ID	Criteria	Implementation Guidance	Must / Should
1.3	The supply chain security program must be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their		

2. Risk Assessment – The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats. CTPAT recognizes that when a company has multiple supply chains with numerous business partners, it faces greater complexity in securing those supply chains. When a company has numerous supply chains, it should focus on geographical areas/supply chains that have higher risk.

When determining risk within their supply chains, Members must consider various factors such as the business model, geographic location of suppliers, and other aspects that may be unique to a specific supply chain.

Key Definition: Risk – A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence. What determines the level of risk is how likely it is that a threat will happen. A high probability of an occurrence will usually equate to a high level of risk. Risk may not be eliminated, but it can be mitigated by managing it – lowering the vulnerability or the overall impact on the business.

ID	Criteria	Implementation Guidance	Must / Should
2.1	CTPAT Members must conduct and document the amount of risk in their supply chains. CTPAT Members must conduct an overall risk assessment (RA) to identify where security vulnerabilities may exist. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. The member must take into account		

CTPAT requirements spec6.4 (h)-9.1 (r)-4.4 n2.217 Td7 Td7 Tfm(eq)-9.88 35.51.1 (r)-18.5 (u mu)-21..1 ( )]T(.)-2 (b)-6.39.1 (er)5.51.1 (r)-18.0.005 Tw 0 9.1 (r)-21.1 (F)44 to
a) to inde0(C)-(2)-10.61 (r)-h6.9 (k)4 (e)3 (9.r)-4.4 n- 90.76 Tm[a) k.1 3 n (i3c 017.2 (8.81.22())-2.2 (1 09.1 (r)-h.3(TP)- (1 09.1 (r)-h(k)-6.9 (18.1-1.9 dm) (n)-nn0.6 (

ID	Criteria	Implementation Guidance	Must / Should
2.3	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 level from a specific country, periods of heightened alert, following a security breach or incident, changes in business partners, and/or changes in corporate structure/ownership such as mergers and acquisitions etc.	Must
2.4	CTPAT Members should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.	An4920.6 (s /P <</MC;2.24 356.0( )TjETP0.6 (s /P <</m)8. .7.9002 p .6 (h)-12.2 (a)2.1 (t)-0.A)5.713mt (a)2.1 di	

3. **Business Partners –** CTPAT Members engage with a variety of business partners, both domestically and internationally. For those business partners who directly handle cargo and/or import/export documentation, it is crucial for the Member to ensure that these business partners have appropriate security measures in place to secure the goods throughout the international supply ctic (ns)6 (ur)rts ia.

ID	Criteria	Implementation Guidance	Must / Should
3.7	To ensure their business partners continue to comply with CTPAT's security criteria, Members should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.	Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. If a member never required updates to its assessment of a business partner's security program, the Member would not know that a once viable program was no longer effective, thus putting the member's supply chain at risk. Deciding on how often to review a partner's security assessment is based on the Member's risk assessment process. Higher risk supply chains would be expected to have more frequent reviews than low risk ones. If a Member is evaluating its business partner's security by in person visits, it may want to consider leveraging other types of required visits. For example, cross-train personnel that test for quality control to also conduct security verifications. 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, etc.).	Should

ID	Criteria	Implementation Guidance	Must / Should
4.2	To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.		Must
4.3	CTPAT Members using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.	A secure computer network is of paramount importance to a business, and ensuring that it is protected requires testing on a regular basis. This can be done by scheduling vulnerability scans. Just like a security guard checks for open doors and windows at a business, a vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company's IT system. The VS does this by comparing the results of its scan against a database of known vulnerabilities and produces a correction report for the business to act upon. There are many free and commercial versions of vulnerability scanners available. The frequency of the testing will depend on various factors including the company's business model and level of risk. For example, companies should run these tests wheneveel-0. art	

ID	Criteria	Implementation Guidance	Must / Should
4.4	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 5.1 (ng/Na0.5 (k)2 (v)11.2 y10.4 (pa)2.1 (r)4.6 (t)5.1 (o.8 (e)9f6 /8 (e)9f69)5.1 (ng)6/(h 8.8 (a)2.1 (	

Second Focus Area: Transportation Security

5. **Conveyance and Instruments of International Traffic Security** – Smuggling schemes often involve the modification of conveyances and Instruments of International Traffic (IIT), or the hiding of contraband inside IIT. This criteria category covers security measures designed to prevent, detect, and/or deter the alterin

ID	Criteria	Implementation Guidance	Must / Should
5.2	The CTPAT inspection process must have written procedures for both security and agricultural inspections.	With the prevalence of smuggling schemes that involve the modification of conveyances or Instruments of International Traffic, it is imperative that Members conduct inspections of conveyances and Instruments of International Traffic to look for visible pests and serious structural deficiencies. Likewise, the prevention of pest contamination via conveyances and IIT is of paramount concern, so an agricultural component has been added to the security inspection process. Pest contamination is defined as visible forms 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, excretions); 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 instruments of international traffic (i.e. containers, unit load devices, etc.).	Must
5.6	All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.		Should
5.9	Vessels that visited Asian Gypsy Moth (AGM) high-risk areas during AGM flight periods (in the current or previous season) must present a pre-departure AGM inspection certificate from an approved entity in the high-risk country stating that the vessel is free of AGM life stages. The AGM inspections must be performed as close to vessel departure time from the regulated port as possible. CTPAT sea carriers must provide U.S. Customs and Border Protection with two-year port of call data at least 96 hours prior to arrival to a U.S. port.	Current high-risk countries for AGM include Russia, China, Korea, and Japan. For additional information, visit https://www.aphis.usda.gov/aphis/resources/pests-diseases/hungry-pests/the-threat/asian-gypsy-moth/asian-gypsy-moth	Must

ID	Criteria	Implementation Guidance	Must / Should
5.29	If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the Member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.		Must
5.31	CTPAT vessels must ma C ma pap/2d(a)-5 (y(a)-413.)-6.7mua ent cPc1 (pap2)-6.eW 6 m719.76 5 (o)-D(o)-7 (o)-7.(oc.6 m719fha)2.1 2oe C mo)		

6. **Seal Security –** The sealing of trailers and containers to attain continuous seal integrity, continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security, such as using the correct seals per CTPAT requirements; properly placing a seal on IIT, and verifying that the seal has been affixed properly.

ID	Criteria	Implementation Guidance	Must / Should
6.1	CTPAT Members must have detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during transit. Procedures must provide the steps to take if a seal is altered, tampered with, or has		

ID	Criteria	Implementation Guidance	Must / Should
	Seals Broken in Transit: • If a load is examined, record the replacement seal number. • The driver must immediately notify did8G itthead8G1.3 (i)5 (a)l(y di) 4.6 (i5.1 (d8G be)9 (r)0.8 (o)k6 (/)1.3 (n,)5o)2.7 (i)n8 (y di)ctachewh		

ID	Criteria	Implementation Guidance	Must / Should
6.6	If a Member maintains an inventory of seals, company management or a security supervisor must conduct a seal audit that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents. All audits must be documented. As part of the overall seal audit process, dock supervisors and/or warehouse managers must periodically verify seal numbers used on conveyances and Instruments of International Traffic.		Must

7. **Procedural Security –** Procedural Security encompasses many aspects of the import-export process, documentation, and cargo storage and handling requirements. Other vital procedural criteria pertain to reporting incidents and notification to pertinent law enforcement. Additionally, CTPAT often requires that procedures be written because it helps maintain a uniform process over time. Nevertheless, the amount of detail needed for these written procedures will depend upon various elements such as a company's business model or what is covered by the procedure.

   CTPAT recognizes that the technology used in supply chains continues to evolve. The terminology used throughout the criteria references written, paper-based procedures, documents, and forms. Electronic documents and signatures, and other digital technologies, however, are also -51ippchains c(ed[Tc 0.003 Tw -18.74 -1.22[)-4 ()-4 (n)6 (ou))6 (ri)-4 ()9--4 244TJ)i-9.9 (c)-2 (,)11 (

ID	Criteria	Implementation Guidance	Must / Should
7.7	If paper documents are used, forms and other import/export related documentation should be secured to prevent unauthorized use.		

ID	Criteria	Implementation Guidance	Must / Should
7.23	CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process. A notification protocol must be in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc.) that take place anywhere around the world and which affects the security of the member's supply chain. As applicable, the Member must report any global incidents to its Supply Chain Security Specialist, the closest port of entry, any		

ID	Criteria	Implementation Guidance	Must / Should
7.25	CTPAT Members 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 reported anonymously. Members can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken.	Should
7.34	Access to Sensitive Security Information (SSI) must be restricted to authorized personnel only. When SSI is released to unauthorized individuals, U.S. vessels must file a report with the U.S. Department of Homeland Security and a copy of such report must be sent to the SCSS. Non U.S. vessels must inform the SCSS when SSI was released to unauthorized persons. All carriers must document the steps taken to ensure that similar incidents will not occur.	The Federal Code of Regulations (49 CFR) on the protection of SSI dictates that only persons with a "need to know," as defined in 49 CFR 1520.11, will have access to security assessments, plans and amendments. Vessel and facility owners and operators must follow procedures stated in the 49 CFR 1520 for the marking, storing, distributing and destroying of SSI material, which includes many documents that discuss screening processes and detection procedures. Expectation is that foreign vessels and foreign marine port terminal operators also comply with 49 CFR.	Must

ID	Criteria	Implementation Guidance	Must / Should
7.37	Members must initiate their own internal investigations of any security related incidents (terrorism, narcotics, stowaways,		

8. Agricultural Security – Agriculture is the largest industry and employment sector in the U.S. It is also an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and in all types of cargo may decrease CBP cargo holds, delays, and commodity returns or treatments. Ensuring compliance with CTPAT's agricultural requirements will also help protect a key industry in the U.S. and the overall global food supply.

Key Definition: Pest contamination – The International Maritime Organization defines pest contamination as visible forms 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, excretions); 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 instruments of international traffic (i.e. containers, unit load devices, etc.).

ID	Criteria	Implementation Guidance	Must / Should
8.1	CTPAT Members must, in accordance with their business model, have written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations. Visible pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).	WPM is defined as wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. WPM includes items such 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, and therefore remain a pathway for the introduction and spread oTJ0.00(t)2.6 (he)9 (i)5 (y f)8.8 (o)1.9 (r)93 (e(he)94a3.8 (e	

Third Focus Area: People and Physical Security

ID	Criteria	Implementation Guidance	Must / Should
9.5	Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.	Locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.	Should
9.6	Adequate lighting must be provided inside and outside the facility including, as appropriate, 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 lights are useful additions to lighting apparatus.	

ID	Criteria	Implementation Guidance	Must / Should
	• That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly; • That the results of the inspections and performance testing is documented; • That if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented; • That the documented results of these inspections be		

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
9.15	If camera systems are deployed, 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 in accordance with the law. Results of the reviews must be summarized in writing to include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes.	If camera footage is only reviewed for cause (as part of an investigation following a security breach etc.), the full benefit of having cameras is not being realized. Cameras are not only investigative tools. If used proactively, they may help prevent a security breach from occurring in the first place. Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following: • Cargo handling activities; • Container inspections; • The loading process; • Sealing process; • Conveyance arrival/exit; and • Cargo departure, etc. **Purpose of the review:** The review is intended to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and prescribe corrective actions in support of improvement to security processes. Based on risk (previous incidents or an anonymous report on an employee failing to follow security protocols at the loading dock, etc.), the Member may target a review periodically. **Items to include in the written summary**: • The date of the review; • Date of the footage that was reviewed; • Which camera/area was the recording from; • Brief description of any findings; and • If warranted, corrective actions.	Must

ID	Criteria	Implementation Guidance	Must / Should
9.16	If cameras are being used, recordings of footage covering key import/export processes should be maintained on monitored shipments for a sufficient time to allow an investigation to be completed.	If a breach were to happen, an investigation would need to be conducted, and maintaining any camera footage that covered the packing (for export) and loading/sealing processes would be of paramount importance in discovering where the supply chain may have been compromised. For monitoring, the CTPAT pc539.52 0.48 0.48 r8(ne)9 (d)]1 (et)-1j0.003 Tc -10.337 -24 539.e-3.9 (l.9 (w[	

ID	Criteria	Implementation Guidance	Must / Should
10.10	If security guards are used, work instructions for security guards must be contained in written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.	Though guards may be employed at any facility, they are often employed at manufacturing sites, seaports, distribution centers, storage yards for Instruments of International Traffic, consolidator, and forwarders operating sites.	Must
10.12	Sea Carriers should have a security guard(s) on vessels operating in well-known high-risk areas for narcotics smuggling and terrorism. The security guard (s) should be i0 9.96 113.4 420.242) should be ihokg ah.4 (21 (ua)2.1 (r8(o)1.9 2.8 (o)-441 (r)-1.7r)2.6 (n)-2.1 (at)v0 Tc e2 (e)9 (w 0 -1w (-1 (rl4 ( )-1’9 (ul		

11. Personnel Security – A company's human resource force is one of its most critical assets, but it may also be one of its weakest security links. The criteria in this category focus on issues such as employee screening and pre-employment verifications. Many security breaches are caused by internal conspiracies, which is where one or more employees collude to circumvent security

ID	Criteria	Implementation Guidance	Must / Should
11.3	Vessel masters must account for all crewman prior to the vessel's departure from a U.S. port. If the vessel master discovers that a crewman has deserted or absconded, the vessel master must report this finding to U.S. Customs and Border Protection immediately and prior to the vessel's departure.	Per CFR - Title 8 - § 251.2 Notification of Illegal Landings, and U.S. Customs and Border Protection's Vessel Inspection Guide, July 2012 (https://www.cbp.gov/sites/default/files/documents/vessel_guide_4.pdf), the owner, agent or master is required to report immediately, by telephone, the desertion or absconding of a nonimmigrant crew member to the U.S. Customs and Border Protection office at the location of the incident. In addition, the following forms and documents are required: 1. Completed U.S. Customs [illegible] f8c'9BDF9Q%hB;ompo er	

12. **Education, Training and Awareness –** CTPAT's security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and