1 For a CTPAT Member's supply chain security program to become and remain effective, it must have the support of a company's upper management. Instillinse.4nae

	Criteria		
1.1	In promoting a culture of security, CTPAT Members should demonstrate their commitment to supply chain security and the CTPAT Program through a statement of support. The statement should be signed by a senior company official and displayed in appropriate company locations.	Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Senior company officials who should support and sign the statement may include the president, CEO, general manager, or security director. Areas to display the statement of support include the company's website, on posters in key areas of the company (reception; packaging; warehouse; etc.), and/or be part of company security seminars, etc.	Should
1.2	To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. These new security measures should be included in existing company procedures, which creates a more sustainable structure and emphasizes that supply chain security is everyone's responsibility.	Supply Chain Security has a much br	

2

D	e

3 **Business Partner Requirements** 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 chain. When business partners subcontract certain functions, an additional layer of complexity is added to the equation, which must be considered when conducting a risk analysis of a supply chain.

Definition A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the United States via a CTPAT Member's supply chain. A business partner may be any party that provides a service to fulfil a need within a company's international supply chain. These roles include all parties (both directly and indirectly) involved in the purchase, document preparation, facilitation, handling, storage, and/or movement of

D	E	F	M

D	E	F	M S
3.6	If weaknesses are identified during business partners' security assessments, they must be addressed as soon as possible, and corrections must be implemented in a timely manner. Members must confirm that deficiencies have been mitigated via documentary evidence.	CTPAT recognizes that there will be different timelines for making corrections based on what is needed for the correction. Installing physical equipment usually takes longer than a procedural change, but the security gap must be addressed upon discovery. For example, If the issue is replacing a damaged fence, the process to purchase a new fence needs to start immediately (addressing the deficiency) and the installation of the new fence (the corrective action) needs to take place as soon as it is feasible. Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. If it is a deficiency that may jeopardize the security of a container, for instance, it should be addressed as soon as possible. Some examples of documentary evidence may include copies of contracts for additional security guards, photographs taken of a newly installed security camera or intrusion alarm, or copies of inspection checklists, etc.	Must

D	[illegible]	[illegible]	[illegible]
3.9	CTPAT Members should have a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, indentured, or indentured child labor.	The private sector's efforts to protect workers' rights in their operations and supply chains can promote greater understanding of labor laws and standards and mitigate poor labor practices. These efforts also create an environment for better worker-employer relations and improve a company's bottom line. Section 307 of the Tariff Act of 1930 (19 U.S.C. § 1307) prohibits the importation of merchandise mined, produced or manufactured, wholly or in part, in any foreign country by forced or indentured child labor – including forced child labor. Forced Labor is defined by the International Labor Organization's Convention No. 29 as all work or service exacted from any person under the menace of any penalty and for which the said person has not offered himself voluntarily. A social compliance program is a set of policies and practices through which a company seeks to ensure maximum adherence to the elements of its code of conduct that cover social and labor issues. Social compliance refers to how a business addresses its responsibilities in protecting the environment, as well as the health, safety, and rights of its employees, the communities in which they operate, and the lives and communities of workers along their supply chains.	Should

4 **Cybersecurity** – In today's digital world, cybersecurity is the key to safeguarding a company's most precious assets – intellectual property, customer information, financial and trade data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of a company's information systems. This threat pertains to businesses of all types and sizes.

D	[illegible]	[illegible]	[illegible]
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 is a key part of the Department of Homeland Security's mission to create shared situational awareness of malicious cyber activity. CTPAT Members may want to join the National Cybersecurity and Communications Integration Center (NCCIC - https://www.us-cert.gov/nccic). The NCCIC shares information among public and private sector partners 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.	Should
4.5	A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.		Must
4.6	Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.	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.	Must
4.7	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 is based on job requirements. Computer and network access must be removed upon employee separation.		Must

D			
4.8	Individuals with access to Information Technology (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		

5

D			
	Additional inspection requirements for land border crossings via highway carriers: Inspections of conveyances and IIT must be conducted at conveyance/IIT storage yards. Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing. These systematic inspections must include 17-point inspections: [illegible] 1. Bumper/tires/rims; 2. Doors, tool compartments and locking mechanisms; 3. Battery box; 4. Air breather; 5. Fuel tanks; 6. Interior cab compartments/sleeper; and 7. Faring/roof. [illegible]: 1. Fifth wheel area - check natural compartment/skid plate.		

D	[illegible]	[illegible]	[illegible]

D	C	P	M S
5.7	If visible pest contamination is found during the conveyance/Instruments of International Traffic 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 they were found (conveyance location), and how the pest contamination was eliminated, are helpful actions that may assist Members in preventing future pest contamination.	Must
5.8	Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic u		

7 Procedural Security encompasses many aspects of the import-export process, documentation, and cargo

D			
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 anyysu plrotourtnnyyd]TJ0.01.229 Td[(a)5.1 (c)6.3 (.)hny8.8 (i)f3.6 (e)9 (p6.3 (e)2.7 (a)10.4 ( )]2.7 (ha)9 (pl)12 ((10.5 (,)-9.3 p6.3 (e)u4.6 aoirys2.6 (i)5.1 (f)1.9 (l)n 2.6 (o)(2.1 (t)2.6 (t)5.1 (a)5.1 (c)10.5 (t)2.6 (b10.5 (,) 2.6 (o))9 (pl)n2.1 (t)m3.6 (e)9 (p)0.6 (s)4..4 (e))6.9 8 anyydl ausb-9(r)4.95-0.s,ris, rnn9 (	

D	[illegible]	[illegible]	[illegible]
		document that each reported item was investigated and that corrective actions were taken.	
7.27	All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.		Must
7.28	Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.		Should
7.29	Seal numbers assigned to specific shipments should be transmitted to the con (pe)-3 (c)6.3 (i)524 BDC Qq108.24 354.96 282.96 36.72 rQ7TJETQBT0.005 Tc -0.0((e)9 .24 354 Tc -0.(t)2.7 (he)9 (6nBT0.005 Tc -0.005 Tw 3)18 (i nBTTw 9. 6		

v)11a

8 [redacted] 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.

[redacted] – 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,hoere s 2l (: Pp

9 [redacted] Cargo handling and storage facilities, Instruments of International Traffic storage areas, and facilities where import/export documentation is prepared in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

One of the cornerstones of CTPAT is flexibility, and security programs should be customized to fit each company's circumstances. The need for physical security can vary greatly based on the Member's role in the supply chain, its business model, and level of risk. The physical security criteria provides a number of deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information, and Members should employ these security measures throughout their supply chains.

D			
	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 maintained for a sufficient time for audit purposes. If a third party central monitoring station (off-site) is used, the		

D	ẽ	

D			
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	

D	[illegible]	[illegible]	[illegible]
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 program recommends allotting at least 14 days after a shipment has arrived at its first point of distribution. This is where the container is first opened after clearing Customs.	Should

9 [illegible] Access controls prevent unauthorized access into facilities/areas, help maintain control of employees and visitors, and protect company assets. Access controls include the positive identification of all employees, visitors, service providers, and vendors at all points of entry.

D	[illegible]	[illegible]	[illegible]
10.1			

D			
10.2	Visitors, vendors, and service providers must present photo identification upon arrival, and a log must be maintained that records the details of the visit. All visitors should be escorted. In addition, all visitors and service providers should be issued temporary identification. If temporary identification is used, it must be visibly displayed at all times du		

D			

D	[illegible]	[illegible]	[illegible]
11.2	In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted. Based on the sensitivity of the position, employee vetting requirements should extend to temporary workforce and contractors. Once employed, periodic reinvestigations 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, encompassing 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.		

D	[illegible]	[illegible]	[illegible]
12.2	Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and Instruments of International Traffic (IIT) must be trained to inspect their conveyances/IIT for both security and agricultural purposes. Refresher training must be conducted periodically, as needed after an incident or security breach, 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; and • Signs of pest contamination.		Must
12.4	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/drill, or regular audits of procedures etc. are some of the measures that the Member may implement to determine the effectiveness of the training.	Should
12.8	As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.	Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	Must

D			
12.10	Personnel must be trained on how to report security incidents and suspicious activities.	Procedures to report security incidents or suspicious activity are extremely important aspects of a security program. Training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures, including specifics on the process, such as, what to report, to whom, how to report the incident, and	