



Protected B (when completed)
*formulaire disponible en français

specimen

PARTNERS IN PROTECTION: SECURITY PROFILE

**Canada Border Services Agency
Enforcement Branch
Policy and Program Development Directorate
Program Development Division**

Privacy Statement

Except for the information specified in Section 1.8 and solely for the purpose specified and to the entity specified therein, the information provided in this Security Profile, including any supporting documentation, is collected under the *Customs Act* (Canada), and is “customs information” as that term is defined therein.



General Information

This Security Profile was designed to ensure that PIP program applicants implement effective security practices to secure their supply chain and mitigate the risk of contraband smuggling.

The Canada Border Services Agency (CBSA) recognizes the complexity of international supply chains and endorses the application and implementation of security measures and systems using a risk-based approach. Therefore, the PIP program allows for the flexibility and customization of security measures based on the applicant's business model.

To be eligible for the PIP Program applicants must meet the following eligibility criteria:

NUMBER	CRITERIA
1	The applicant must fall within one of the authorized eligible business categories: importer; exporter; carrier; customs broker; courier; warehouse operator (including marine terminals); freight forwarder; or shipping agent.
2	The applicant must own or operate facilities in Canada that are directly involved in the importation or exportation of commercial goods. OR The applicant must be a U.S. highway carrier company that is a member of or is applying for FAST into Canada.
3	The applicant and its directors must be of good character and have a good record of compliance with the CBSA.

Application Process

1. The PIP application process has three stages:
 - i) The completion of the Security Profile by the applicant;
 - ii) The completion of a security review and a site validation by the CBSA; and
 - iii) The signing of a Memorandum of Understanding (MOU) by both the applicant and the CBSA.
2. Upon receipt of a completed Security Profile, a security review and site validation will be undertaken by the CBSA to confirm the security measures, detailed in the Security Profile.
3. If the security review and site validation conclude that the applicant meets or exceeds the minimum security criteria, the applicant will be notified and asked to sign two original copies of the PIP MOU prepared by the CBSA and return both to the Agency for its signature. The MOU sets out the roles and responsibilities of the applicant to maintain its status as an authorized member of the PIP program.



4. After the CBSA has signed both copies of the PIP MOU, one copy will be returned to the applicant along with a certificate of membership. At this time, the applicant will be considered to be an authorized PIP member.
5. An application may be rejected for any omission or the submission of false information.
6. Should the security review and site validation of the CBSA conclude that the applicant does not meet the minimum security criteria, the application will not be considered further without the applicant having addressed the security vulnerabilities identified in the site validation report to the complete satisfaction of the CBSA.

Application Instructions

1. Complete Sections 1 and 2 of the Security Profile with the requested company information.
2. Detail how the company meets or exceeds each of the minimum security criteria set out in Sections 3 to 11.
3. Complete the sector-specific sections (12-17) relevant to section 1.4.
4. Return a completed electronic copy of the Profile by e-mail as a PDF attachment to the PIP program: PIP-PEP@cbsa-asfc.gc.ca, or if you have printed and completed a paper copy, mail it to the CBSA: Partners in Protection, 191 Laurier Avenue West, 10th floor, Ottawa, ON K1A 0L8.

Since the information collected is sensitive, the Security Profile form is encrypted and password protected. If a hard copy form is submitted instead of an electronic attachment, protect your information by mailing in your form using an inner and outer envelope.

5. An incomplete Security Profile will not be processed.
6. Direct any questions about the Security Profile to the CBSA by e-mail through the PIP program: PIP-PEP@cbsa-asfc.gc.ca

Additional Security Requirements (if accepted into the PIP program)

1. Notification in writing of any changes to the company information contained in Sections 1 and 2 must be provided to the CBSA within 30 days of such changes.
2. When changes to the Security Profile information provided by the applicant occur, an updated Security Profile must be provided to the CBSA no later than three years from the date of the present Security Profile.



1. COMPANY INFORMATION

1.1 Company Name (legal entity)

1.2 Operating/Doing Business As (if different)

1.3 Business Profile

Business Number (BN) (Provide 9-digit Registration Number)

Account security number

Carrier code (your company must have a valid carrier code issued by the CBSA)

Dunn and Bradstreet number (xx-xxx-xxxxx)

Business Start Date

Number of employees

1.4 Business Sector(s)

Please select the sector(s) that best describe your business. Each applicant company must complete sections 1 to 11 of this form, as well as the section indicated next to the sector(s) selected.

- highway carrier - section 12
- rail carrier - section 17
- freight forwarder
- customs broker - section 13
- importer
- shipping agent
- courier - section 14
- exporter
- marine carrier - section 15
- warehouse operator (includes marine terminals)
- air carrier - section 16

1.5 Participation in Other Programs

Please indicate whether you participate in the following programs:

- Customs Self Assessment (CSA)
- Free and Secure Trade (FAST) Canada (CSA/FAST approved importers or carriers)
- Free and Secure Trade (FAST) U.S. (FAST approved importers or carriers)
- Customs – Trade Partnership Against Terrorism (C-TPAT) (Please provide C-TPAT Account Number)
- Authorized Economic Operator country(ies)
- Other Programs (Specify)

If your company is based in the U.S., please provide the following information, where applicable:

U.S. carriers: Standard Carrier Alpha Code (SCAC)

U.S. importers: Importer of Record (IOR) number

U.S. manufacturers: Manufacturer ID (MID)



1.6 CBSA PIP Web site

Do you agree to allow the CBSA to post your name on its Web Site as a member of the PIP program?

Yes No

1.7 Company Web Site Address

1.8 Information Sharing

Other Government of Canada agencies and departments and foreign governments may ask the CBSA for information regarding your status/membership in the PIP program. For example, PIP program information may be shared with C-TPAT for mutual recognition purposes, and with Transport Canada for the Air Cargo Security Initiative. The information to be shared may include the member's name, address, membership status and site validation report information. Any information disclosed for a specified purpose to a specified entity will be treated confidentially by the entity and will be used solely for that specified purpose.

1.9 Business Address

Physical address		Mailing address (if different)	
Unit number		Unit number	
Street		Street	
City		City	
Prov./terr./state		Prov./terr./state	
Country		Country	
Postal code/zip code		Postal code/zip code	
Additional delivery info.		Additional delivery info.	

1.10 Names and Dates of Birth of all Company Directors

Surname/Last Name	Given Name(s)	Date of Birth
		yyyy-mm-dd

1.11 Multiple Locations

List all locations and their addresses (in Canada) covered by this application:

Site Contact Person	Complete Address	Brief Description of Business



2. COMPANY CONTACT INFORMATION

For the purposes of this application, we require the name of a designated company contact and an alternate contact. Should these contacts change, you must advise the CBSA within 30 days. The contact should be the person within the company responsible for security commitments.

2.1 Company Contact

Company Contact		Alternate Contact	
First and Last Name	<input type="text"/>	First and Last Name	<input type="text"/>
Position Title	<input type="text"/>	Position Title	<input type="text"/>
Telephone	<input type="text"/>	Telephone	<input type="text"/>
Fax	<input type="text"/>	Fax	<input type="text"/>
E-mail	<input type="text"/>	E-mail	<input type="text"/>

2.2 Security Profile Completed By

If this application has been completed by a third party, you must attach a letter of authorization signed by the company director.

2.3 Security Profile Completed On (yyyy-mm-dd)

2.4 Brief Company History/Background

2.5 Criminal Offences

Has the company or any director been charged with and/or convicted of an offence for which a pardon was not received?

- Yes No

2.6 Correspondence Language

Please select your preferred language of correspondence.

- English French



Complete sections 3 to 11 by describing in detail your company's policies, practices and procedures, and demonstrating how the minimum security criteria have been met. In the text box for each section, provide a narrative description of your company's security procedures (do not merely repeat the criteria). Responses such as "Not applicable" or "Does not apply" are NOT sufficient. If you feel that a section does not apply to your company's business model, give a brief explanation of the reasons why. Each response must make reference to the section number.

Acceptance of your company into the PIP program is dependant on the responses provided in this Profile. Inadequate or incomplete responses will result in the application being rejected.

3. Physical Security and Access Controls

Applicants must implement measures that assure the security of buildings, as well as those that monitor and control exterior and interior perimeters. They must also implement access controls that prohibit unauthorized access to facilities, conveyances, loading docks and cargo areas.

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Access controls prevent unauthorized entry into facilities, maintain control of employees, visitors and individuals, and protect company assets.

Procedures must be in place to prevent, detect and deter unmanifested material and unauthorized personnel from gaining access to conveyances and facilities. PIP applicants should incorporate the physical security criteria in this section throughout their supply chain, as applicable.

3.1 Facilities

Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained through periodic inspection and repair. All external doors, windows, gates and fences must be secured with locking devices. Cargo handling and storage facilities must have physical barriers and/or deterrents that guard against unauthorized access.

Provide details:

specimen



3.2 Key Control

Management or security personnel must control the issuance of all locks and keys.

Provide details:

specimen

3.3 Lighting

Adequate lighting must be provided inside and outside the facility including in the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Provide details:

3.4 Communications

Communications systems must be in place to contact internal security personnel and local law enforcement officials as required. These systems should have some form of backup and be tested on a regular basis.

Provide details:

specimen



3.5 Parking

Private passenger vehicles for visitors and employees should be prohibited from parking in or adjacent to cargo handling and storage areas.

Provide details:

specimen

3.6 Fencing

Perimeter fencing should enclose the areas around cargo handling and storage facilities, and be of sufficient height and type to restrict the threat of unlawful access. Interior fencing within a cargo handling facility should be used to segregate domestic, international, high value and hazardous cargo. All fencing must be inspected regularly for integrity and damage.

Provide details:

3.7 Signage

Signage should exist to direct conveyances and persons to appropriate areas and prevent or deter unauthorized personnel from accessing restricted areas.

Provide details:



3.8 Gates and Gate Houses

Gates through which vehicles and/or personnel enter and exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

Provide details:

specimen

3.9 Alarm Systems and Video Surveillance

Alarm systems and video surveillance should be used to monitor premises and prevent unauthorized access to cargo handling and storage areas. Signage indicating the use of surveillance equipment should be posted around the facility.

Provide details:

3.10 After-Hours Access

For companies that do not operate 24/7, provide details of after-hours access.

Provide details:

specimen



3.11 Physical Access Controls

Access controls prevent unauthorized entry into facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors and vendors at all points of entry.

Unauthorized access to shipping, loading dock and cargo areas must be prohibited.

Provide details:

specimen

3.12 Employees

An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to the secure areas needed for the performance of their duties. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys and key cards) must be documented.

Provide details:

3.13 Visitors

Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification. To the extent feasible and as threat conditions warrant, the access of contractors and visitors to non-public areas of company-designated critical infrastructure should be restricted, and the activities of visitors in or around such infrastructure should be monitored.

Provide details:



3.14 Challenging and Removing Unauthorized Persons and Vehicles

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons and vehicles.

Provide details:

specimen

3.15 Deliveries (including mail)

Proper vendor and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be screened periodically before being disseminated.

Provide details:

specimen



4. Procedural Security

Measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, customs clearance and storage of cargo in the supply chain. Applicants must ensure that business partners develop security processes consistent with PIP security criteria to enhance the integrity of the shipment at its point of origin up to its point of final destination. Periodic reviews of business partners' processes and facilities should be conducted based on risk. These processes and facilities should maintain the security standards required by the PIP member.

4.1 Process Mapping

Map your process by illustrating or describing (step by step) the flow of goods and documentation/information through your international supply chain.

Provide details:

4.2 Shipping and Receiving (drivers)

Drivers delivering or receiving cargo must be positively identified before cargo is received or released. A designated security representative or employee should supervise the introduction/removal of cargo.

Provide details:

specimen



4.3 Cargo Tracking

Procedures should be in place to track the timely movement of incoming and outgoing cargo.

Provide details:

specimen

4.4 Cargo Reconciliation

Arriving cargo must be reconciled against information on the cargo manifest. Measures must be in place to detect and report cargo shortages and overages. All shortages, overages and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. The cargo should be accurately described and the weights, labels, marks and piece counts indicated and verified.

Provide details:

4.5 Security Sweeps

Random, unannounced security assessments should be conducted of areas in your company's control within the supply chain.

Provide details:

specimen



4.6 Reporting Anomalies or Suspicious Cargo Activity

In cases where anomalies or illegal activities are detected or suspected, the CBSA and/or other law enforcement agencies must be notified, as deemed appropriate.

Provide details:

specimen

4.7 Cargo Documentation Processing

Procedures must be in place to ensure that all information used in the clearing of cargo is legible, complete, accurate and protected against the exchange or introduction of erroneous information. To help ensure the integrity of cargo received from abroad, procedures must be in place so that information received from business partners is timely and reported accurately.

Procedures must be in place to ensure that the information in the carrier's cargo manifest (e.g. bill of lading) accurately reflects the information provided to the carrier by the shipper or its agent, and is filed with the CBSA in a timely manner. Documentation control must include safeguarding computer access and information.

Provide details:

specimen



5. Container, Trailer and Rail Car Security

Security must be maintained on all containers, trailers and rail cars used to import or export goods to protect them against the introduction of unauthorized material and/or persons. At the point of stuffing/packing, procedures must be in place to properly seal and maintain the integrity of the shipping container, trailer or rail car.

Companies should maintain an open dialogue with the CBSA on areas of common concern to collectively benefit from advancements in industry standards and container integrity technologies.

5.1 Cargo Integrity

Procedures must be in place for affixing, replacing, recording, tracking and verifying seals on containers, trailers and rail cars. Describe the security measures your company has implemented with respect to loaded and empty containers, trailers and rail cars used in the transport of international cargo.

Provide details:

5.2 Container, Trailer and Rail Car Inspections

Procedures must be in place to verify the physical integrity of the container structure, trailer and rail car prior to stuffing/packing, including verifying the reliability of the locking mechanisms of the doors and searching for signs of tampering. A seven-point inspection process is recommended for all containers:

- | | |
|-----------------------|----------------------|
| front wall | floor |
| left side | ceiling/roof |
| right side | inside/outside doors |
| outside/undercarriage | |

Provide details:



5.3 Container, Trailer and Rail Car Seals

Foreign business partners should have documented procedures that set forth their internal policy regarding the processing of cargo with high-security seals that meet or exceed the current ISO/PAS 17712 standard and/or other devices designed to prevent tampering with cargo.

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers and must include procedures for recognizing and reporting, as necessary, compromised seals and/or containers to the CBSA and other appropriate foreign authorities. Only designated employees should distribute container seals for integrity purposes.

Provide details:

5.4 Container, Trailer and Rail Car Storage

Containers, trailers and rail cars must be properly stored to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and deterring unauthorized entry into containers, storage areas, trailers and rail cars.

Provide details:

specimen



6. Data and Document Security

A well-defined physical security policy and system controlling access to any office or secure area must be in place to ensure that there is no unauthorized access to computers and equipment. Measures must be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access.

6.1 Cargo Manifest/Forms

Your company must have procedures in place for securing the storage of used and unused forms and related cargo documentation to prevent the loss or unauthorized use of such documentation.

Provide details:

6.2 Information Technology (IT) Security

Automated systems must use individually assigned accounts that require a periodic change of password. Trade-sensitive data should be protected through the use of necessary IT security policies and automated back-up capabilities.

Procedures and standards must be in place and provided to employees in the form of training to protect against unauthorized access to and the misuse of information.

Provide details:

6.3 Company Policies on IT Violations

A process must be in place to identify abuses of IT including improper access, or the tampering with or altering of business data. All system violators must be subject to appropriate disciplinary actions.

Provide details:



7. Personnel Security

Personnel security programs must incorporate the screening of employees and prospective employees. These programs should include periodic background checks on employees working in security-sensitive positions and the noting of unusual changes in an employee's apparent social and economic situation.

7.1 Pre-Employment Application Verification

Application information, such as employment history and references, must be verified prior to employment. Companies must maintain a permanent employee list.

Provide details:

7.2 Employee Background Checks

Consistent with foreign, federal and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed when needed.

Provide details:

7.3 Terminated/Departing Employees

Companies must have procedures in place to remove identification cards, as well as facility and system access for terminated and departing employees, and ensure that all company property is returned.

Provide details:



8. Security Training and Awareness

A security awareness program should be in place to inform and regularly remind individuals of security responsibilities, issues and concerns. The security awareness program provided to employees should include recognizing internal conspiracies and fostering awareness of the threats posed by criminal and terrorist elements in the supply chain.

8.1 Corporate Security Policies

Companies are encouraged to enhance border security by establishing threat awareness programs to ensure that security threats, such as contraband, human smuggling and terrorism, are recognized at each point in the supply chain.

Provide details:

8.2 Security Awareness

Employees must be made aware of the procedures the company has in place to address security situations and how to report them. Programs should encourage active employee participation in security controls. Records should be maintained of attendance at security meetings.

Provide details:

8.3 Security Policy Manual

Companies should develop and maintain a security policy manual that contains detailed guidelines of efforts to secure cargo within their control.

Provide details:



9. Business Partner Requirements

When a company contracts out elements of its international supply chain, it is vital that the company works with its business partners to ensure that sound security measures are in place and adhered to in order to achieve an effective secure supply chain globally.

Business partners that are not eligible for PIP must be subject to a verification of their compliance with PIP security criteria by the company through a documented risk-assessment process.

9.1 Selection Criteria

Companies must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers, vendors and carriers.

Provide details:

9.2 Satisfying the Business Partner Security Requirements

International supply chain business partners must demonstrate that they are meeting company supply chain security obligations. Businesses that are not eligible for PIP can demonstrate that they are meeting these security criteria in a number of ways:

- through written or electronic confirmation;
- through contractual obligations;
- through a letter from a senior business partner officer attesting to compliance;
- through a written statement demonstrating their compliance with these criteria or another country's supply chain security criteria, e.g. the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) or an equivalent World Customs Organization (WCO)-accredited security program administered by a foreign customs authority (e.g. Authorized Economic Operator); or
- by providing a completed supply chain security profile.

Provide details:



9.3 Business Partners - Point of Origin

Companies must ensure that business partners develop security procedures consistent with the security criteria in this Profile to enhance the integrity of the shipment at the point of origin. Periodic risk assessments of your business partners' procedures and facilities should be conducted. As well, business partners should maintain your company's security standards.

Provide details:

specimen

9.4 Business Partners - Other Internal Selection Criteria

Using a risk-based approach, the selection of business partners should be based on factors such as financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies as needed.

Provide details:

specimen



10. Supply Chain Security Planning

Policies and procedures should be in place for companies to undertake a risk assessment of their supply chain, identify gaps and weaknesses, and implement strategies to mitigate risks.

specimen

10.1 Determining Risks

Companies should have measures to identify, analyze and mitigate supply chain security risks.

Provide details:

10.2 Compliance with Security Profile

Procedures should be in place to ensure regular reassessments of and compliance with the company's Security Profile.

Provide details:

10.3 Contingency Planning

Contingency plans should be in place to ensure the continuation of trade in the event of an emergency/ security situation. Describe what contingency plans your company has in place.

Provide details:



11. Other Security Measures

11.1 Other Security Measures

Companies may have security measures for the protection of the international supply chain that have not been described in other sections of this Profile.

Provide details:

specimen



12. Highway Carrier

To be eligible for the PIP program, companies must have a valid carrier code issued by the CBSA and be directly involved in the importation or exportation of commercial goods.

12.1 Physical Security and Access Controls

Procedures must be in place to prevent, detect and deter unauthorized access to conveyances, including concealment of unmanifested material and unauthorized personnel in trailers or containers. Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Highway carriers should incorporate physical security criteria throughout their supply chain as applicable.

Provide details:

12.2 Document Review

Personnel should be trained to review manifests and other documents in order to identify or recognize suspicious cargo shipments that:

- originate from or are destined for unusual locations;
- have been paid by cash or certified cheque;
- have unusual routing methods;
- exhibit unusual shipping/receiving practices; or
- provide vague, generalized or poor information.

All instances of suspicious cargo shipments should be reported immediately to the nearest Canadian or U. S. port of entry.

Provide details:



12.3 Bill of Lading/Manifesting Procedures

Bill of lading information filed with the CBSA should show the first foreign location/facility where the highway carrier takes possession of the cargo destined for Canada. Additionally, to help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is timely and reported accurately.

Provide details:

specimen

specimen



Conveyance, Trailer and Container Security

Security must be maintained on all conveyances, containers, trailers and rail cars used in the international transportation of persons and goods. At the point of packing/stuffing, security measures must be in place to properly seal and maintain the integrity of the conveyance, container, trailer or rail car.

12.4 Conveyance Inspection Procedures

Using a checklist, drivers should be trained to inspect their conveyances, trailers, rail cars or containers for natural or hidden compartments. Training in conveyance searches should be adopted as part of companies' on-the-job training program.

Conveyance inspections must be systematic. They should be completed upon entering and departing the truck yard and at the last point of loading prior to reaching the border.

To counter internal conspiracies, a security manager should search the conveyance after the driver has conducted a search. These searches should be random, documented and conducted at the truck yard after the truck has been loaded.

Written procedures must exist to identify specific factors or practices that may deem a shipment from a certain shipper to be of greater risk.

Highway carriers must visually inspect all empty trailers and containers to include the interior of the trailer at the truck yard and at the point of loading. Inspections of the following items are recommended for all conveyances, trailers and containers.

CONVEYANCES:

bumpers/tires/rims
doors/tool compartments
battery box
air breather
fuel tanks
interior cab compartments/sleeper
faring/roof

TRAILERS:

exterior - front/sides
rear - bumper/doors
front wall
left side
right side
floor
ceiling/roof
inside/outside doors
outside/undercarriage
fifth wheel - natural compartment
fifth wheel - skid plate

CONTAINERS:

front wall
left side
right side
floor
ceiling/roof
inside/outside doors
outside/undercarriage

Provide details:

specimen



12.5 Trailer and Container Security

For all trailers in the highway carrier's custody, trailer integrity must be maintained at all times to protect against the introduction of unauthorized material and/or persons. Highway carriers must have related procedures in place.

Even though a carrier may not "exercise control" over the loading of trailers and the contents of cargo, highway carriers must be vigilant in ensuring that merchandise is legitimate and that there is no loading of contraband at the loading dock/manufacturing facility. Highway carriers must ensure that while in transit to the border, no loading of contraband or tampering with cargo has occurred, even at unforeseen vehicle stops.

Trailers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and preventing unauthorized entry into trailers, tractors or storage areas.

Carriers must notify the CBSA of any structural changes such as hidden compartments discovered in trailers, tractors or other rolling-stock equipment that crosses the border.

Provide details:

12.6 Conveyance Tracking and Monitoring Procedures

Highway carriers must ensure that conveyance and trailer integrity is maintained while the conveyance is en route transporting cargo to the border by using a tracking and monitoring activity log or equivalent technology. If driver logs are used, they must reflect that trailer integrity was verified.

Predetermined routes should be identified, and procedures should consist of random route checks as well as the documentation and verification of the length of time between the loading point/trailer pickup, the border and the delivery destination during peak and non-peak times. Drivers should notify the dispatcher of any route delays due to weather, traffic and/or rerouting.

Highway carrier management must perform a documented, periodic and unannounced verification process to ensure that the logs are maintained and conveyance tracking and monitoring procedures are being followed and enforced.

During Ministry of Transportation inspections or other physical inspections on the conveyance as required by state, local or federal law, drivers must report and document any anomalies or unusual structural modifications found on the conveyance.

Provide details:



12.7 Trailer Seals

The sealing of trailers to ensure continuous seal integrity is a crucial element in a secure supply chain, and remains a critical part of a carrier's commitment to PIP. A high-security seal that meets or exceeds the current ISO/PAS 17712 standard must be affixed to all loaded trailers bound for the border. Based on risk, a high-security barrier bolt seal must be applied to the door handle and/or a cable seal must be applied to the two vertical bars on the trailer doors.

Clearly defined written procedures must stipulate how seals in the highway carrier's possession are to be controlled during transit. These written procedures should be briefed to all drivers, and there should be a mechanism to ensure that these procedures are understood and are being followed.

These procedures must include the following:

- a verification must be done to ensure that the seal is intact, and determine if it exhibits evidence of tampering along the route;
- the original seal number must be documented properly;
- a verification of the seal number and location of the seal must be done to ensure that it is the same as stated by the shipper on the shipping documents;
- if the seal is removed in-transit to the border, even by government officials, a second seal must be placed on the trailer, and the seal change must be documented;
- the driver must immediately notify the dispatcher when a seal is broken and whether a second seal has been affixed; and
- the carrier must immediately notify the shipper, the customs broker and the importer of the placement of the second seal.

Provide details:

specimen



12.8 Less Than Truck Load (LTL)

LTL carriers must use a high-security padlock or a similar appropriate locking device when picking up local freight in an international LTL environment. LTL carriers must ensure that strict controls are in place to limit access to keys or combinations that can open these padlocks.

After the freight from the pickup and delivery run is sorted, consolidated and loaded onto a line haul carrier destined to cross the border, the trailer must be sealed with a high-security seal that meets or exceeds the current ISO/PAS 17712 standard for high-security seals.

In LTL or pickup and delivery operations that do not use consolidation hubs to sort or consolidate freight prior to crossing the border, the highway carrier must use ISO high-security seals for the trailer at each stop and to cross the border.

Written procedures must be established to record the change in seals, as well as stipulate how the seals are controlled and distributed, and how discrepancies are noted and reported.

In both the LTL and non-LTL environments, procedures should also exist for recognizing and reporting compromised seals and/or trailers to the CBSA or other appropriate foreign authorities.

Provide details:

specimen



Business Partner Requirements

Highway carriers must have written and verifiable processes for the screening of business partners, including the carriers' agents, subcontracted highway carriers and service providers. It is vital that carriers work with their business partners to ensure that sound security measures are in place and are adhered to in order to achieve an effective secure supply chain globally.

12.9 Security Procedures

Written procedures for screening business partners must exist that identify specific factors or practices, the presence of which would trigger additional scrutiny by the highway carrier, including a detailed physical inspection of the customer's cargo trailer or container.

A record should be maintained of business partners who are PIP-certified.

Non-PIP business partners should be subject to additional scrutiny by highway carriers.

Highway carriers should ensure that contract service providers commit to PIP security criteria through contractual agreements. For international shipments, PIP highway carriers that subcontract transportation services to other highway carriers must use other PIP-approved highway carriers or carriers under the direct control of the PIP carrier through a written contract.

Current or prospective business partners who have obtained certification in a supply chain security program administered by a foreign customs administration should be required to indicate their status of participation to the highway carrier.

As highway carriers have ultimate responsibility for all cargo loaded aboard their conveyance or trailer, they must communicate the importance of supply chain security and maintaining the chain of custody as fundamental aspects of their company security policy.

Provide details:

specimen



13. Customs Broker

Customs brokers play an important part in the international trade supply chain. To reduce the security vulnerabilities associated with imported and exported goods, customs brokers must take appropriate measures to ensure that their part of the chain is secure.

specimen

13.1 Screening and Selection Criteria/Service Providers

Customs brokers should have written and verifiable procedures for the selection of contracted service providers in order to check their validity, financial soundness, ability to meet contractual security requirements and ability to identify and correct security deficiencies as needed. Procedures should use a risk-based approach.

Provide details:

13.2 Customer Screening Procedures

Customs brokers should have documented, risk-based procedures to screen prospective customers in order to check their validity, financial soundness, ability to meet contractual security requirements and ability to identify and correct security deficiencies as needed.

Provide details:

specimen



14. Courier

14.1 Cargo Reconciliation

Arriving express shipments must be reconciled against information on the express cargo manifest. Measures must be in place to detect and report cargo shortages and overages. Express shipments should be accurately described and their weights, labels, marks and piece counts indicated and verified.

Provide details:

14.2 Express Cargo Documentation Processing

Procedures must be in place to ensure that all information used in the clearing of express cargo is legible, complete, accurate and protected against the exchange or introduction of erroneous information. To help ensure the integrity of express cargo received from abroad, procedures must be in place to ensure that the information received from business partners is timely and reported accurately.

Provide details:

14.3 Container Inspection (if applicable)

Procedures must be in place to verify the physical integrity of the container structure prior to stuffing/packing, including the reliability of the locking mechanisms of the doors. A seven-point inspection is recommended for all containers:

left side	front wall	inside/outside doors	ceiling/roof
right side	floor	outside/undercarriage	

Provide details:



14.4 Trailer Inspections

Procedures must be in place to visually inspect all empty trailers, including the interior of the trailer at the truck yard and at the point of loading, if possible. Inspections of the following items are recommended for all trailers:

- | | | |
|------------|----------------------|---|
| left side | floor | exterior - front/sides |
| right side | ceiling/roof | rear - bumper/doors |
| front wall | inside/outside doors | outside/undercarriage |
| | | fifth wheel area/natural compartment/skid plate |

Provide details:

Conveyance Security

Conveyance integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material.

14.5 Conveyance Inspection Procedures

Using a checklist, drivers should be trained to inspect their international conveyances, e.g. trailers and tractors, for natural or hidden compartments. Training in conveyance searches should be adopted as part of the couriers' on-the-job training program.

Conveyance inspections must be systematic and should be completed upon entering and departing from the truck yard, as well as at the last point of loading prior to reaching the border.

To counter internal conspiracies, a security manager, held accountable to senior management for security, should search the conveyance after the driver has conducted a search. These searches should be random, documented and conducted at the truck yard and after the truck has been loaded and is en route to the border.

Inspections of the following items are recommended for all tractors:

- | | | | |
|--------------|-------------|-------------------------|-----------------------------------|
| battery box | fuel tanks | bumpers/tires/rims | interior cab compartments/sleeper |
| air breather | faring/roof | doors/tool compartments | |

Provide details:



14.6 Determining Risks

Courriers should have measures to identify, analyze and mitigate supply chain security risks. Written procedures must exist that identify specific factors or practices that may deem a shipment from a certain shipper of greater risk.

Provide details:

specimen

specimen



15. Marine Carrier

Marine carriers must conduct a comprehensive assessment of their security practices based upon the following PIP minimum security criteria. When a marine carrier does not control a specific element of the cargo transportation service it has contracted to provide, such as a marine facility, port operator or time-chartered vessel, the marine carrier must work with these business partners to ensure that pertinent security measures are in place and adhered to. The marine carrier is responsible for all cargo loaded on-board its vessel, pursuant to applicable laws and regulations and the terms of the PIP program.

PIP recognizes that many marine carriers are already subject to defined security mandates created under International Codes and Transport Canada legislation. It is not the intention of PIP to duplicate existing vessel and facility security requirements. Rather, PIP seeks to build upon Transport Canada requirements, and the CBSA may require additional security measures and practices that enhance overall security throughout the international supply chain.

Compliance with Transport Canada's Marine Transportation Security Regulations (MTSR) is a prerequisite for PIP marine carrier membership. PIP members may only use vessels in compliance with MTSR. Marine facilities and ports operated by PIP members must also comply with MTSR. The Physical Access Controls and Physical Security provisions in this Profile are satisfied by regulated vessels and port facilities holding a certificate of compliance issued by a flag state or Transport Canada.

Physical Security and Access Controls

Marine carriers shall establish access controls to prevent unauthorized entry into their vessels and cargo facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, government officials and vendors at all controlled access points of entry and again at the boundaries of all restricted areas. Shore employees and service providers should only have access to those areas of the vessel where they have legitimate business. Transport Canada's MTSR govern vessel and facility access controls. The Physical Access Controls provisions of this Profile are satisfied for MTSR-regulated vessels and port facilities certified compliant with Transport Canada's regulations.

Non-MTSR-regulated cargo handling and storage facilities and container yards operated by marine carriers in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access. Marine carriers should adhere to the following physical security criteria as applicable.

15.1 Lighting

While at port, the pier and waterside of the vessel must be adequately illuminated.

Provide details:



15.2 Alarm Systems and Video Surveillance

At the locations determined appropriate by the marine carrier's risk assessment, alarm systems and video surveillance should be used to monitor premises and prevent unauthorized access to vessels and cargo handling and storage areas. Signage indicating the use of surveillance equipment should be posted around the facilities.

Provide details:

specimen

15.3 Boarding and Disembarking Vessels

Consistent with the vessel's security plan, all crew, employees, vendors and visitors may be subject to a search when boarding or disembarking vessels. A vessel visitor log must be maintained and a temporary visitor pass must be issued as required by the vessel's security plan. All crew, employees, vendors and visitors, including government officials, must display proper identification as required by the applicable security plan.

Provide details:

specimen



Procedural Security

Consistent with the marine carrier's security plan, procedures must be in place to prevent unauthorized personnel from gaining access to the vessel. In those geographic areas where risk assessments warrant checking containers for human concealment, such procedures should be designed to address the particular identified risk at the load port or the particular port facility. The CBSA will inform marine carriers when it is aware of a high risk of human concealment or stowaways at particular ports or geographic regions. Documented procedures must also include pre-departure vessel security sweeps for stowaways while at the foreign load port, and during normal watch activity while en route to Canada as warranted by risk conditions at the foreign load port.

15.4 Passenger and Crew

Marine carriers must ensure that they comply with Canadian notice of arrival and departure requirements so that accurate, timely and advance transmission of data associated with international passengers and crew is provided to the Canadian government and the CBSA.

Provide details:

15.5 Bill of Lading/Manifest Procedures

Procedures must be in place to ensure that the information in the marine carrier's cargo manifest accurately reflects the information provided to the carrier by the shipper or its agent.

All shortages, overages and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. The CBSA and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected. Bill of lading information should show the first foreign port where the marine carrier takes possession of the cargo destined for Canada.

Provide details:



Container Security

Security must be maintained for all containers in the marine carrier's custody to protect them against the introduction of unauthorized material and/or persons. A high-security seal must be affixed to all loaded containers bound for Canada. All seals used or distributed by the marine carrier must meet or exceed the current ISO standards for high-security seals.

15.6 Container Inspection

Marine carriers must visually inspect all empty containers bound for Canada, including the interior of the containers at the foreign port of lading.

Provide details:

15.7 Container Seals

Written procedures must stipulate how seals in the marine carrier's possession are to be controlled. Procedures should exist for recognizing and reporting, as appropriate, compromised seals and/or containers to the CBSA or other appropriate foreign authorities. Only designated employees should distribute container seals for integrity purposes.

Provide details:

15.8 Deserter/Absconder Notifications

Vessel masters must account for all crew prior to the vessel's departure from a Canadian port. If the vessel master discovers that a crew member has deserted or absconded, the vessel master must report this using the most practical means to the CBSA immediately upon discovery and prior to the vessel's departure.

Provide details:



Business Partner Requirements

Marine carriers must have written and verifiable procedures for the screening of the carriers' agents and service providers contracted to provide transportation services for the carriers.

15.9 Selection Criteria

Marine carriers must have screening procedures for new customers beyond financial soundness issues, including indicators of whether the customer appears to be a legitimate business and/or poses a security risk.

Marine carriers must have written or Web-based procedures for screening new customers to whom they issue bills of lading. These procedures must identify specific factors or practices, the presence of which would trigger additional scrutiny by the marine carrier, including a detailed physical inspection of the exterior of the customer's container prior to loading onto the vessel. These procedures may also include a referral to the CBSA or other competent authorities for further review. The CBSA works in partnership with marine carriers to identify specific information regarding what factors, practices or risks are relevant.

Marine carriers should ensure that contracted vessel service providers comply with PIP security criteria. Periodic reviews of service provider security should be conducted.

Provide details:

15.10 Business Partners/Point of Loading

Marine carriers must have procedures to review their customers' requests that could affect the safety of the vessel or cargo, or otherwise raise significant security questions. These may include unusual customer demands, such as specific stowage placement aboard the vessel (beyond a request for below-deck or on-deck stowage).

Provide details:



16. Air Carrier

16.1 Air Cargo Facilities

Cargo handling and storage facilities in domestic and foreign locations must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained through periodic inspection and repair. All external doors, windows, gates and fences must be secured with locking devices. Air cargo handling and storage facilities must have physical barriers and/or deterrents that guard against unauthorized access.

Provide details:

16.2 Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of air cargo and baggage in the secure supply chain. Security must be maintained for all cargo and baggage while in the possession or control of the air carrier. Procedures must be in place to ensure that all checked baggage has an accompanying passenger checked onto the aircraft. Control must be maintained of all baggage from the time of check-in to the aircraft to the time of transfer from the aircraft to the customs baggage area.

Provide details:

specimen



17. Rail Carrier

17.1 Privately Owned Vehicles

Privately owned vehicles should be monitored if parked in close proximity to rolling stock that crosses the international border.

Provide details:

specimen

17.2 Physical Access Controls

To the extent practical, rail carriers should institute access controls to prevent unauthorized entry to rail property and rail cars, and should maintain control of employees and visitors. Access controls must include the positive identification of employees, visitors, service providers and vendors. Rail companies should also conduct spot inspections of motor vehicles on railroad property where international shipments are handled.

Provide details:

17.3 Employees

Employees should only be given access to high-security areas such as dispatch centres if necessary for the performance of their duties.

Railroad supervisors and railroad police must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys and key cards) must be documented. Employee identification measures must be established for all employees. Identification spot checks must be conducted as threat conditions warrant.

Provide details:



17.4 Unauthorized Persons

Measures must be implemented to deter unauthorized entry and increase the probability of detection at company-designated critical infrastructure. Safety and security training must be provided for employees at facilities where international shipments are handled.

Procedures must be established to detect unmanifested material and unauthorized personnel, and deter them from being introduced onto trains crossing the border.

The need for employees to immediately report to the proper authorities all suspicious persons, activities or objects encountered must be reinforced.

Proactive community safety and security outreach and trespasser abatement programs must be focused on areas adjacent to company-designated critical infrastructure to reduce the likelihood of unauthorized individuals entering company property and to enhance public awareness of the importance of reporting suspicious activity.

Provide details:

17.5 Rail Car Seals

The sealing of rail cars and intermodal maritime containers, along with continuous seal integrity, are crucial elements in a secure supply chain, and remain critical aspects of a rail carrier's commitment to PIP. To the extent practical, a high-security seal should be affixed to all loaded rail cars destined for export. Seals must meet or exceed the standards for high-security seals (ISO/PAS 17712). Rail cars crossing the border must also fully comply with seal verification rules and seal anomaly reporting requirements.

Clearly defined written procedures must stipulate how seals in the rail carrier's possession are to be controlled during transit. These written procedures should be briefed to all rail crew, and there should be a mechanism to ensure that these procedures are understood and are being followed.

Provide details:



Rolling Stock

Security must be maintained on all rail cars used to import or export goods to protect them against the introduction of unauthorized material and/or persons. At the point of stuffing/packing, procedures must be in place to properly seal and maintain the integrity of shipping containers, trailers and rail cars. Even though rail carriers may not exercise control over the loading of rail cars and the contents of cargo, they must be vigilant in preventing stowaways and the smuggling of contraband.

Rail carriers should maintain open dialogue with the CBSA on areas of common concern to collectively benefit from advancements in industry standards and rail security technologies.

17.6 Rolling Stock Security

Rail carriers shall have procedures in place to protect against the introduction of unauthorized personnel and material.

Rail carriers shall have procedures in place to protect against the loading of contraband while trains are in transit to the border, even during unforeseen train stops.

Rail carriers must have procedures in place for reporting unauthorized entry into rail cars and locomotives.

Rail carriers must maintain inventory information and movement records on each rail car and use the physical rail car tracking technology that is inherent to the North American rail network system.

Provide details:

17.7 Inspection Procedures

Rail personnel should be trained to inspect their rail cars and locomotives for anomalies. Training in conveyance searches should be adopted as part of the carrier's on-the-job training program. Training should be recorded in attending employees' personnel files.

A systematic inspection must be made prior to reaching the border.

During required safety inspections of rolling stock, security inspections must be conducted to find any apparent signs of tampering, sabotage, attached explosives, contraband, stowaways and other unusual or prohibited items.

Provide details:



Business Partner Requirements

Rail carriers must have written and verifiable procedures for the screening of new business partners, including the carriers' agents, subcontracted rail carriers and service providers. As well, screening procedures must be in place for new customers beyond financial soundness issues, including security indicators. Rail carriers should strongly encourage their contracted service providers and shippers to comply with PIP security criteria. These procedures apply to business partners and service providers not eligible for PIP membership.

17.8 Security Measures

Written procedures must exist to address specific factors or practices, the presence of which would trigger additional scrutiny by the rail carrier.

Business partners who are not PIP members may be subject to additional scrutiny by the rail carrier. Rail carriers should institute appropriate security procedures for their contracted service providers.

Provide details:

specimen