maintenance et la protection de ces technologies. Au minimum, ces politiques et procédures doivent stipuler: • Que l'accès aux sites de commande/de gestion des technologies et	Les technologies de sécurité doivent être régulièrement testées pour s'assurer de leur bon fonctionnement. Il y a des directives générales à suivre: • Tester les systèmes de sécurité après toute tâche de maintenance ainsi que pendant et après toute réparation, modification ou ajout important apporté à un bâtiment ou une installation. L'un des composants du système peut avoir été compromis, intentionnellement ou non;	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
	d'entreposage du matériel connexe (panneaux de commande, unités d'enregistrement vidéo, etc.) est limité au personnel autorisé; • Les procédures mises en place pour régulièrement tester/inspecter les technologies; • Que les inspections impliquent de vérifier le bon fonctionnement du matériel et, le cas échéant, que celui-ci est correctement positionné; • Que les résultats des inspections et tests de performance doivent être documentés; • Que si des actions correctives sont nécessaires, elles doivent être mises en œuvre dès que possible puis documentées; • Que les résultats des inspections soient conservés suffisamment longtemps aux fins d'audit. Si un membre du CTPAT utilise la station de surveillance centrale (hors site) d'un tiers, il doit disposer de procédures écrites stipulant les fonctionnalités essentielles du système et les protocoles d'authentification, comme – entre autres – les modifications des codes de sécurité, l'ajout ou le retrait de personnel autorisé, les modifications des mots de passe et les accès système autorisés ou refusés. Les politiques et procédures afférentes aux technologies de sécurité doivent être réexaminées une fois par an, voire plus fréquemment en fonction des circonstances et des facteurs de risque.	• Tester les systèmes de sécurité après toute modification importante des services téléphoniques ou internet. Tout ce qui pourrait affecter la capacité du système à communiquer avec le centre de surveillance mérite une double vérification; • S'assurer que les paramètres vidéo ont correctement été configurés: enregistrement activé par mouvement, notifications de détection de mouvement, images par seconde (IPS) et niveau de qualité; • S'assurer que les objectifs des caméras (ou les globes protégeant les objectifs) sont propres et que leurs images sont nettes. La visibilité ne doit pas être entravée par des obstacles ou des lumières vives; • Effectuer un test pour s'assurer que les caméras de sécurité sont correctement orientées et qu'elles le restent (l'orientation d'une caméra peut avoir été délibérément ou accidentellement modifiée).	

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.9	Les membres du CTPAT devraient utiliser des ressources sous licence/certifiées pour la conception et l'installation de leurs technologies de sécurité.	Les technologies de sécurité actuelles sont complexes et en constante évolution. Il arrive souvent que les entreprises acquièrent les mauvaises technologies de sécurité, lesquelles s'avèrent soit inefficaces soit plus coûteuses que nécessaire. Un acquéreur devrait employer les services d'un professionnel pour choisir les options technologiques adaptées à ses besoins et à son budget. Selon la National Electrical Contractors Association (NECA), il y a, aux États-Unis, 33 États qui imposent actuellement des exigences en matière de licence pour les professionnels impliqués dans l'installation des systèmes de sécurité et d'alarme.	Recommandé
9.10	Toute infrastructure technologique de sécurité doit être physiquement sécurisée contre les accès non autorisés.	L'infrastructure technologique de sécurité comprend les ordinateurs, les logiciels de sécurité, les panneaux de commande électroniques, les caméras de vidéosurveillance ou de télévision en circuit fermé, les composants d'alimentation électrique et disques dur des caméras, et les enregistrements.	Obligatoire
9.11	Les systèmes technologiques de sécurité doivent être équipés d'une source d'alimentation de secours leur permettant de continuer à fonctionner en cas de panne de courant.	Un criminel tentant de neutraliser votre sécurité pourra essayer de désactiver votre alimentation électrique afin de contourner vos dispositifs. C'est pourquoi il est important d'installer une source de secours qui, le cas échéant, alimentera vos technologies de sécurité. Les groupes électrogènes d'appoint et les batteries de secours constituent des sources d'alimentation de secours acceptables. On peut également utiliser des générateurs de secours pour d'autres systèmes importants comme l'éclairage.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.12	Si le site est équipé d'un système de vidéosurveillance, les caméras devraient surveiller les locaux et les zones sensibles afin de dissuader tout accès non autorisé. Il convient d'utiliser des alarmes pour prévenir les responsables en cas d'accès non autorisé dans une zone sensible.	En fonction du site, les zones sensibles sont, entre autres: les zones de manutention et d'entreposage de la marchandise, les zones d'expédition/de réception où sont conservés les documents d'importation, les serveurs informatiques, les parcs et aires d'entreposage des instruments de trafic international (IIT), les zones d'inspection des IIT et les zones d'entreposage des scellés.	Recommandé
9.13	Si le site est équipé d'un système de vidéosurveillance, les cameras doivent être orientées sur les zones clés qui concernent le processus d'importation/d'exportation. Les caméras devraient être configurées sur la plus haute qualité d'image possible et programmées pour enregistrer en permanence.	Il est important de bien positionner les caméras afin qu'elles puissent enregistrer autant que possible la « chaîne de possession » telle qu'elle se produit sur le site. En fonction du risque, les zones et processus clés peuvent comprendre les aires de manutention et d'entreposage de la cargaison, les aires d'expédition/de réception, les aires de chargement des marchandises, les aires de scellement, les aires d'arrivée/de sortie des moyens de transport, les serveurs informatiques, les zones d'inspection (de sécurité/agricole) des conteneurs et les zones d'entreposage des scellés, ainsi que toute autre zone liée à la sécurisation du fret international.	Obligatoire
9.14	Si le site est équipé d'un système de vidéosurveillance, les caméras devraient être configurées de manière à émettre une alarme ou une notification en cas de « panne d'enregistrement/de fonctionnement ».	Une panne du système de vidéosurveillance peut indiquer qu'il a volontairement été désactivé pour empêcher toute preuve vidéo en cas d'atteinte à la chaîne d'approvisionnement. En cas de panne de fonctionnement, une notification électronique peut être envoyée aux personnes préalablement désignées pour les prévenir que le périphérique nécessite une intervention immédiate.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
9.15	Si le site est équipé d'un système de vidéosurveillance, les responsables (cadres supérieurs, responsables de la sécurité ou tout autre personnel désigné à cet effet) doivent examiner périodiquement et aléatoirement les séquences filmées pour s'assurer que les procédures de sécurité relatives au fret sont appliquées conformément à la loi. Les résultats de ces examens doivent être résumés par écrit et mentionner toutes les mesures correctives prises, le cas échéant. Il convient de conserver les résultats suffisamment longtemps à des fins d'audit.	Une entreprise qui examine uniquement les séquences enregistrées quand un problème survient (dans le cadre d'une enquête, à la suite d'une atteinte à la sécurité, etc.) ne tire pas pleinement profit de son système de vidéosurveillance. Les caméras ne sont pas seulement des outils d'investigation. Si elles sont utilisées de manière proactive, elles peuvent également contribuer à prévenir toute atteinte à la sécurité. Il est recommandé de concentrer son attention sur les séquences filmant la chaîne de possession physique pour s'assurer que le fret a été sécurisé en permanence et que tous les protocoles de sécurité ont été suivis. Voici quelques exemples de procédures filmées à examiner: • Les activités de manutention de la marchandise; • Les inspections de conteneurs; • Le chargement; • Le scellement; • L'arrivée/le départ des moyens de transport; • Le départ de la cargaison; **Objectif de l'examen:** Ces examens ont pour objet de contrôler si les procédures de sécurité établies sont suivies et efficaces, d'identifier d'éventuelles lacunes ou faiblesses et, de prescrire des actions correctives en vue de l'amélioration de ces procédures. Selon le niveau de risque (en cas d'incidents antérieurs ou si quelqu'un a anonymement signalé qu'un employé ne respecte pas les protocoles de sécurité sur le quai de chargement, par ex.), le membre pourra opter pour des examens plus réguliers.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
		Informations à fournir dans le résumé écrit: • La date de l'examen; • La date d'enregistrement de la séquence; • Les caméras et zones concernées; • Une courte description des constatations; • Les actions correctives entreprises, le cas échéant.	
9.16	Si le site est équipé de caméras, les séquences montrant les procédures clés d'importation/d'exportation devraient être conservées suffisamment longtemps à des fins d'enquête, en cas de cargaison surveillée.	En cas de problème, une enquête devrait être menée. C'est pourquoi toutes les séquences montrant l'emballage (pour l'exportation) et le chargement/scellement seraient primordiales pour déterminer à quel endroit la chaîne d'approvisionnement a pu être compromise. Certains experts recommandent d'attendre au moins 14 jours après que la cargaison surveillée est arrivée au premier point de distribution. C'est à ce moment que le conteneur est ouvert pour la première fois après le dédouanement.	Recommandé

10. **<u>Les contrôles d'accès physique</u> –** Les contrôles d'accès empêchent la pénétration non autorisée à l'intérieur des installations/zones, contribuent à maintenir le contrôle des employés et des visiteurs et protègent les biens de l'entreprise. Les contrôles d'accès exigent l'identification positive de tous les employés, visiteurs, prestataires de services et distributeurs à tous les points d'entrée.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
10.1	Les membres du CTPAT doivent disposer de procédures écrites régissant comment octroyer, modifier et retirer les badges d'identification et dispositifs d'accès. S'il y a lieu, un système d'identification du personnel doit être mis en place aux fins d'identification positive et de contrôle d'accès. L'accès aux zones sensibles doit être limité en fonction de la description de poste des employés ou des tâches qui leur sont assignées. Le dispositif d'accès d'un employé doit lui être retiré lorsqu'il quitte l'entreprise.	Les dispositifs d'accès sont, entre autres: les badges d'identification des employés, les badges temporaires des visiteurs et des fournisseurs, les systèmes d'identification biométrique, les cartes-clés de proximité, les codes et les clés. Lorsqu'un employé quitte l'entreprise, utiliser une liste de vérification permet de s'assurer que tous les dispositifs d'accès ont été désactivés ou rendus à l'entreprise. Les petites entreprises, où le personnel se connaît, n'ont pas besoin d'un système d'identification. D'une manière générale, une entreprise de plus de 50 employés devra recourir à un système d'identification.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
10.2	Les visiteurs, les distributeurs et les prestataires de services doivent présenter une pièce d'identité avec photo à leur arrivée et un registre spécifiant les détails de leurs visites doit être tenu. Tous les visiteurs devraient être escortés. En outre, tous les visiteurs et prestataires de services devraient recevoir un badge d'identification temporaire. Les personnes ayant reçu un badge d'identification temporaire doivent constamment le porter de manière visible pendant leur visite. Le registre des visites doit préciser les informations suivantes: • La date de la visite; • Le nom du visiteur; • Le type de pièce d'identité avec photo qui a été vérifié (permis de conduire ou carte nationale d'identité). Il n'est pas nécessaire que les visiteurs fréquents et bien connus de l'entreprise (les distributeurs habituels, par ex.) présentent leur pièce d'identité avec photo à chaque visite, mais leurs entrées et sorties du site doivent être consignées dans le registre de la manière suivante: • Heure d'arrivée; • Nom du contact dans l'entreprise; • Heure de sortie.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
10.3	Les chauffeurs qui livrent ou qui reçoivent du fret doivent être clairement identifiés avant la réception ou la livraison du fret. Les chauffeurs doivent présenter une pièce d'identité officielle (avec photo) à l'employé chargé d'autoriser l'accès afin qu'il puisse confirmer leur identité. Si le chauffeur n'est pas en mesure de présenter une pièce d'identité officielle, l'employé chargé de l'accès peut accepter une pièce d'identité avec photo délivrée par le transporteur routier qui emploie le chauffeur.		Obligatoire
10.7	Avant l'arrivée, le transporteur doit indiquer à l'entreprise l'heure approximative à laquelle son chauffeur devrait se présenter pour récupérer la marchandise, ainsi que son nom et le numéro de son camion. Dans la mesure du possible, les membres du CTPAT ne devraient autoriser les livraisons et ramassages que sur rendez-vous.	Ce critère aidera les expéditeurs et les transporteurs à éviter les ramassages frauduleux. Les ramassages frauduleux sont des opérations criminelles visant à dérober la cargaison par la tromperie: un chauffeur présentant une fausse pièce d'identité et/ou une entreprise de transport fictive créée uniquement pour se livrer au vol de marchandise. Lorsqu'un transporteur emploie régulièrement les mêmes chauffeurs pour venir récupérer les marchandises, une bonne pratique consiste à dresser une liste de ces chauffeurs avec leurs photos. Ainsi, si le transporteur n'est pas en mesure d'indiquer lequel de ses chauffeurs il enverra, l'entreprise pourra vérifier que le chauffeur qui se présente figure bien sur la liste des chauffeurs autorisés à venir chercher les cargaisons.	Recommandé
10.8	Il faut régulièrement inspecter les colis et le courrier à l'arrivée avant de les accepter, pour confirmer qu'ils ne contiennent pas d'articles de contrebande.	Les articles de contrebande sont, entre autres, les explosifs, les drogues illicites et l'argent en espèces.	Recommandé
10.10	Si l'entreprise emploie des agents de sécurité, les consignes de travail de ces derniers doivent figurer dans les politiques et procédures écrites. La direction doit régulièrement vérifier – par le biais d'audits et d'examens des politiques – que ces procédures sont respectées et qu'elles restent pertinentes.	Les agents de sécurité peuvent être présents dans tout type d'installations, cependant, ils sont souvent employés dans les sites de fabrication, les ports maritimes, les centres de distribution, les entrepôts pour instruments de trafic international, les entrepôts de groupage et les sites des transitaires.	Obligatoire

11. <u>La sécurité du personnel</u> – Les ressources humaines d'une entreprise constituent l'un de ses atouts les plus essentiels, mais elles peuvent être également l'un de ses maillons les plus faibles en matière de sécurité. Les critères de la présente catégorie abordent, entre autres, les procédures de vérification des employés avant et pendant leur service dans l'entreprise.

Les atteintes à la sécurité sont fréquemment le résultat d'un complot interne: un ou plusieurs employés conspirent pour contourner les procédures de sécurité et, ainsi, permettre une infiltration de la chaîne d'approvisionnement. Par conséquent, les membres doivent exercer une diligence raisonnable pour vérifier que les employés qui occupent des postes sensibles sont fiables et dignes de confiance. Les postes sensibles sont ceux impliquant une manutention directe du fret ou de sa documentation ainsi que le contrôle de l'accès aux zones ou équipements sensibles. Les employés occupant ces types de poste sont, entre autres, les préposés à l'expédition, à la réception et au courrier, les chauffeurs, les répartiteurs, les agents de sécurité ainsi que toute personne chargée de l'affectation du personnel de chargement, du suivi des moyens de transport et/ou du contrôle des scellés.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
11.1	Des procédures écrites doivent être mises en place afin de passer au crible les employés potentiels et de contrôler périodiquement les employés actuels. Les informations des postulants, telles que leurs antécédents professionnels et leurs références, doivent être confirmées avant l'embauche, dans la mesure du possible et conformément à la loi.	Le CTPAT comprend que, dans certains pays, les lois relatives au travail et à la protection de la vie privée n'autorisent pas toujours la vérification de certaines des informations figurant sur les formulaires de candidature. Néanmoins, il convient d'exercer une diligence raisonnable pour confirmer la véracité des informations fournies par le postulant lorsque cela est permis.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
11.2	Il convient de mener des enquêtes sur les antécédents judiciaires des employés, dans le respect des restrictions juridiques applicables et selon la disponibilité des vérifications de casier judiciaire. En fonction de la sensibilité du poste, les exigences en matière de vérification des employés devraient également s'appliquer au personnel intérimaire et aux entrepreneurs. De nouvelles enquêtes devraient être effectuées régulièrement si le poste est de nature sensible et/ou en cas de motif valable. La vérification des antécédents des employés devrait inclure la vérification de leur identité et des antécédents judiciaires aux niveaux municipal, départemental, régional et national, le cas échéant. Les membres du CTPAT et leurs partenaires commerciaux devraient prendre en compte – dans le respect de la législation locale – les résultats de la vérification des antécédents lorsqu'ils prennent leurs décisions d'embauche. La vérification des antécédents ne se limitent pas à la vérification de l'identité et du casier judiciaire. Dans les domaines plus à risque, des enquêtes plus approfondies peuvent être justifiées.		Recommandé
11.5	Les membres du CTPAT doivent disposer d'un code de conduite à l'intention des employés. Celui-ci doit définir les attentes de l'entreprise vis-à-vis des employés ainsi que les comportements considérés comme acceptables. Les sanctions et procédures disciplinaires prévues par l'entreprise doivent figurer dans le code de conduite. Les employés et sous-traitants doivent signer le code de conduite pour confirmer qu'ils l'ont lu et compris. Cette confirmation doit être conservée dans le dossier de l'employé à des fins documentaires.	L'existence d'un code de conduite protège votre entreprise et informe les employés des attentes de l'entreprise vis-à-vis d'eux. Son objectif est d'élaborer et de perpétuer des normes de bonne conduite au sein de l'entreprise. Cela permet également aux entreprises de développer une image professionnelle et d'instiller une robuste culture de déontologie. Même les petites entreprises doivent se doter d'un code de conduite, même s'il n'est pas particulièrement complexe par sa structure ou son contenu.	Obligatoire

12. <u>La formation et la sensibilisation</u> – Les critères de sécurité du CTPAT ont été conçus pour former le socle d'un système de sécurité multi-strates. Si l'une des strates du système de sécurité est neutralisée, une autre strate devrait intervenir pour empêcher toute atteinte à la sécurité ou pour alerter l'entreprise. La mise en œuvre et le bon fonctionnement d'un programme de sécurité multi-strates nécessitent la participation active et le soutien de plusieurs services et de divers employés.

La formation constitue l'un des aspects clés du bon fonctionnement d'un programme de sécurité. Former les employés aux menaces existantes et au rôle important qu'ils jouent dans la protection de la chaîne d'approvisionnement de leur entreprise est primordial pour garantir le succès et la pérennité d'un programme de sécurité d'une chaîne d'approvisionnement. Par ailleurs, lorsque les employés comprennent la nécessité des procédures de sécurité, ils sont beaucoup plus susceptibles de les respecter.

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
12.1	Les membres doivent établir et maintenir un programme de formation et de sensibilisation à la sécurité afin que les employés sachent reconnaître, à chaque étape de la chaîne d'approvisionnement, les vulnérabilités en matière de sécurité des installations, des moyens de transport et du fret pouvant être exploitées par des terroristes ou des contrebandiers. Le programme de formation doit être complet et couvrir toutes les exigences du CTPAT en matière de sécurité. Le personnel occupant des postes sensibles doit recevoir une formation spécialisée supplémentaire axée sur les responsabilités spécifiques aux postes. La formation est l'un des aspects clés d'un programme de sécurité. Lorsque les employés comprennent pourquoi les procédures de sécurité sont nécessaires, ils sont plus susceptibles de les respecter. La formation à la sécurité doit être régulièrement dispensée aux employés, selon leurs fonctions et leurs postes, et les nouveaux employés doivent suivre cette formation dans le cadre de leur orientation/formation professionnelle. Les membres doivent conserver des preuves des formations dispensées (registres, listes de présence signées par les participants, dossiers électroniques, etc.) Les dossiers de formation devraient indiquer la date de la formation, le nom des participants et les thèmes abordés.	Les sujets de formation peuvent aborder, entre autres, la protection des contrôles d'accès, l'identification des complots internes et les procédures de signalement des activités suspectes et incidents de sécurité. Dans la mesure du possible, une formation spécialisée devrait comprendre une démonstration pratique. Lors de celle-ci, l'instructeur devrait donner aux participants le temps de faire une démonstration de la procédure étudiée. Dans le cadre du programme CTPAT, les postes sensibles sont ceux impliquant une manutention directe du fret d'importation/d'exportation, ou de sa documentation, ainsi que le contrôle de l'accès aux zones ou équipements sensibles. Les employés occupant ces types de poste sont, entre autres, les préposés à l'expédition, à la réception et au courrier, les chauffeurs, les répartiteurs, les agents de sécurité ainsi que toute personne chargée de l'affectation du personnel de chargement, du suivi des moyens de transport et/ou de contrôle des scellés.	Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
12.2	Les chauffeurs et autres membres du personnel chargés des inspections de sécurité et des inspections agricoles des moyens de transport et des instruments de trafic international (IIT) vides doivent avoir été formés à l'inspection de leurs moyens de transport/IIT à des fins de sécurité générale et agricole. Des formations d'appoint doivent être dispensées périodiquement, après un incident ou une atteinte à la sécurité – si nécessaire, ou encore si les procédures de l'entreprise ont été modifiées. La formation à l'inspection doit aborder les sujets suivants: • Les signes indiquant un compartiment secret; • La dissimulation d'articles de contrebande dans les compartiments connus; • Les signes d'une contamination par des organismes nuisibles.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
12.3	Le personnel doit être formé à l'établissement de rapports de situation, c'est-à-dire, aux procédures à suivre si une anomalie est détectée pendant l'inspection d'un moyen de transport ou si un incident de sécurité se déclare pendant le transit. En outre, le personnel doit être formé au contrôle et à l'utilisation des scellés pendant le transit, et à la détection d'individus qui observeraient les déplacements du moyen de transport et/ou des marchandises. Par exemple, les chauffeurs doivent être formés à l'exécution de la méthode VVTT pour le contrôle des scellés. La procédure de vérification des scellés dans le cadre du programme CTPAT est la suivante: V – Vérifier l'intégrité du scellé et des mécanismes de verrouillage du conteneur; V – Vérifier la correspondance entre le numéro de scellé et les documents de transport; T – Tirer sur le scellé pour vérifier qu'il est correctement attaché; et T – Tordre et tourner le scellé boulon pour vérifier qu'aucune partie ne se dévisse ou ne se sépare.		Obligatoire
12.4	Les membres du CTPAT devraient avoir mis en place des mesures pour vérifier que les formations dispensées répondent à tous les objectifs énoncés.	Comprendre les enseignements de la formation et pouvoir les utiliser dans le cadre de ses fonctions (pour les employés occupant un poste sensible) est d'une importance capitale. Des examens ou quiz, des exercices de simulation, des contrôles réguliers des procédures (etc.) font partie des outils qu'un membre peut utiliser pour déterminer l'efficacité de sa formation.	Recommandé

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
12.7	Conformément à son modèle commercial, le membre doit dispenser une formation à la prévention en matière de contamination par des organismes nuisibles visibles au personnel concerné. La formation doit aborder les mesures de prévention relatives aux organismes nuisibles, les exigences réglementaires applicables aux matériaux d'emballage en bois et, la détection du bois infesté.	Le Service des douanes et de la protection des frontières et le département de l'agriculture des États-Unis ont élaboré conjointement une formation portant sur la contamination par des organismes nuisibles visibles. Plusieurs modules de formation ont été développés pour les différents environnements commerciaux: frontières aériennes, frontières maritimes et frontières terrestres (transporteur ferroviaire et routier). Tous les membres pourront accéder à ces modules de formation via le portail du CTPAT.	Obligatoire
12.8	Selon leurs fonctions et/ou leurs postes, les employés doivent être formés aux politiques et procédures de l'entreprise en matière de cybersécurité. Notamment, la nécessité pour les employés de protéger les mots de passe/phrases passe et l'accès à l'informatique.	Il est important de dispenser des formations de qualité pour atténuer les vulnérabilités aux cyberattaques. Un solide programme de formation en cybersécurité se doit d'être dispensé au personnel concerné dans un cadre formel plutôt que par simple courrier électronique ou circulaire.	Obligatoire
12.9	Le personnel en charge de l'exploitation et de la gestion des systèmes technologiques de sécurité doit avoir suivi une formation relative à leur fonctionnement et leur entretien. Une expérience antérieure avec des systèmes similaires est acceptable. L'autoformation avec des manuels d'exploitation et d'autres méthodes est également acceptable.		Obligatoire

Id.	Critère	Conseils de mise en œuvre	Obligatoire/ recommandé
12.10	Le personnel doit être formé sur la manière de signaler les incidents de sécurité et les activités suspectes.	Les procédures de signalement des incidents de sécurité et activités suspectes sont des éléments extrêmement importants d'un programme de sécurité. Toute formation s'y rapportant peut être intégrée à la formation générale sur la sécurité. Les modules de formation spécialisée (élaborés pour des postes spécifiques) peuvent comprendre plus de détails sur les procédures de signalement, en indiquant, par exemple, ce qu'il convient de signaler, à qui et comment, ainsi que le suivi à effectuer.	Obligatoire

Publication Number – 1089-0420