**Company Information**

**Company Name:**

**Street Address:**

**City: State: Postal Code: Country:**

**DUNS Number: MID Number**:

**PREPARER INFORMATION:**

**Name: Title:**

**Phone: E-Mail Address:**

**Is the company public or private? If private, list majority owner(s) (holding over 10% ownership):**

**Indicate Type(s) of Business**

**(Check all that apply)**  **Importer**  **Foreign Manufacturer**  **Highway Carrier**

**Exporter**  **3PL**  **Warehouse**

**Consolidator**  **Air Carrier**  **Rail Carrier**

**Sea Carrier  US Marine Port or Terminal Operator**

**Broker  Foreign Based Marine Port Terminal Operator**

**Mexican Long Haul Highway Carrier**

**Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Indicate if your company participates in any of the following programs (check all that apply):**

**CTPAT: Customs-Trade Partnership Against Terrorism**

**Has your company sent us a request to monitor CTPAT status using the Status Verification Interface (SVI) portal?**

**CTPAT Contact e-Mail address: \_\_\_\_\_\_\_\_\_\_\_\_\_**

**PIP: Partners In Protection (Canada) # \_\_\_\_\_\_\_\_\_\_\_\_\_**

**AEO: Authorized Economic Operator Security # \_\_\_\_\_\_\_\_\_\_\_\_\_**

***CTPAT, PIP or AEO/OEA approved companies do not need to complete the remaining sections of this questionnaire.***

***INSTRUCTIONS:***

1. Respond to each question below using one of the following response codes:

* **Yes** The practice or procedure is firmly in place.
* **Partially** The practice or procedure is partially in place.
* **No** The practice or procedure is not in place.
* **N/A = Not Applicable** The practice or procedure is not in place.

1. Provide any additional information in the “Comments” box. If additional space is needed to fully respond, please attach a separate sheet, referring to the section number and question number.
2. Return the completed questionnaire to the Tenneco Requester.

|  |  |  |
| --- | --- | --- |
| **Section 1: Security Vision and Responsibility** | **Code** | **Comments** |
| (1) Is your supply chain security program 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. |  |  |
| (2) Confirm your company’s point(s) of contact (POC) who is knowledgeable about Security program requirements (List in "Comments" Section). These individuals need to provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security related exercises, and Security validations. |  |  |
| **Section 2: Risk Assessment** | **Code** | **Comments** |
| (1) Confirm your company conducts and documents the amount of risk in their supply chains. Business Partners must conduct an overall risk assessment (RA), no less than annually to identify where security vulnerabilities may exist. The RA must identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities.  The Business Partner must take into account applicable security program requirements specific to the member’s role in the supply chain. |  |  |
| **Section 3: Business Partners** | **Code** | **Comments** |
| (1) Business Partners must have a written, risk based process for screening new business partners and for monitoring current partners. A factor that Business Partners should include in this process is checks on activity related to money laundering and terrorist funding. |  |  |
| (2) If a Business Partner outsources or contracts elements of your supply chain, the Business Partner must exercise due diligence (via visits, questionnaires, etc.) to ensure these business partners have security measures in place that meet or exceed Minimum Security Criteria (MSC). |  |  |
| (3) 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. |  |  |
| **Section 4: Cyber Security** | **Code** | **Comments** |
| (1) Are comprehensive written cybersecurity policies and/or procedures in place to protect information technology (IT) systems? |  |  |
| (2) If a data breach occurs or an event results in the loss of data and/or equipment, do procedures include the recovery (or replacement) of IT systems and/or data? |  |  |
| (3) Are policies and procedures in place to prevent attacks via social engineering? |  |  |
| (4) Is a system 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? |  |  |
| (5) Has software/hardware been installed for the protection from malware (viruses, spyware, worms, Trojans, etc.) and has an internal/external intrusion detection system been installed (firewalls)? |  |  |
| (6) Is security software current and does it receive regular security updates? |  |  |
| (7) If employees are allowed to use personal devices to conduct company work, do all such devices adhere to the company’s cybersecurity policies and procedures to include regular security updates and a method to securely access the company’s network? |  |  |
| (8) When users are allowed to remotely connect to a network, are secure technologies employed, such as virtual private networks (VPNs), to allow employees to access the company’s intranet securely when located outside of the office? Are procedures in place that are designed to prevent remote access from unauthorized users? |  |  |
| (9) Do individuals with access to IT systems use individually assigned accounts protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication? |  |  |
| (10) Is user access restricted and reviewed based on job description or assigned duties? |  |  |
| **Section 5: Conveyance and IIT Security** | **Code** | **Comments** |
| (1) Conveyances and Instruments of International Traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instrument of International Traffic or (as applicable) allow the seal/doors to be compromised. |  |  |
| (2) Business Partners must ensure that the following systematic security and agricultural inspections are conducted. Included in these inspections include a 17 Point Inspection (as applicable) of the Tractor, Trailer/Container. These processes must be documented. |  |  |
| (3) Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. 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. |  |  |
| (4) 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. |  |  |
| (5) 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) Tenneco immediately after any law enforcement agencies, as appropriate. |  |  |
| **Section 6: Seal Security** | **Code** | **Comments** |
| (1) Business Partners must have written processes relating to seal security; including: • Controlled access to seals • Inventory, distribution and tracking • Control of seals in transit / broken in transit • Identification of seal discrepancies  Procedures must undergo annual review. |  |  |
| (2) Business Partners must be able to document that the high-security seals they use meet or exceed the most current ISO 17712 standard. |  |  |
| (3) 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 – 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. |  |  |
| **Section 7: Procedural Security** | **Code** | **Comments** |
| (1) When cargo is staged overnight, or for an extended period of time, measures must be taken to secure the cargo from unauthorized access. 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. |  |  |
| (2) Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo is legible; complete; accurate; protected against the exchange, loss, or introduction of erroneous information; and reported on time |  |  |
| (3) 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. |  |  |
| (4) Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. 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 unauthorized individual from the premises. |  |  |
| (5) All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate. |  |  |
| (6) Business Partners must initiate their own internal investigations of any security-related incidents (terrorism, narcotics, stowaways, absconders, etc.) immediately after becoming aware of the incident. The company investigation must not impede/interfere with any investigation conducted by a government law enforcement agency. |  |  |
| **Section 8: Agricultural Security** | **Code** | **Comments** |
| (1) If Wood Packaging Materials (WPM) are used, are measures regarding WPM used to meet the International Plant Protection Convention’s (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15)? |  |  |
| (2) Are cargo staging areas, and the immediate surrounding areas, inspected on a regular basis to ensure these areas remain free of visible pest contamination? |  |  |
| (3) If visible pests are detected, are prevention measures taken where applicable in the supply chain? |  |  |
| **Section 9: Physical Security** |  |  |
| (1) All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access. |  |  |
| (2) 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 labor laws. |  |  |
| (3) 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 |  |  |
| **Section 10: Access Controls** | **Code** | **Comments** |
| (1) Business Partners 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 place 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 when the employees separate from the company. |  |  |
| (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 during the visit.  The registration log must include the following: • Date of the visit; • Visitor's name; • Verification of photo identification (type verified such as license or national ID card). Frequent, well known visitors such as regular vendors may forego the photo identification, but must still be logged in and out of the facility; • Time of arrival; • Company point of contact; and • Time of departure |  |  |
| (3) Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load. |  |  |
| 4) A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it. The cargo pickup log should have the following items recorded: • Driver's name; • Date and time of arrival; • Employer; • Truck number; • Trailer number; • Time of departure; • The seal number affixed to the shipment at the time of departure. |  |  |
| **Section 11: Personnel Security** |  |  |
| (1) Written processes must be in place to screen prospective employees and to periodically check current employees. Application information, such as employment history and references, must be verified prior to employment, to the extent possible and allowed under the law |  |  |
| (2) Business Partners must have an Employee Code of Conduct that includes expectations and defines acceptable behaviors. Penalties and disciplinary procedures must be included in the Code of Conduct. Employees/contractors must acknowledge that they have read and understood the Code of Conduct by signing it, and this acknowledgement must be kept in the employee’s file for documentation. |  |  |
| **Section 12: Education, Training & Awareness** |  |  |
| (1) Business Partners must establish and maintain a security training and awareness program to recognize 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 supply chain security requirements |  |  |
| (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. |  |  |
| (3) 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. |  |  |
| (4) Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable. |  |  |
| (5) Personnel must be trained on how to report security incidents and suspicious activities. |  |  |