Minimum Security Criteria – Third Party Logistics Providers (3PLs)

November 2019

Note: Criteria ID numbers may not be sequential. ID numbers not listed are not applicable to 3PLs.

First Focus Area: Corporate Security

1. **Security Vision & Responsibility –** 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. Instilling security as an integral part of a company's culture and ensuring that it is a companywide priority is in large part the responsibility of the company's leadership.

ID	Criteria	Implementation Guidance	Must / Should
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' (o)-7.1te1 ((12./.2 (e1 (;9 (12.B>(o)-7.1 (dp (e) hEM4J0T7 Tw [T/09 (k ('	
	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 broader scope than traditional security programs. It is inters among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	Should

ID

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

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.	A crisis may include the disruption of the movement of traud 6306.1pude t o a cerd 630.8 (t)lacu,h a n	

ID		Criteria	Implementation Guidance	Must / Should
3.1	CTPAT Me	[redacted] must have a written, risk based pro[redacted] screening new business partners a[redacted] monitoring current		

ID	Criteria	Implementation Guidance	Must / Should
3.4	The business partner screening process must take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition		

ID	Criteria	Implementation Guidance	Must / Should
3.8	For inbound shipments to the United States, if a Member subcontracts transportation services to another highway carrier, the Member must use a CTPAT certified highway carrier or a highway carrier that works directly for the Member as delineated through a written contract. The contract must stipulate adherence to all minimum security criteria (MSC) requirements.	The carrier should provide a list of subcontracted carriers and drivers to the facilities where it picks up and delivers cargo. Any changes to the subcontractor list should be immediately conveyed to relevant partners. When reviewing service providers for compliance, the Member should verify that the company subcontracted is actually the company transporting the loads—and has not further subcontracted loads without approval. Members should limit subcontracting transportation services to one level only. If exceptions are allowed for further subcontracting, the CTPAT Member and the shipper should be notified that the load was further subcontracted.	Must

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. Measures to secure a company's information technology (IT) and data are of paramount importance, and the listed criteria provide a foundation for an overall cybersecurity program for Members.

   Key Definitions: Cybersecurity – Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

   Information Technology (IT) – IT includes computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

ID	Criteria	Implementation Guidance	Must / Should
4.1	CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover		

ID	Criteria	Implementation Guidance	Must / Should
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 ava	

ID	Criteria	Implementation Guidance	Must / Should
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 uneulj nl-uss18.1 (3)-d m63 (r9 1.49.i1 (r9dac d m63 (e4 9 (ch.16.)9	

ID	Criteria	Implementation Guidance	Must / Should
4.9	Members that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.	VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method. An example of a multi-factor authentication would be a token with a dynamic security code that the employee must type in to access the network.	Must
4.10	If Members allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.	[redacted] devices include storage media like CDs, D[illegible] (d)-egulnd pro4e CDdersona01M	

ID	Criteria	Implementation Guidance	Must / Should
4.12	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	Data backups should take place as data loss may affect individuals within an	

Breaches in supply chains occur most often during the transportation pr

ID	Criteria	Implementation Guidance	Must / Should
5.3	CTPAT Members must ensure that the following systematic CTPAT security and agricultural inspections are conducted. Requirements for these inspections will vary depending upon if the supply chain is land-based (Canada or Mexico) or if the supply chain originates overseas (ocean and air modes). Prior to stuffing/packing, all empty Instruments of International Traffic (IIT) must be inspected, and conveyances must also be inspected when they are crossing land borders into the United States. <u>Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight:</u> A seven-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an eight-point inspection must be conducted on all empty refrigerated containers and ULDs: 1. Front wall; 2. Left side; 3. Right side; 4. Floor; 5. Ceiling/Roof; 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors; 7. Outside/Undercarriage; and 8. Fan housing on refrigerated containers. <u>Additional inspection requirements for land border crossings via highway carriers:</u> 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.		

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria

ID	Criteria	Implementation Guidance	Must / Should
5.19	If a GPS tracking system is used, carriers should use a sensor coupling/connector or equivalent technology from the tractor to the trailer to ensure the trailer is also monitored and tracked.		Should
5.20	Carriers should use electronic dispatch logs; the logs should be recorded and kept for audit purposes.	Electronic dispatch logs 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 a supply chain.	Should

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

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 dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number.		

ID	Criteria	Implementation Guidance	Must / Should
6.5	CTPAT Members (that maintain seal inventories) must be able to document that the high-security seals they use meet or exceed the most current ISO 17712 standard.	Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high-security seal standard. CTPAT Members are expected to be aware of the tamper indicative features of the seals they purchase.	Must

ID	Criteria	Implementation Guidance	Must / Should
7.5	As documented evidence of the properly installed seal, digital photographs should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.	Photographic evidence may include pictures taken at the point of stuffing to document evidence of the cargo markings, the loading process, the location where the seal was placed, and properly installed seal.	Should
7.6	Procedures must be in place to ensure that all information used in		

ID	Criteria	Implementation Guidance	Must / Should
7.10	Personnel must review the information included in import/export documents to identify or recognize suspicious cargo shipments. Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment. Based on risk, CTPAT Members should take into account those CTPAT key warning indicators for money laundering and terrorism financing activities mostinundering and		

ID	Criteria	Implementation Guidance	Must / Should
7.13	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	

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 docume,co 2.1 (s)1h[co)-4.1 (nh96705 T 0 -1.2298t)2.6 (a)2.0.004 cin annh96705 T 0 -13 (h)-9.1 (	

ID	Criteria	

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

Third Focus Area: People and Physical Security

ID	Criteria	Implementation Guidance	Must / Should
9.6	Adequate lighting must be provided inside and outside the facility		

ID	Criteria	Implementation Guidance	Must / Should
9.10	All security technology infrastructure must be physically secured from unauthorized access.	Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed circuit television cameras, power and hard drive components for cameras, as well as recordings.	Must
9.11	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 your security may attempt to disable the power to your security technology in order to circumnavigate it. Thus, it is important to have an alternative source of power for your security technology. An alternative power source may be an auxiliary power	

ID	Criteria	Implementation Guidance	Must / Should
		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.	

10. **Physical Access Controls –** 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.

ID	Criteria	Implementation Guidance	Must / Should
10.1	CTPAT Members must have written procedures governing how identification badges and access devices are granted, changed, and removed.		

11. <u>Personnel Security</u> – 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 emwTj-0.00m.-dw1mee screen21n2[3)3 56a3d10 (ap)4 (e)3TJ0 Tc 0 Tw 738.32 62

12. <u>Education, Training and Awareness</u> – 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 maintaining a layered security program needs the active participation and support of several departments and various personnel. One of the key aspects to maintaining a security program is training. Educating employees on what the threats are and how their role is important in protecting the company's supply chain is a significant aspect to the success and endurance of a supply chain security program. Moreover, when employees understand why security procedures are in place, they are much more likely to adhere to them.

ID	Criteria	

ID	Criteria	Implementation Guidance	Must / Should
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
12.7	Training must, in accordance with the Member's business model, be provided to applicable personnel on preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirem (e)34a.96 113.64 420.12 Tm[(T)1 (i)hmC1 113.8r c h 1 (c n d b a) 2 . 1 (n c) 6 . 3 (0 . 5		