Minimum Security Criteria – Mexican Long Haul Highway Carriers

November 2019

Note: Criteria ID numbers may not be sequential. ID numbers not listed are not applicable to Mexican Long Haul Highway Carriers.

First Focus Area: Corporate Security

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'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 broader scope than traditional security programs. It is intertwined with Security, in many departments such as Human Resources, Information Technology, and Import/Export offices. Supply Chain Security programs built on a more traditional, security department-based model may be less viable over the long run because the responsibility to carry out the security measures are concentrated among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	Should

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 responsibilities and all security procedures outlined by the security program are being carried out as designed. The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk.	The goal of a review for CTPAT purposes is to ensure that its employees are following the company's security procedures. The review process does not have to be complex. The Member decides the scope of reviews and how in-depth they will be - based on its role in the supply chain, business model, level of risk, and variations between specific locations/sites.	

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. **c.376 scn675 318.84 39.6EM.24 ref*0 CS0 csI1 scnTw f62 up9.**

ID	Criteria	Implementation Guidance	Must / Should
3.1	CTPAT Members must have a written, risk based process for screening new business partners and for monitoring current partners. A factor that Members should include in this process is checks on activity related to money laundering and terrorist funding. To assist with this process, please consult CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities.	The following are examples of some of the vetting elements that can help determine if a company is legitimate: • Verifying the company's business address and how long they have been at that address; • Conducting research on the internet on both the company and its principals; • Checking business references; and • Requesting a credit report. Examples of business partners that need to be screened are direct business partners such as manufacturers, product suppliers, pertinent vendors/service providers, and transportation/logistics providers. Any vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information/equipment are also included on the list to be screened; this includes brokers or contracted IT providers. How in-depth to make the screening depends on the level of risk in the	

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 Arrangement (MRA) with the United States (or an approved MRA). Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners, and Members must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification.	Business partners' CTPAT certification may be ascertained via the	

ID	Criteria	Implementation Guidance	Must / Should
		may conduct an onsite audit at the facility, hire a contractor/service provider to conduct an onsite audit, or use a security questionnaire. If security questionnaires are used, the level of risk will determine the amount of detail or evidence required to be collected. More details may be required from companies located in high-risk areas. If a Member is sending a security questionnaire to its business partners, consider requiring the following items: •Name and title of the person(s) completing it; •Date completed; •Signature of the individual(s) who completed the document; •*Signature of a senior company official, security supervisor, or authorized company representative to attest to the accuracy of the questionnaire; •Provide enough detail in responses to determine compliance; and •Based on risk, and if allowed by local security protocols, include photographic evidence,cllooo theued t 7-0.9 (u)-671J(y)-2(l)-8 (nn (l)-uk0co)-7 (-0.004 Tc 0.007 Tw	

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 all of the individual Cybersecurity criteria.	Members are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards. The *National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The Framework complements an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one. *NIST is a non-regulatory federal agency under the Department of Commerce that promotes and mai.4 (c)-14.7 (e .19 (l)5.1 (o) c (o)1.9 (c)6.)-6e (,)9.9 (i)-16neomege c	

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 available. The frequency of the testing will depend on various factors including the company's business model and level of risk. For example, companies shoerofwaa (f)8. (w0.00r)4.6 (e)9 (po)1B (l)5.1 ( )]TJ(a) e tca.9 (e)-9 -1.229 Td[(o	

ID	Criteria	Implementation Guidance	Must / Should
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.	Personal devices include storage media like CDs, DVDs, and USB flash drives. Care must be taken if employees are allowed 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.	Must
4.11	Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.	Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer or 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 authorized copies of 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 civil penalties and criminal prosecution. Software pirates increase (r)-7.2 (n 3 (o)1.)10.5 (1 (he)9pm)-1624.4 (e,)-7 22.771 1 (he)901 Tc 0as.s os foi w . 5 (2 2 . (	

Second Focus Area: Transportation Security

5. **<u>Conveyance and Instruments of International Traffic Security</u>** – 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 altering of IIT structures or surreptitious entry into them, which could allow the introduction of unauthorized material or persons.

   At the point of stuffing/loading, procedures need to be in place to inspect IIT and properly seal them. Cargo in transit or "at rest" is under less control, and is therefore more vulnerable to infiltration, which is why seal controls and

ID	Criteria	Implementation Guidance	Must /

ID	Criteria	Implementation Guidance	Must / Should
	Additional inspection requirements for land border crossings via highw8 re.2 (8 r.005 Tw 9.96 -0 0 9.96 236.)/ents8 cn684.84 5o6 -0 0 9. -0 0 9. -0 0 9. -0 0 9. -0 q189 0.48 ref103.32 (s)10.47.32 56(2001r.005 Tw 9 539.0 1 4 Tm[(A)5..2 1		

ID	Criteria	Implementation Guidance	Must / Should
5.24	In areas of high risk, and immediately prior to arrival at the border crossing, CTPAT Members should incorporate a "last chance" verification process for U.S. bound shipments for checking conveyances/Instruments of International Traffic for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process. Properly trained individuals should conduct the inspections. V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.		Should
5.26	Drivers must report and record any anomalies or unusual structural modifications found on the conveyance following a government inspection.	These include U.S. Department of Transportation (DOT) inspections or other regulatory agency inspections. It also includes inspections taking place in Mexico and Canada.	Must
5.27	Management must regularly conduct random reviews of the tracking and monitoring procedures. The review findings must be recorded. The revieo-25.39[usco ervh erf28.8 (i)-0.9 ( )-1181 (a)-3.9 (t)-3.4 (i)-0.9 (o)-4.1 (n)-6.1 (o)-4.1 (f28.8 (t)-3.4 hd)-6.1 (e)3 (t)-3.4 (r)-1.4 (a)-3.9 c(k)-3.8 (i)19 (n)-6.1 (gli)-0. ando(vh12.2 (ro)-4.4 (i)1.6 fia)-3.9 cI aons (n)96.1 roo		

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 allh3.9 (y)-8eW nBT30.008.84-9.31 2 Cy dri-9.31 1(d)-9.6y-4.4yy-4.06 (t)-2.-9.ru2 (y (-9.iil -2.)--4.06 (l-4.4)2m.1 (n9.14)-a)6a0144(7 338671 -108.8t)2ryp2 (yp2 (yly4-9. c)		

ID	Criteria	Implementation Guidance	Must / Should
	Inventory, Distribution, & Tracking (Seal Log): • Recording the receipt of new seals. • Issuance of seals recorded in log. • Track seals via the log. • Only trained, authorized personnel may affix seals to Instruments of International Traffic (IIT). **Controlling Seals in Transit**: • When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering. • Confirm the seal number matches what is noted on the shipping documents. 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. • The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number. • The shipper must note the replacement seal number in the seal log. **Seal Discrepancies:** • Retain altered or tampered seals to aid in investigations. • Investigate the discrepancy; follow-up with corrective measures (if warranted). • As applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation.		

ID	Criteria	Implementation Guidance	Must / Should
6.2	All CTPAT shipments that can be sealed must be secured immediately after loading/stuffing/packing by the responsible party (i.e. the shipper or packer acting on the shipper's behalf) with a high-security seal that meets or exceeds the most current International Organization for Standardization (ISO) 17712 standard for high-security seals. Qualifying cable and bolt seals are both acceptable. All seals used must be securely and properly affixed to Instruments of International Traffic that are transporting CTPAT Members' cargo to/from the United States.	The high-security seal used 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 center most vertical bar of the right container door. Alternatively, the seal could be placed on the center most left-hand locking handle on the right container door if the secure cam position is not available. If a bolt seal is being used, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp.	Must
6.3	Less Than Truck Load (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. At the last pickup site prior to crossing the border, the carrier must seal the load with an ISO 17712 complian s31llia2.1 (s)10.5 (t)2.61c.723 0 Td( )TjETEMC-1.9 (r)-11.8 49.919 122.16 reW nBT- Td[24.34.6 (e)3 (cu)-6.1 (()-2.2		

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
6.7	CTPAT's seal verification process must be followed to ensure all high-security seals (bolt/cable) have been affixed properly to Instruments of International Traffic, and are operating as designed. The procedure is known as the VVTT process: V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T –		

7. **<u>Procedural Security –</u>** 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 [illegible]

ID	Criteria	Implementation Guidance	Must / S

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 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 drivers' view, frequent documented audits of dispatcher logs, and trend analysis using GPS data to compare drivers' average time against which dispatch staff members are on duty.	Must
7.14	If legally allowed, and permissible under union rules, carriers should conduct random screening of truck drivers' luggage and personal belongings. If any suspicious anomalies are found during the screening, the carrier should document and report its findings to U.S. Customs and Border Protection.		Should
7.16	For U.S. bound shipments, the highway carrier transporting the cargo (including subcontracted carriers) must use its own SCAC code regardless of whether the carrier is using a FAST or regular lane.		Must
7.17	In accordance with U.S. Department of Transportation standards, CTPAT highway carriers should have a comprehensive vehicle preventive maintenance program in place and ensure the drivers		

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
7.25	CTPAT Members should set up a mechanism to report security		

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	

Third Focus Area: People and Physical Security

9. <u>Physical Security</u> – 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.

ID	Criteria	Implementation Guidance	Must / Should
9.1	All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.		Must
9.2			

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.	Must
9.7	Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	Electronic security technology used to secure/monitor sensitive areas and access points includes: burglar4dSn6 -0 0d access	

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 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
9.17	When a loaded trailer is transferred to another carrier for immediate transport across the U.S. border, the Long Haul Highway Carrier must ensure that the location of the transfer is in an area that is controlled to prevent un-manifested material and or unauthorized personnel from gaining access to the trailer/conveyance. If the loaded trailer is not going to be immediately transported across the border, the trailer must be staged or stored in a trailer yard that has physical barriers and deterrents that guard against unauthorized access to the trailer. The driver must also call the dispatcher to notify the time and location whnionu.1 (i)-1 t1 (1)]TJ trate (nu.1 (i wa t)2.5 (s)11 (i 05 Tc -0.002 Tw 0 -1.229 Td[phys)10.d)1.9 (s)10.5 (pp a)2.1 (cg)6.2 (t)2.7 (o)1.9 ( )2.1 (ns)10.5 (f)8		

ID	Criteria	Implementation Guidance	Must / Should

ID	Criteria	Implementation Guidance	Must / Should
12.3	Personnel 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, personnel must be instructed in controlling/using seals during transit, and to look for signs of someone observing the movement of the conveyance and/or the goods. Drivers, for instance, must be trained on how to conduct the seal		