#	CRITERIA	GUIDANCE	CHANGE	Reqd Optional	DEPT & OWNER	DUE	COMPLETE
1	Signed statement of commitment / support of the C-TPAT program issued by senior company official(s and displayed throughout the organisation	Statement should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Post in reception, warehouse and present in company meetings	Addition	O		-	
2	Develop a cross functional team from all relevant departments	Supply Chain Security has a much broader scope than traditional security programs; it intertwines through many depts., along with security including HR, IT, import / export offices. Supply Chain Security programs built on a more traditional Security – Dept model are susceptible to failure over the long term as a result of staff turnover	Addition	O			
3	Implementing the correct framework for a security program is important for its success. To ensure a program's continuity, a written multi-level review / assessment process, which includes a system of checks and balances and accountability must be integrated into the security framework in order to verify that the program continues to operate as designed	Create an audit / review structure that corresponds to the levels of management in the company. Supervisors audit / review their direct reports; supervisors are audited / reviewed by the next level of management up to the most senior management. For members with high risk supply chains based on their risk assessments, simulation or table top exercises may be a part of the targeted check to ensure personnel will know how to react in the event of a real security incident	Addition	R			

4	The role of a company's upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company's supply chain security program. To this end, the CTPAT Points of Contact (POC) must provide regular updates regarding the progress of r outcomes of any audits, exercises or validations. The POCs must be knowledgeable about CTPATs program requirements. In addition this person must be capable of making decisions on behalf of the company in CTPAT matters	CTPAT expects the designated POC to be a proactive individual who engages and is responsive to his or her Supply Chain Security Specialist. Members may identify individuals who may help support this function by listing them as contact in the CTPAT portal	Expanded	Reqd			
5	CTPAT members must conduct and document an overall risk assessment (RA) to identify where vulnerabilities may exist. The RA must identify threats, quantify risks and incorporate sustainable measures to mitigate vulnerabilities specific to the members role in the supply chain	The overall risk assessment is made up of two key parts. The first part is the self-assessment of the member's supply chain security practices, procedures and policies with the facilities that it controls to verify its adherence to CTPAT's Minimum Security Criteria, and an overall management review of how it is managing risk The 2nd part of the RA is the international risk assessment. This portion of the RA includes the identification of geographical threat(s) based on the Member's business model and role in the supply chain, and a process to quantify the possible supply impact of each threat on the security of the Member's supply chain CTPAT developed the *Five Step Risk Assessment* guide as an aid to conducting the international risk assessment portion of a Member's overall risk assessment, and if it can be found at the CBP's website: https://www.cbp.gov/sites/default/fil	Expanded	Req'd			

		es/documents/C-TPAT%27%20%Five%20Step%20Risk%20Assessment%20Process.pdf					
6	The overall risk assessment must incorporate site-specific vulnerabilities applicable to the Member's role in the supply chain, including the extent to which the CTPAT Member relies on third parties with access to the Member's export and cargo loading operations, both inbound and outbound, as applicable.	Third Parties may include seasonal dockworkers, janitorial services, contracted IT provers etc.	Expanded	Reqd			
7							
8	Risk Assessments must be reviewed annually, or more frequently, as risk factors dictate	Circumstances that may require a risk assessment to be reviewed more frequently than once a year include an increased threat from a specific country, periods of heightened alerts, following a security breach, or incident, changes in business partners and or changes in corporate structure / ownership such as mergers and / or acquisitions etc	No change	Reqd			
9	CTPAT Members should have written procedures in place that address crisis, management business continuity security recovery plans and business resumption	A crisis may include a disruption of the movement of trade data due to a cyber-attack, a fire or a carrier driver being hijacked by armed individual. Based on risk and where the Member operates or sources from, contingency plans may include additional security notifications or support and how to recover what was destroyed or stolen and get back to normal operating conditions	Addition	O			
10	CTPAT members must have a written risk based process for screening new business partners and for monitoring current partners. Factors that must be included in this process are checks on the	Vetting the legitimacy of business partners is very important. Criminals often pose as a legitimate business by creating a fake or shell company. The	Expanded	Req'd			

	financial soundness of the business and activity related to money laundering and terrorist funding	fake company may portray itself as an Exporter / Importer or agent representing a company or consortium of small businesses, Or pretend to be a legitimate trucking company a fake company might sign up with a freight broker to perpetrate fictitious or fraudulent pickup. If your company uses the services of a freight broker this is a growing industrywide threat to consider in your risk assessment, The following are some of the vetting elements that can help determine if a company is legitimate. *Verifying the company's business and how long they have been at that address *Verifying landline phone numbers Conducting research on the internet on both the company and its principals; and, *Checking business references To help with this process, Members are encouraged to consult the document *CTPAT's Warning Indicators for Trade Based Money Laundering and Terrorism Financing*					
11							
12	Written screening processes must include indicators to identify shipments or customers that might not be legitimate. If a higher risk factor is flagged when screening a shipment / customer, the carrier must complete a more in-depth review. If vetting leads to substantial doubt as to the	Some of the warning sign could be willing to pay above standard rate, in cash; having little knowledge of the commodity to be shipped; being evasive; minimal contact information	No change	Reqd			

	veracity of the shipment / customer, the carrier must notify US Customs and Border Protection of its suspicions.	(cell phone PO box #) new business / no business history etc.					
13	Members may choose to accept their business partner's certification on CTPAT or an approved Authorised Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) witch the United States as roof of meeting CTPAT's security criteria. However, Members must obtain evidence of the certification as proof of compliance and must continue to monitor these business partners to ensure they maintain their certification	Business Partners CTPAT certification may be ascertained by the CTPAT portal Status Verification Interface System. If the business partner certification is from a foreign AEO program under an MA with the United States, the foreign AEO certification will include the security component, Members may visit the foreign Customs Administration website where the names of the AEO's of that Customs Administration are listed, or request the certification directly from their business partners. Current United States MRA's include: New Zealand, Canada, Jordan, Japan, South Korea, The EU, Taiwan, Israel, Mexico, Singapore and the Dominican Republic.	Expanded	Reqd			
14							
15	If security questionnaires are used to ascertain business partner compliance with CTPAT's security requirements, questionnaire responses must be detailed and if necessary supported by documentary evidence. Security Questionnaires used to determine and document compliance with the program's security criteria must include the following: *Name and title of person completing it *Date Completed *Signature of the individual(s) who completed it	Due to their role in the supply chain some companies may receive numerous questionnaires. CTPAT does not wish to create an undue burden on these companies; therefore Members may be flexible in obtaining needed information. For example an already completed questionnaire from another company may be accepted or a business partner may provide its own document that describes how it meets the program's security requirements.	New	Reqd			

	*signature of a senior company official, security advisor, or authorised company representative to attest to the accuracy of the questionnaire; *provide enough detail in response to determine compliance; and * If allowed by local security protocols, include photographic evidence, copies of policies / procedures, and copies of completed forms like IIT inspections checklists and or guard logs.						
16							
17	Based upon documented risk assessment processes, CTPAT members should require business partners to update their security self-assessments on a regular basis, or as circumstances / risk dictate	Periodic updates to the self-assessment are important to ensure that a strong security program is still in place and operating properly. Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country changes in source location, new critical business partners (those that actually handle the cargo, provide security to a facility)	New	O			
18	For inbound shipments to the US, if a member subcontracts transportation services to another highway carrier, the member must use a CTPAT certified carrier, or a highway carrier that works directly for the member as delineated through a written contract. The contract must stipulate that the subcontracted carrier must follow all MSC requirements. Members must vet their subcontracted Carriers and ensure they comply with all program requirements. Once a subcontracted carrier has been approved, it will be added to a list of approved subcontracted carriers.	Periodic review of the security commitments of the service providers maybe conducted to include verifying that the company subcontracted is actually the company transporting the load. The member may limit subcontracting transportation services to one level only. If exceptions are allowed for further subcontracting, the CTPAT member and this shipper may be notified that the load was further subcontracted. The carrier may provide a list of subcontracted carriers and drivers to the facilities where it picks up and	Expanded	Reqd			

		delivers cargo. Any changes to the subcontractor list may be conveyed to relevant parties					
19	CTPAT Members must have comprehensive written cybersecurity policies and procedures to protect information technology systems. The written IT policy at a minimum must cover all of the individual cyber security criteria.	Members are encourage to follow the National Institute of Standards and Technology's voluntary risk-based Framework for Improving Critical Infrastructure Cybersecurity https://www.nist.gov/cyberframework A set of industry standards and best practices which help organisation manage cyber risks. This framework provides a common language for understanding, managing and expressing cybersecurity risk, both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risks and it is a tool for aligning policy, business and technological approached to managing that risk. The Framework complements but does not replace an organisations risk management process and cybersecurity program. Alternatively an organisation without an existing cybersecurity program can use the Framework as a reference and establish one.	New	Req'd			
20	To defend IT systems against common cybersecurity threats a company must install sufficient software/hardware protection from malware and internal / external intrusion in the Members computer systems. Member must ensure that their security software is current and received regular updates, members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or other		New	Reqd			

	unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and or data						
21	C-TPAT Members utilising network system must regularly test the security of their IT structure. If vulnerabilities are found, corrective actions must be implements as soon as possible	Members should run regular vulnerability and penetration scans. Vulnerability scans identify open ports and IP addresses in use, as well operating systems and software. It will then compare what it has discovered against its database of known vulnerabilities and report back. There are many free and paid versions of vulnerability scans, Penetration testing is when existing vulnerabilities are exploited to see how much of a threat they are to the network.	New	Req'd			
22	Cybersecurity policies should address how a Member shares information on cybersecurity threats with the government and other business partners.	Members are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain. Information sharing is a key part of the DHS mission to create shared situational awareness of malicious cyber activity. CTPAT members way want to join the National Cybersecurity and Communications Integration Center (NCCIC https://www.dhs.gov/national-cybersecurity-and-communications-integration-center) The NCCIC shares information among public and private sector partner to build awareness of vulnerabilities, incidents and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.	New	O			
23	A system must be in place to identify unauthorised access to IT systems / data or abuse of policies and		No change	Req'd			

	procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violations must be subject to appropriate disciplinary actions						
24	Cybersecurity policies and procedures must be viewed and updated annually or more frequently as risk or circumstances dictate	An example of a circumstance that would dictate a policy update sooner than annually is a cyber-attack. Using the lessons learned from the attack would help strengthen a member's cybersecurity policy	New	Req'd			
25	User access must be restricted based on job description or assigned duties, Authorized access must be reviewed on a regular basis to ensure access to sensitive systems based on job requirements. Computer and network access must be removed upon employee separation.		Enhanced	Reqd			
26	Individuals with access to IT systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases or other forms of authentication and user access to IT systems must be safeguarded.	Complex login or passphrases biometric techniques, and electronic ID cards are 3 different types of authentication processes. The use of the two factor authentication (2FA) or multi authentication (MFA) process is preferred. MFAs can assist in closing network intrusions exploited by weak passwords or stolen credentials. FMA can assist in closing these attack vectors by requiring individuals to augment passwords or passphrases (something you know) with something you have, like a token, or one of your physical features – a biometric.	Enhance	Reqd			
27	Members that allow users to connect remotely to a network must employ secure technologies such as VPNs. Members must also have procedures	A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control	New	Req'd			

	designed to secure remote access from unauthorised users.	information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the internet. A VPN can provide several types of data protection including confidentiality integrity data origin authentication replay protection and access control.					
28	If members allow employees to use personal devices to conduct company work, all such devices must adhere to the company7's cyber security policies and procedures to include regular security updates and a method to securely access the company's network.	Personal devices include storage media like CD's DVDs and USB flash drives. Care will be used if employees are allow to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network	Enhanced	Req'd			
29	Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed products	Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer to the publisher, it is illegal to install software, no matter how it is acquired. That permission almost always takes the form of a license from the publisher, which accompanies authorised copies of the software. Unlicensed software is more likely to fail as a result of an inability to update. It is more prone to contain malware, rendering computers and their information useless. Expect no warranties or support for unlicensed software, leaving your company on its own to deal with failures. There are legal consequences for unlicensed software as well including stiff penalties and criminal prosecution.	New	O			

		Software pirates increase the costs to user of legitimate authorised software and decrease the capital available to invest in research and development of new software Members may want to have a policy that requires Product Key Labels and Certificates of Authenticity to be kept when new media is purchased, CD' DVD' and USB media include holographic security features to help ensure you receive authentic products and to protect against counterfeiting.					
30	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format. Media used to store backups should preferably be stored in an offsite facility.	Devices used for backing up data may not be on the same network as the one used for production work	New	O			
31	All media hardware or other IT equipment must be accounted for through regular inventories. When disposed, they must be properly sanitised and / or destroyed in accordance with the National Institute of Standards and technology (NIST) Guidelines for Media Sanitisation or other appropriate industry guidelines	Member may want to consult the NIST guidelines for Media Sanitisation https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf	New	Req'd			
		Conveyances and IIT's					
32	Conveyances and IITs must be stored at all times on a secure area to prevent unauthorised access and / or manipulation.		New	Req'n			
33	The CTPAT inspection process must have a written procedure for both security and agricultural inspections.	Members need to inspect conveyances and IITs to ensure they have not been altered. Likewise the prevalence of pest contamination via conveyances and IITs is of paramount concern so an agricultural component has been added to the security inspection process.	Enhanced	Req'd			

		Pest contamination is defined as visible signs of animals insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts) or any organic material of animal origin (including blood, bones, hair, flesh, secretions, secretions) viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi, or soil or water; where such products are not the manifested cargo within the IITS					
34	Prior to loading, all conveyances and empty IITS must undergo CTPAT approved security & agricultural inspections to ensure their structures have not been modified to conceal contraband or have been contaminated with agricultural pests Empty Containers & Unit Load Devices (ULDs) must be subject to a 7 point inspection. Reefers must be subject to an 8 point inspection: 1. Front Wall 2. 2 Left side 3. Right side 4. Floor 5. Ceiling / Roof 6. Inside / outside doors, including the reliability of the locking mechanism on the doors, 7. Outside / Under carriage 8. Fan housing on reefers. Conveyances and IITs must be systematically inspected at conveyance yards. Where feasible, inspections must be conducted upon entering and departing storage (Parking) yards and at the point of loading. These inspection must include:	The program has uploaded training material to the Public Library Section of the C-TPAT portal on security and agricultural conveyance / ITT inspections, including a USDA – U.S. Customs and Border Protection presentation in .pdf format called "Carrier Conveyance Contamination". A new version of the presentation will be uploaded din the fall of 2018. This presentation outlines how several types of contaminants might be introduced by conveyances, the reasons for concern, CBP's efforts to prevent invasive species introduction and best practices for industry to prevent conveyance contamination.	Enhanced	Req'd			

	Tractors: 1. Bumper/Tires/ Rims 2. Doors, tool compartments & locking mechanisms 3. Battery box 4. Air breather 5. Fuel tanks 6. Interior cab compartment / sleeper 7. Fairing / roof Trailers: 1. Fifth wheel area – check natural compartment / skid plate 2. Exterior – front & sides 3. Rear – bumper / doors 4. Front wall 5. Left side 6. Right side 7. Floor 8. Ceiling / Roof 9. Inside / outside doors & locking mechanism 10. Outside / Under carriage						
35	Conveyance and IITs must be equipped with the right type of external hardware that can reasonably withstand attempts to remove it, which would allow the doors to be taken off without breaking the seal – providing access to the cargo and / or the inside of the IIT. The door handles, rods hasps, rivets, brackets and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.		New	Req'd			
36	The inspection of all conveyances and empty IITs must be recorded on a checklist. The following elements must be documented on the checklist • Container / trailer / IIT#		Enhanced	Reqd			

	• Date of inspection • Time of Inspection • Name of Employee inspecting • Specific areas inspected. If a supervisor observed the inspections, the supervisor should sign the checklist						
37							
38	If visible pest contamination is found during the conveyance IIT inspection washing / vacuuming must be carried out to remove such contamination. Documentation must be retained for one year to demonstrate compliance with these inspection requirements.	Keeping records on the types of contaminants found, where that were found (conveyance location) and how the pests contamination was eliminated are helpful actions that may assist members in preventing future pest contamination	New	Reqd			
39	Based on risk, management personnel should conduct random searches after the transportation staff have conducted conveyance / IIT inspections. The searches of the conveyances should be done periodically with a higher frequency based on risk. The searches should be conducted at random and without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the US border.	Supervisory searches of conveyances are conducted to counter internal conspiracies As a best practice supervisors can hide an item (like a toy or coloured box) in the conveyance to determine of the field test screener / conveyance operator finds it. Supervisor personnel could be a security manager, held accountable to senior management for security or other designated management personnel	-	O			
40							
41							
42	A tracking and monitoring activity log or equivalent technology must be used to track the conveyances while it is in route to the US. If driver logs are used driver must record any stops and not that inspections of the conveyance. IIT and the seal were conducted.	Conveyances are tracked to prevent them from being diverted to tamper with the load or structure of the conveyance / IIT to allow contraband to be introduced on the shipment. Based on risk, transportation providers may want to track and monitor their conveyances / IITs in real time. There are many tracking	New	Req'd			

		tools available to users free of charge via their smart cell phones, For small carriers applications such as Life 360, Find Friends from Google and What's App allow users to track conveyances and people					
43							
44							
45	CTPAT members should work with their transportation providers to track conveyances from origin to final destination point. Specific requirements for tracking, reporting and sharing of data should be incorporated within the terms of service agreements with service providers		New	O			
46							
47	For land border shipments that are in close proximity to the US border, a "No-stop" policy should be implemented	Cargo at rest is at risk. Avoid unnecessary stops for shipments that are in close proximity to the US	New	O			
48							
49							
50	IF a GPS tracking system is used carriers should use a sensor coupling / connector or equivalent technology from the tractor to the trailers to ensure the trailer is monitored and tracked		New	O			
51	Carriers should use electronic dispatch logs; the logs should be recorded and kept for audit purposes	Electronic dispatch records provide a more accessible means of conducting management oversight and enabling information to be shared and / or compared with additional assessment data. It is recommended that records of the logs be maintained for a sufficient amount of time to allow for audits to be conducted and for investigative purposes, if a breach were to occur in the supply chain.	New	O			
52	For cross border shipments, pre designed transportation routes must be established, which	Waypoints are specific geographical locations defined by sets of	No change	Req'd			

	include anticipated transit times between way points. Once the time between the assigned points has been determined, for bo0th peak and non-peak times, these times must be recorded and incorporated in to the tracking process. If GPS technology is employed, geo fencing must be implemented to include alarm notification when a carrier deviates from the assigned route. The parameters for geo fencing must be set to a minimal allowable tolerance for the pre-established transit route.	coordinates – long & lat – used of navigational purposes including driving or transit points. It is recommended waypoints include the length of time the yard to the loading point, trailer pickup, the US border and the delivery destinations. If a stop is made to collect export documents or to verify seals these can also be included as waypoints.					
53	Carriers must have systems or written procedures in place to respond to significant route deviations and late arrivals to transfer points or the final destination. Drivers must notify the dispatch of any significant route delays due to weather and / or re-routing. Dispatch must independently verify the cause of the delay		No change	Req'd			
54	After a stop drivers must inspect the conveyances sealing or locking devices for any signs of tampering prior to resuming the trip. These inspections must be documented		New	Req'd			
55	In areas of high risk CTPAT members should incorporate a "last chance" verification process for US bound shipments for checking conveyances / IITs for signs of tampering to include visual inspection of conveyances and the VVTT seal verification process. Properly trained individuals should conduct the inspections		New	O			
56							
57	Drivers must record and report any anomalies or usual structural modifications found on the conveyance following a government inspection	These include US DOT inspections or other regulatory agency inspections. It also includes inspections taking place in Mexico or Canada	No change	Req'd			
58	Management must regularly conduct random audits of the tracking and monitoring procedures to ensure the tracking logs are properly		New	Req'd			

	maintained and conveyance tracking and monitoring procedures are being followed. The audit musty include verification of the tracking log against time indicative documents and internal systems. A review to look for unaccounted transit time lapses must also be a part of the audit protocols. The audit process must include verifications en route; management should conduct periodic random route checks, and the finding s must be recorded. The audit process must also include time indicative documents and systems such as fuel receipts scale logs, toll receipts, ACE, Mexico SAT, broker status information, etc.						
59	CTPAT highway carriers should notify appropriate parties (shippers, consignee and importer) of any significant delays including mechanical failures during transit		New	O			
60	If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the member must alert (as soon as possible) any business partners in the supply chain that may be affected		New	Req'd			
Seal Security							
61	CTPAT members must have detailed high security seal procedures that describe how seals are issued and controlled at the facility and during transit. Written protocols mast provide steps to take if a seal is found to be altered, tampered with, or as the incorrect seal number to include documentation of the event. The findings from the investigation must be recorded in a report, and any corrective actions must be implemented as quickly as possible. When the carrier or facility is a component of a larger entity, the written procedures must be maintained at the terminal / local level. Procedures must be reviewed at least		Enhanced	Req'd			

	once a year. Written Seal controls must include the following elements: <u>Controlling Access to Seals</u> • Management of seals is restricted to authorised persons • Secure Storage <u>Inventory, Distribution & Tracking (seal Log)</u> • Recording the receipt of new seal • Issuance of seals recorded in a log. Track seals via log • Only trained, authorised persons may affix seals to IIT <u>Controlling Seals in Transit</u> • Ensure the packed IITs are sealed <u>Seals broken in transit</u> • If load is examined, record replacement seal # • The driver (or pertinent employee) must immediately notify dispatch (or applicable staff) when a seal is broken, indicate who broke it, & provide new seal # • The carrier must immediately notify the shipper, broker and importer of the seal change & new #. • The shipper must note the replacement seal # in the seal log. <u>Seal Discrepancies</u> • Hold any seal discovered to be altered or tampered with to aid in the investigation • Investigate the discrepancy; follow up with corrective actions if warranted • As applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation						
62	All CTPAT shipments that can be sealed must be secured immediately after loading / stuffing/packing by the responsible party and / or shipper or packer acting on the shippers behalf	New	Reqd				

	with a high security seal that meets are exceeds the most current ISO 17712 standard for high security seals. Qualifying cable and bolt seals are acceptable, All seals used must be securely and properly affixed to IIT that are transporting CTPAT members' cargo to / from the US. If a cable seal is used, it must envelop the handle hubs of the 2 centre vertical bars of the container /trailer doors in order to prevent the upward or downward movement of the cable. All excess cable remaining after the seal has been tightened and secured to the container /trailer must be removed. If a high security bolt seal is used, the seal must be placed on the Secure Cam position, if available, instead of the right door handle The seal must be placed at the bottom of the centre most vertical bar of the right container door. Alternatively, the bold seal could be placed on the center most /left hand locking handle of the right container door if the secure cam position is not available. Whenever possible it is recommended that the bolt seal be placed with the barrel portion facing upwards with the barrel portion above the hasp. Any packed IIT that can be sealed must be sealed, Some packed IIT cannot be sealed such as flatbed trailers and other conveyances way vary with certain types that can be sealed and others that cannot. If a tank container has opening that can be sealed they must be sealed, and the party filling the container is responsible for sealing it. When cargo is transported via sealable air cargo containers / IIT like Unit Load Devices (ULDs), high security seals must be used.						
63	For commercial loads or conveyances not suitable for dealing with a high security seal, CTPAT	Describe the measures in place to ensure that bulk or open top loads, dump trailers, tractors, open van	New	Req'd			

	members must demonstrate how they ensure the integrity of the cargo while in transit.	trailers, step decks, flatbeds, livestock trailers and other types of open trailers or oversized load (where a seal will not deter access) are secured during transit.					
64	LTL carriers must at the very least use a high security padlock when picking up local freight in an international LTL environment where consolidation hubs are not used. A the last pick up site prior to crossing the border the carrier must seal the load with an ISO 17712 compliant high security seal; LTL Carriers must have strict controls limiting access to padlocks, keys, or combinations that can open padlocks		Enhance	Req'd			
65							
66							
67							
68	CTPAT's seal verification process must be followed to ensure all high security seals (bolt or cable) have been affixed properly to IIT, and are operating as designed. The procedure is known as the VVTT process: V – View the seal and container locking mechanisms; ensure they are OK: V – Verify seal number against shipment documents for accuracy: T – Tug on seal to make it is properly affixed. T - Twist and turn the bold seal to make sure its components do not unscrew or separate from one another.		New	Req'd			
Procedural Security							
69	Members must have written processes for reviewing their security procedures	All security procedures are subject to audits. It is recommended that an overall general audit be conducted	New	Req'd			

		periodically Specialised areas that are key to supply chain security such as inspections and seal controls may undergo audits specific to those areas. For example to ensure compliance with CTPAT inspection procedures, management can conduct and document periodic reviews of the conveyance and IIT inspection process.					
70							
71	Cargo staging areas and the immediate surrounding areas must be inspected on a regular basis to ensure these areas remain free of visible pest contamination.	Preventative measures such as the use of baits, traps or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.	New	Req'd			
72							
73							
74							
75	Procedures must be in place to ensure that all information used in the clearing of merchandise / cargo is legible, complete, accurate, protected against exchange, loss or introduction of erroneous information and reported on time		No change	Req'd			
76	Cargo must be properly marked and manifested to include accurate weight and piece count. For sealed containers carriers may rely on the information provided on the shipper's instructions.		No change	Req'd			
77	If paper is used, forms and other import / export related documentation should be secured to prevent unauthorized use.	Measures such as using locked file cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorised use of such documentation	No change	Req'd			
78	Bill of lading / manifest procedures must ensure information in the carriers cargo manifest accurately reflects the information provided to the		No change	Req'd			

	carrier by the shipper or its agent and is filed with CBP in a timely manner, Bill of lading information must show the first foreign location / facility where the carrier takes possession of the cargo destined for the US.						
79							
80							
81	Personnel must review the information included in import / export documents to identify or recognise suspicious cargos Relevant personnel must be trained ton how to identify information in shipping documents such as manifests that might indicate a suspicious shipment As a resource and based on risk, CTPAT members should take into account those CTPAT Key Warning Indicators for Money Laundering and Terrorism Financing Activities most applicable to the functions that they and / or their business entity performs in the supply chain. Highway carrier personnel must be trained to review manifests and other documents in order to identify or recognise suspicious cargo shipments such as: • Originated from a or destined to unusual locations • Paid by cash or certified check • Unusual routing methods • Exhibited unusual shipping / receiving practices • Provide vague, generalised or lack of information		No change	Req'd			
82							

83	Drivers must collect personal garbage and dispose of it before entering the US. Otherwise the driver must declare it to US Customs so it may be properly disposed of.		New	Req'd			
84	Based on risk highway carriers must have specific procedures in place to mitigate the risk of collusion between employees, such as between driver and dispatch personnel which might allow a security measure to be overcome	An example of an internal conspiracy would be a driver and dispatch staff colluding to falsify travel times to undermine tracking and monitoring procedures., Procedures to prevent collusion may include assignment rotation, restricted driver access to physical location of dispatcher operations, separate break rooms for dispatch staff and drivers, placement of GPS monitors out of the driver's view, frequent documented audits of driver logs and trends analysis using GPS data to compare drivers average time against which dispatch staff members are on duty	New	Req'd			
85	If legally allowed, and permitted under union rules, carriers should conduct random inspections of driver's luggage and personal belongings. If any suspicious anomalies are found during the screening, the carrier should document and report its findings to CBP.		No change	O			
86	CTPAT highway carriers must ensure their FAST certified drivers follow all fast requirements when using the FAST lane, to include only having passengers in the cabin of the truck that are FAST certified.		New	Req'd			
87	For US bound shipments the highway carrier transporting the cargo (including subcontracted carriers) must use its one SCAC code regardless of whether the carrier is using a FAST% or regular lane		New	Req'd			
88	In accordance with the US DOT standards CTPAT carriers should have a comprehensive vehicle	Cargo at rest is at risk. A comprehensive maintenance program	New	O			

	preventative maintenance program in place and ensure drivers are performing adequate checks of their vehicles. Maintenance records should be kept for a minimum of one year.	may help avoid unforeseen stops due to mechanical issues					
89	In areas of high risk, where operationally feasible, the carrier should use the convoy method (e.g. a minimum of two trucks travelling together) to transport cargo. Each truck in the convoy should have the means to communicate with the other trucks in the convoy and with dispatch staff		New	O			
90							
91							
92							
93							
94	CTPAT members must have a written procedure for reporting an incident to include a description of the facilities internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents that may affect the security of the member's supply chain. As applicable, the member must report an incident to the SCSS, the closest port of entry any pertinent law enforcement agencies and business partners that may be part of the affected supply chain. Notifications should be made as soon as feasibly possible Notification procedures must include the accurate contact information that lists the names and phone numbers of personnel requiring notification as well as for law enforcement agencies, Procedures must be periodically reviewed to ensure contact information is accurate	Examples of incidents warranting notification of CBP include (but are not limited to) the following: • Discovery of tampering with a container / IIT or high security seal • An unaccounted for new seal has been applied to an IIT • Smuggling of contraband to include people; stowaways: • Unauthorised entry in conveyances, locomotives, vessels or aircraft carriers • Extortion, payments for protection, threats, and / or intimidation • Unauthorised use of a business entity identifier (i.e. Importer of Record Number (IOR), SCAC code etc)	New	Req'd			
95	Procedures must be in place to identify, challenge and address unauthorised / unidentified persons.		No change	Req'd			

	Personnel must know the protocol to challenge an unknown, unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorised person from the premises						
96	CTPAT member should set up a mechanism to report security related issues anonymously. When an allegation is received, it should be investigated and if applicable , corrective actions should be taken	Internal problems such as theft fraud and internal conspiracies may be reported more readily if the reporting party knows the concern may be filed anonymously. Members can set up a hotline program or similar mechanism that allows people to retain anonymous if the fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each item was investigated and corrective actions taken.	New	O			
97							
98							
99							
100							
101	Seal numbers should be electronically printed on the bill of lading or other shipping documents		New	o			
102	CTPAT highway carriers (or an authorised party transmitting on behalf of the carrier) must transmit data in the ACE platform for empty containers / trailers prior to arrival of the conveyance at the border.	The time frame is not subject to the time constraint limitations of 1 hour (regular crossing) / 30 minutes (FAST crossing), but must be transmitted prior to arrival at the primary booth. Data to be transmitted includes driver name, ID number, license plate of the conveyance, and container / trailer.	New	Req'd			
Agricultural Security							
103	CTPAT members must have written procedures designed to prevent pest contamination to include wood packaging materials (WPM) regulations. Pest	WPM is defined as wood products (excluding paper products) used in supporting, protecting or carrying a	New	Req'd			

	prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the international plant protection convention (IPPC) International standards for phytosanitary measures No. 15 (ISPM 15)	commodity. WPM includes such items as pallets, crates boxes, reels and dunnage. Frequently these items are made of raw wood that may not have undergone sufficient processing or treatment to remove or kill pests. Dunnage in particular has been shown to present a high risk of introduction and spread of pests. The IPPS is a multilateral treaty overseen by the UN's Food and Agriculture Organisation that aims to secure, coordinated, effective action to prevent and control the introduction and spread of pests and contaminants. ISPM includes internationally accepted measures that may be applied to WPM to reduce significantly the risk of introduction and spread of most pests that may be associated with WPM. ISPM 15 affects all wood packaging material requiring that they be debarked and then heat treated with fumigated with methyl bromide and stamped or branded with the IPPC mark of compliance. This mark of compliance is colloquially known as the "wheat stamp". Products exempt from the ISPM 15 are made from alternate materials, such as paper, metal, plastic or wood panel products (orientated strand board, hardboard and plywood.)					
104	All cargo handling facilities including trailer yards should have physical barriers and /or deterrent that prevent unauthorised access		Enhance	O			

105	Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas. Based on risk, additional interior fencing should segregate various types of cargo, such as domestic, international, high value. And / or HM. Fencing should be regularly inspected for integrity and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.	Other acceptable barriers maybe sued instead of fencing, such as a dividing wall or natural features that impenetrable or otherwise imped access such as a steep cliff or dense thickets etc	Enhance	O			
106							
107	Gates where vehicles and / or personnel enter or exit (as well as other points of egress) must be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labour laws	It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated.	Enhance	Req'd			
108	Private passenger vehicles must be prohibited from parking in or adjacent to cargo handling and storage areas	In order to minimize the risk of cargo being stolen or compromised, locate parking areas outside of fence operational areas or at least substantial distances from cargo handling and storage areas.	Enhanced	Req'd			
109	Adequate lighting must be provided inside and outside the facility, including the following areas: entrances and exits; cargo handling and storage areas. Fence lines and parking areas.	Automatic timers or light sensors that automatically turn on appropriate security light are useful additions to lighting apparatus	No change	Req'd			
110	Members who rely on security technologies for physical security must have written policies and procedures governing the use, maintenance and protection of security technology. These policies must include the following: • Limit access to locations of controls / hardware for security devices • Procedures to test /inspect the technology on a regular basis	Security technology used to secure sensitive areas / access points includes alarms access control devices and video surveillance systems	New	Req'd			

	• Inspections include verification that equipment is correctly positioned and / or working properly • Document the results of the inspections and performance testing • If corrective actions are warranted, implement and document the actions taken • Documented results must be maintained for a sufficient time for audit purposes If third party (off-set) security monitoring resources are utilised, written agreements must be in place stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes adding or subtracting authorized personnel password revisions and systems of access or denial Security Technology policies and procedures must be reviewed and updated annually or more frequently as risk or circumstances dictate						
111	CTPAT members should utilise licensed /certified resources when considering design and installation of technology	Today's security technology is complex and evolves rapidly. Security and fire alarm systems are often the first line of defence against theft. Often time's companies purchase the wrong type of security technology that proves ineffective when needed and / or pay more than necessary. Seeking qualified guidance will help a buyer select the right technology options for their needs and budget. It is important to do business with individuals with a track record of successful integrations with this type of technology. Virtually all	New	O			

		certifications are granted, at least in part, on some type of regulatory authority's licensing. According to the National Electronic Contractors Association (NECA) in the US, 33 states currently have licensing requirements for professionals engaged in the installation of security and alarm systems.					
112	All security technology infrastructure must be physically secured from unauthorised access	Security technology infrastructure includes computers, security software, control panels, video surveillance or closed circuit TV cameras, power and hard drive components for cameras as well as recordings.	New	Req'd			
113	Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.	A criminal trying to breach security may attempt to disable the power to the security technology in order to circumvent it. Thus it is important to have an alternate power source. This may be a generator or back up batteries.	New	O			
114	If security cameras are deployed cameras should monitor a facilities premise and sensitive areas to deter unauthorised access. Alarms should be used to alert a company to unauthorised access into sensitive areas.	Sensitive areas for importer and their business partners include cargo handling and storage areas, shipping / receiving areas where import documents are kept, IT servers, yards and storage areas for IITs, areas where IITs are inspected and seal storage areas.	New	O			
115	If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to export / import processes	Positioning cameras correctly is important to enable them to record as much as possible of the physical chain of custody with the facilities control as possible. Specific areas of security focus would include cargo handling activities, container inspections,	New	Req'd			

		loading process, sealing process, conveyance arrival / exit, cargo and departure.					
116	If camera systems are deployed, cameras should have an alarm notification feature which would signal a failure to record condition	A failure of video surveillance could be the result of someone disabling the system in order to breach the supply chain without leaving video evidence of the crime, The failure to operate feature can result in an electronic notification being sent to designated persons notifying them that device requires immediate attention.	New	O			
117	If camera systems are deployed cameras should be programmable to record at the highest picture quality setting reasonably available and be set to record on a 24/7 basis.		New	O			
118	Periodic random reviews of the camera footage must be conducted (by management, security or other designated personnel) to verify that cargo security procedures are being properly followed. Results of the reviews must be summarized in writing to include any corrective actions taken, The results must be maintained for sufficient time for audit purposes.	The review of the footage is primary geared towards the physical chain of custody to ensure the shipment remained secure, Some examples of processes that can be included in the review are cargo handling activities, container inspections, the loading process, sealing process, conveyance arrival / exit and cargo departure. **Purpose of the Review** - to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses and proscribe corrective actions in support of improvement to security processes **Written Summary** may include the date of the review, date of the footage viewed, which camera, area the recording was from a brief description of any findings and if warranted, corrective actions.	New	Reqd			

		Time to maintain documentation; may vary between 2 to 5 years.					
119	Recordings of footage covering key import / export processes must be maintained for a minimum of 14 days after the shipment being monitored has arrived at the point of destination where the container is first opened after clearing customs		New	Req'd			
120	CTPAT members must have written procedures governing how identification badges and access devices are granted, changed and removed. Where applicable, a personnel identification system must be in placed for positive identification and access control purposes. Access to sensitive areas must be restricted based on job description or assigned duties. Removal of access devices must take place upon the employee separation from the company.	Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes and keys. Exit checklists are recommended when employees are separated from a company to ensure that all access devices have been turned it. For smaller companies where personnel where employee know each other, no identification system is required.	No Change	reqd			
121	Visitors, vendors and service providers must present photo ID upon arrival and a log must be maintained that records the details of the visit. All visitors and service providers should be issued temporary identification. If a temp ID is used, it must be visibly displayed at all times during the visit The registration log must include: • Date of visit • Visitor's name • Verification of phot ID (type of ID verified) Frequent visitors may forgo the photo ID but must still log in and out • Time of arrival • Company POC • Time of departure.		Enhanced	Req'd			

122	Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government issued photo id to facility employee granting access to verify their identity. If presenting a government issued photo id is not feasible, the employee may accept a recognisable for of ID issued by the highway carrier company that employees the driver picking up the load		No change	Req'd			
123							
124							
125							
126	Prior to arrival the carrier must notify the facility of the estimated time of arrival for the scheduled pick up, the name of the driver and truck number. Where operationally feasible, CTPAT members must allow deliveries and pickups by appointment only.	This is designed to avoid fictitious pickups. Fictitious pickups are criminal schemes that result in the theft of cargo by deception that includes truck drivers using fake ID New and / or fictitious businesses set up for the purpose of cargo theft.	New	Req'd			
127	Arriving packages and mail should be periodically screened for contraband before being admitted	Examples of contraband include drugs, explosives and currency	No change	O			
128							
129	Work requirements for security guards must be contained in written polies and procedures. Management must periodically verify compliance with these work instructions and policies through audits, policy reviews and simulated exercise	Security guards are often employed at manufacturing sites, seaports, distribution centers. Consolidators and forwarder operations sites.	New	Req'd			
Physical Access Controls							
130							
131	Application information such as employment history and references must be verified prior to employment, to the extent possible and allowed under law		No change	Req'd			
132	In accordance with the applicable legal limitations and the availability of criminal records, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirement should extend to temporary		No change	O			

	workforce and contractors. Once employed, periodic re-investigations should be performed based on cause and / or the sensitivity of the employee's position. Employee background screening should include verification of the employee's identity and criminal history that encompass City, State, Provincial and Country databases. CTPAT members and their business partners should factor in the results of background checks as permitted by local statutes in making hiring decisions. Background checks are not limited to verification of identity and criminal records, In areas of greater risk, it may warrant more in depth investigations.						
135	Members must establish and maintain a security training and awareness program to recognise and foster awareness of the security vulnerabilities to facilities conveyances and cargo at each point in the supply chain which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPATs security requirements. More in-depth specialised training must be given to those personnel in sensitive positions. One of the key aspects of a security program is training. Employees who understand why a security measures are in place are more likely to adhere to them. Security training must be provided to all employees and contractors on a regular basis, and newly hired employees and contractors must receive this training as a part of their orientation / job skills training. Training topics should include protecting access controls, recognising internal conspiracies, and reporting procedures for suspicious activities and security incidents. When possible specialised training should include hands-on demonstrations. If a	The CTPAT program has already commenced the development of training on the new MSC. Once the MSc's finalised, the program will make training available to its members via the CTPAT portal.	Enhance	Req'd			

	hands-on demonstration is conducted the instructor should allow time for the students to demonstrate the process. Members must retain evidence of training such as training logs, sign in sheets (roster), or electronic training records. Training records should include the date of training, the names of attendees and the topics covered.						
136	Drivers and other employees that conduct security inspections of empty conveyances and IITs must be trained to inspect their conveyances / IITs for both security and agricultural purposes Refresher training must be conducted periodically as needed after an incident or security breach and or when there are changes to company procedures. Inspection training must include the following topics • Signs of hidden compartments • Concealed contraband in naturally occurring compartments • Signs of pest contamination.		No change	Req'd			
137	Drivers must receive training on situational reporting – the procedures to follow if something is found during a conveyance inspection or if a security incident takes place while in transit. In addition, drivers must look be instructed in controlling / using seals during transit, and to look for signs of someone observing the movement of the conveyance and / or goods Drivers for instance must be trained on how to conduct the seal verification (VVTT) process.		Enhance	Req'd			
138	Personnel in sensitive positions must receive additional specialised training geared toward		New	Req'd			

	responsibilities that the person holds. Sensitive positions include staff working directly with cargo or its documentation as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to shipping, reviewing, mailroom staff, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances , and or seal controls. One training topic that must be given to employees dealing with import / export processes and documentations is corporate identity theft (and measures to prevent it).						
139	CTPAT members should have measures in place to verify that the training provided met all training objectives	Understanding the training and being able to use that training in one's position for sensitive employees is of paramount importance. Exams or quizzes, a simulation exercise or regular audits of procedures etc. are some of the measures that the member may implement to determine the effectiveness of the training.	New	O			
140							
141							
142	Training must be provided to applicable personnel of preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirements applicable to wood packaging materials (WPM) and identification of infested wood	CBP has collaborated with the US Dept of Agriculture to develop training on visible plant contamination., Different training modules have been developed for the different trade environments; air; sea; and land border (rail and highway). The training modules will be made available to all members via the C-TPAT portal.	New	Req'd			
143	Personnel must be trained on the company' cyber security policies and procedures, This must include the need for employees to protect passwords and computer access	The lack of quality training across industry sectors has been found to be one of the primary reasons companies become vulnerable to cyberattacks. Members can combat this by utilising	Enhance	Req'd			

		a robust cybersecurity training program, preferably one that is delivered to all personnel in a formal setting rather than simply through emails and slide shows.					
144	Personnel operating and managing security technology systems must have received training in their operations and maintenance	Prior experience with similar systems is acceptable. Self-training via operational manuals wand other methods is acceptable for smaller enterprises.	New	Req'd			
145	Training must be given on situational reporting. Employees must be trained to what to report, how to report it, and to whom. In addition to reporting responsibilities, training must also be provided on what to do after the employee has reported the situation.	Procedures to report security incidents or suspicious activity are extremely important aspects of a security program, and training on how to report an incident can be included in the overall security training. Specialised training modules (based on job duties) may have more detailed training on reporting procedures to include specific response protocols after the incident is reported. The CTPAT training for members will have a module around situational reporting, which will include what details of an incident needed to be reported on, and by whom and when etc.					