



Memorandum D23-1-1

Ottawa, December 18, 2020

Partners in Protection Program

In Brief

This memorandum outlines and explains the policies and membership requirements of the Partners in Protection (PIP) program. PIP is a voluntary Canada Border Services Agency (CBSA) program that enlists the cooperation of private industry to enhance border and trade chain security while providing pre-approved, low-risk businesses with streamlined and efficient border processes.

Legislation

[Customs Act](#) – sections 11, 12, and 13

Guidelines and General Information

Definitions

Action plan – Issued by the CBSA to a PIP applicant or member, the action plan outlines necessary corrective action and a reasonable time frame for completion in order to comply with PIP MSRs. If the action plan is acted upon accordingly, a PIP applicant can avoid being denied program membership or a PIP program member can avoid suspension or cancellation of their program membership.

Articles of incorporation – A legal document creating a corporation and outlining its purpose and regulations in order to be deemed ‘incorporated.’ In Canada, this document is filed with a provincial, territorial, or federal government by the founders of a corporation. In the United States, it is filed with a state and is governed by the laws of that state.

Authorized Economic Operator (AEO) – A party involved in the international movement of goods in a function approved by (or on behalf of) a national customs administration as complying with WCO or equivalent supply chain security requirements as outlined in the SAFE Framework. Term also used to describe national customs administration’s commercial trade programs that align with the SAFE Framework.

Authorized officer – An authorized officer is an individual with legal signing authority who acts in an official capacity to represent a business and make decisions on behalf of that business. Examples may include Chief Executive Officer (CEO), Chief Financial Officer (CFO), President, Vice-President, Owner, Partner, Secretary Treasurer, Executive Director, Director, or other authorized individual. This individual will become the TTP account owner with responsibility for accepting the Terms and Conditions of PIP program membership, completing the Certification and Authorization to Disclose Information (CADI), and receiving notifications related to the PIP application or membership status of the business. For the purposes of administering

membership in the PIP program, the CBSA may request documented proof of the individual's authorized status.

Awareness session – An information presentation given by a CBSA officer to promote awareness of security related issues among PIP members.

Bill of Lading (or Manifest) – A document issued by a shipper to a carrier containing the terms of the contract for cartage and a list of all goods to be shipped. The shipper is responsible for completing the bill of lading and providing it to the carrier when the shipment is sent. The carrier, in turn, is responsible for providing a copy to the importer as evidence of the transfer of goods and acknowledgment of their receipt.

Border services officer – Officers who were formerly designated as customs officers, immigration officers and food inspection officers.

Business – A corporation or sole proprietorship.

Business Number (BN) – A 15-character alphanumeric identifier assigned by the Canada Revenue Agency (CRA) to identify a business. It consists of a nine-digit registration number and six-character account identifier (e.g., 123456789RM0002: the registration number 123456789 identifies the legal entity and the account identifier RM0002 identifies a division or branch of the legal entity).

Carrier code – A unique four-character identifier issued by the CBSA to identify a specific carrier.

Certification and Authorization to Disclose Information (CADI) – A form allowing PIP members to authorize the exchange of program-related information between the CBSA and other customs organization(s) under an established MRA.

Commercial goods – Goods imported into Canada for sale or for any commercial, industrial, occupational, institutional, or other similar use.

Courier Low Value Shipment (CLVS) Program – A commercial program intended to help simplify the process to import low value goods. The program streamlines the customs processing of shipments valued at CAN\$2,500.00 or less and provides the courier industry with expedited release.

Customs-Trade Partnership Against Terrorism (C-TPAT) – A voluntary supply chain security program led by U.S. Customs and Border Protection (CBP) and focuses on improving the security of private business' supply chains.

Customs and Border Protection (CBP) – A federal law enforcement agency of the United States Department of Homeland Security charged with regulating and facilitating international trade, collecting import duties, and enforcing U.S. regulations, including trade, customs, and immigration.

Customs Self-Assessment (CSA) – A pre-approval commercial program that simplifies border requirements to give approved importers, approved carriers, and registered drivers the benefits of a streamlined clearance option for CSA eligible goods.

Dunnage – Any materials used to secure, support, and/or transport cargo while in transit, including wooden pallets, racks, straps, bags, packaging, etc.

Facility – Any location at which a member conducts business operations in relation to the cross-border movement of commercial goods, including locations where cargo is handled and/or stored. A list of all facilities must be provided in the security profile.

Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework) – The Framework of Standards to Secure and Facilitate Global Trade is a regime developed by the WCO to enhance the security and facilitation of international trade. It sets forth principles and standards and presents them for adoption as a minimal threshold by WCO members.

Free and Secure Trade (FAST) – A joint Canada-U.S. initiative that provides an accelerated commercial clearance option to pre-approved importers, carriers, and registered drivers to move pre-approved eligible goods across the border.

Freight forwarder code – A unique four-character identifier issued by the CBSA to identify a specific freight forwarder.

GCKey – This is a unique username and password of your choosing that protects your online communications with the Government of Canada. This is the recommended credential for the TTP. This allows the Government of Canada to authenticate your identity. Credentials provide you with safe and secure access to information and services. All individuals, even if they are from the same business, will require their own credential to access the TTP.

High-security Seal – For PIP purposes, high-security mechanical freight container seals are categorized as seals that meet or exceed the current ISO/PAS 17712 standard for freight container mechanical seals. Seals that conform or exceed this standard are manufactured with strong metal materials with the intent to delay intrusion, and the seals generally require removal with bolt or cable cutters. Seals are categorized into the following security levels: indicative (I), security (S), or high-security (H). Businesses must agree to use seals that meet the “H” (high security) level for PIP purposes.

ISO/PAS 17712 – International Organization for Standardization / Publicly Available Specification 17712 defines the various types of security seals available and describes in detail the general performance requirements for each product type as well as details of testing specifics.

Legal entity – An association, corporation, partnership, proprietorship, trust, or individual that has legal standing in the eyes of law. A legal entity has legal capacity to enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued in its own right, and to be held responsible for its actions.

Letter of Authorization – A letter provided by the applicant/member business to the CBSA authorizing a third party representative to provide information to the CBSA on behalf of the business. The business maintains full liability for all information provided to the CBSA by their representative.

LTL/LCL – Less-than-truck-load (LTL) and less-than-container-load (LCL) are terms used when a quantity of freight does not fill a standard truck or container and/or more than one shipper’s freight or consignment occupies a single container. This often applies to businesses doing pick-up and delivery operations wherein cargo is added to an existing load en route.

Minimum Security Requirements (MSR) – A set of security requirements, covering all components of a business’ supply chain, that must be met in order to be recognized as a PIP member. They are outlined in the PIP security profile.

Mutual Recognition Arrangement (MRA) – An arrangement that expands the international trade network of accredited low-risk businesses. An MRA between the CBSA and compatible national customs agencies means that both country’s customs-trade partnership programs apply similar security standards and site validation practices when approving businesses for membership in their respective programs, and both countries recognize each other’s members and may grant them similar benefits.

Partners in Protection (PIP) – A cooperative program between private industry and the CBSA aimed at enhancing border and trade chain security.

Post-Incident Analysis (PIA) – The activities undertaken with a member following a breach of supply chain security. The PIA will investigate the incident, identify any mitigating circumstances, and formulate a strategy for the prevention of future incidents.

Risk assessment – A screening process which verifies a business’ eligibility for PIP membership, identifies potential vulnerabilities, and evaluates an acceptable level of risk.

SAFE Framework – See Framework of Standards to Secure and Facilitate Global Trade. **Seal**

– See High-security Seal

Security profile – The fundamental document of the PIP program in which applicants or members provide tombstone information and details on their business operations, including supply chain partners, cargo handling

facilities and procedures, security practices, physical access controls, sealing protocols, information technology infrastructure, etc.

Site Validation – A physical inspection of an applicant’s or member’s premises to verify the information provided in the security profile.

Supply chain partner – A third-party facility involved in a member’s business operations in relation to the crossborder movement of commercial goods, such as domestic or foreign suppliers, manufacturers, distribution centres, conveyances, warehouses, truck yards, and cargo handling/storage areas.

Terms and Conditions – A voluntary agreement between a PIP program member and the CBSA to enhance the security of the member’s supply chain and to certify their participation in the PIP program.

Tombstone information – Basic applicant or member identifying information, including the business’ names), divisions), points) of contact, location addresses), telephone numbers), e-mail addresses), business numbers), carrier codes), etc.

Trusted Trader Portal (TTP) – A secure online tool that allows members of the trade community to complete and submit applications for membership in the Partners in Protection (PIP) program, as well as maintain their membership documentation online.

World Customs Organization (WCO) – An organization whose primary purpose is to facilitate the development of international trade through the improvement and harmonization of customs procedures.

General Information

1. The PIP program is designed to establish partnerships with trusted businesses in order to enhance the integrity of Canada’s borders and the security of the international supply chain.
2. PIP program members agree to implement and adhere to high security standards, while the CBSA agrees to support program members through the assessment of their physical and procedural security measures. Members are recognized as being Trusted Traders and enjoy benefits such as border recognition, facilitated processing, enhanced industry marketability, awareness sessions on security issues, and access to the Trusted Trader Portal (TTP), while the CBSA is able to focus its resources on areas of higher or unknown risk.
3. In addition, businesses that hold membership in both PIP and the CBSA’s other Trusted Trader program, Customs Self-Assessment (CSA), may use the Free and Secure Trade (FAST) lanes into Canada or the United States (U.S.), providing access to the accelerated border clearance process. Under FAST, eligible goods (including empty conveyances) arriving for PIP and CSA approved members, and transported by PIP and CSA approved carriers using Commercial Driver Registration Program (CDRP) or FAST registered drivers, are cleared into Canada or the U.S. through dedicated lanes/booths, resulting in both time and cost savings.
4. The PIP program is an Authorized Economic Operator (AEO) program, which means it is aligned with the World Customs Organization’s (WCO) Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework). The SAFE Framework establishes universal standards for supply chain security that have been adopted by customs organizations worldwide.
5. Based on the SAFE Framework, the PIP program specifies a set of Minimum Security Requirements (MSRs) that must be met in order to be recognized as a PIP program member. The MSRs are outlined in the PIP security profile, a program application document. The MSRs cover all components of a business’ supply chain, including the following categories:
 - (a) Physical security and access controls;
 - (b) Procedural security;
 - (c) Container, trailer, and rail car security;
 - (d) Data and document security;
 - (e) Personnel security;

- (f) Security training and awareness;
 - (g) Business partner requirements; and (h) Supply chain security planning.
6. In addition to the requirements outlined in the MSRs, the PIP security profile includes recommendations which are suggested best practices for businesses to further enhance their security practices. Some examples of recommendations include:
- (a) Security awareness program for employees;
 - (b) Code of conduct regarding security violations;
 - (c) Security policy manual;
 - (d) Monitoring business partners to ensure conformity with PIP MSRs;
 - (e) Electronic-security, including protection of electronic assets and information technology (IT) infrastructure.
7. The CBSA continues to reserve the right to examine any shipment or conveyance that crosses the border into Canada, regardless of program membership. The CBSA may refer a PIP program member's shipment for verification activities such as:
- (a) Documentation review;
 - (b) Contraband inspection;
 - (c) Cab check; or
 - (d) Random examination. **Privacy Statement**
8. The information collected in the PIP program application and supporting documents is done so under the authorities of sections 11, 12, and 13 of the [Customs Act](#) for the purposes of administering or enforcing the PIP Program. The information will be used to determine the eligibility of an applicant and to conduct compliance reviews (e.g. to ensure that members continue to adhere to program requirements) and may be disclosed internally for the purposes of investigation and enforcement activities relating to program applicants and members. The information may also be used for statistical purposes, to plan awareness sessions and to evaluate the program. Disclosure of the information collected in the PIP program application and supporting documents is governed by section 107 of the *Customs Act*.

PIP Program Membership

Eligibility Criteria

9. To be eligible for membership in the PIP program, an applicant must:
- (a) own or operate facilities based in Canada or the U.S. that are involved in the cross-border movement of commercial goods;
 - (b) have been in existence for a period of no less than one calendar year and, in the case of importers and carriers, have imported or transported commercial goods to or from Canada at least once prior to the 90 days before the day on which the application was received;
 - (c) be solvent and have no unresolved debts to the Crown or undischarged bankruptcy;
 - (d) have a good record of compliance with the CBSA and Other Government Departments (OGDs); (e) have no convictions (for which a record suspension has not been received) under the [Criminal Code](#) of Canada or under any other federal or provincial legislation;
 - (f) have no convictions outside of Canada under foreign law that, if enforced in Canada, would constitute an offence under an Act of Parliament or under any other federal or provincial legislation;

- (g) have no history of significant contraventions under the [Customs Act](#) or any of its regulations, or under any act or regulation enforced by the CBSA or other international customs organization; and
- (h) be compliant with all MSRs outlined in the PIP security profile unless special consideration is given to the business' particular operations or security structure at the discretion of the CBSA.

10. For businesses based in Canada, membership in the PIP program is available to the following lines of business:

- (a) **Commercial carriers operating in the highway, rail, marine and/or air modes, including couriers** — defined as an individual or business with a valid carrier code issued by the CBSA that undertakes, in a contract of carriage, to transport commercial goods by highway, rail, sea, or air, or by a combination of these modes.

Notes:

For further information on carrier codes please refer to [Memorandum D3-1-1](#) and/or [contact the CBSA's Commercial Registration Unit \(CRU\)](#).

Couriers wishing to participate in the CBSA's Courier Low Value Shipment (CLVS) Program must be PIP-approved carriers. CLVS Program shipments must also be imported and transported by PIP-approved carriers. When applying to the PIP program, couriers must identify themselves as a carrier in the mode of transport that best describes their operations. For further information on the CBSA's CLVS Program please refer to [Memorandum D17-4-0](#).

- (b) **Importer or exporter** — defined as an individual or business with a valid Business Number (BN) that brings commercial goods from a source outside of Canada into a domestic market, or vice versa, in the course of trade.
- (c) **Warehouse operator (including marine terminal operator)** — defined as an individual or business with a valid Business Number (BN) that charges a fee for the receipt, storage, and handling (or other value-added service) of goods belonging to others. **Note:** For further information on business numbers please refer to the [Canada Revenue Agency](#) website.
- (d) **Freight forwarder** — defined as an individual or business with a valid (bonded or non-bonded) freight forwarder code issued by the CBSA that arranges for the transportation of goods, and may provide other services such as consolidation and deconsolidation of shipments and de-stuffing containers. **Note:** For further information on freight forwarder codes please refer to [Memorandum D3-1-1](#) and/or [contact the CBSA's CRU](#).
- (e) **Shipping agent** — defined as an individual or firm that transacts all business in a port on behalf of ship owners or charterers.
- (f) **Customs broker** — defined as an individual or business licensed to carry out customs-related responsibilities on behalf of a client. **Note:** For further information on the CBSA's broker licensing requirements please refer to [Memorandum D1-8-1](#).

11. For businesses based in the U.S., membership in the PIP program is available to carriers in all modes of transport, provided that they hold a valid Canadian carrier code, and to importers that conduct business in Canada (i.e., hold a valid Canadian business number and file Canadian customs declarations). **Note:** PIP membership remains mandatory for U.S.-based highway carriers wishing to access FAST lanes when entering Canada.

Application Process

- 12. There is no fee for applying to the PIP program. Applications may be [submitted electronically through the TTP](#). **Note:** A Business Number (BN), CC or FFC is required in order to access the TTP.
- 13. In order to apply for PIP membership, a business' authorized officer (see "Definitions" for details) must: (a) visit the TTP to request an activation code, obtain an online credential, such as a GCKey, and register for a

TTP account. **Note:** TTP activation codes will be only be sent through a secure method where the identity of the recipient can be verified;

- (b) submit a completed security profile;
 - (c) accept the Terms and Conditions of PIP program membership;
 - (d) fill out the Certification and Authorization to Disclose Information (CADI) form; and
 - (e) provide the Articles of Incorporation (in the case of a corporation) or first page of Minute Book (in the case of a U.S. resident), including the certificate number, date of issue, and number of years in existence. In the case of a sole proprietorship, the following must be provided: criminal record check, credit check, and proof of operating as a business for a period of no less than one calendar year.
14. The PIP program's Terms and Conditions set out the respective roles and responsibilities of the CBSA and the applicant to enhance the physical security and integrity of the production, transportation, importation, and/or exportation processes involved in the supply chain. Acceptance of the Terms and Conditions serves to formalize the business' commitment to uphold these roles and responsibilities upon approval of PIP membership.
 15. The Terms and Conditions represent administrative understandings between the CBSA and PIP members that are not intended to be legally binding or enforceable before the courts. Nothing in the Terms and Conditions is intended to create a relationship of agency, financial partnership, employer-employee, or joint enterprise between the CBSA and PIP members.
 16. The CADI is a form through which businesses may authorize the exchange of program-related information with other AEO programs through the CBSA's established Mutual Recognition Arrangements (MRAs). This means both countries can recognize each other's members and may grant them similar benefits. Businesses may modify the CADI at any time to extend or revoke information sharing permissions.
 17. The processing of a PIP application consists of the two distinct stages:
 - (a) **preliminary review** of the information submitted to confirm eligibility and ensure completeness; and (b) **validation** of the accuracy of the information submitted through the conduct of site visits. This confirms compliance with program MSRs and includes risk assessment and the identification of potential vulnerabilities.
 18. A request for additional or revised information will be sent to the applicant if any errors or omissions are identified at any stage in the application process. Failure to respond to such a request within the specified timeframe may result in denial of the application.
 19. Upon final approval of membership in the PIP program, an official certification letter will be sent to the member.
 20. Once accepted into the PIP program, members must confirm their continued participation, and verify their security profile information, on an annual basis. This may be done by [logging on to the TTP](#). In addition, members are responsible for providing updates through the TTP regarding any changes to their business' information, as they occur, including changes to their supply chain, business structure, security practices, location(s) of operations, or contact information. This may also be done through the TTP.
 21. In accordance with the PIP program's Terms and Conditions, members must submit up-to-date security profile information and inform the CBSA of any substantive business changes, including security-related incidents or breaches, and any modifications to facilities or processes that may affect conformity with MSRs.
 22. If a PIP applicant or member changes the location of its operations and/or acquires a subsidiary facility, they must immediately notify the CBSA of the change and update the security profile accordingly. Depending on the nature and magnitude of the change, the CBSA will determine whether the conduct of an additional site visit is required on a case-by-case basis. **Site Validations**
 23. Applicants to the PIP program must undergo a site validation to verify that the information provided in the security profile accurately reflects their supply chain. A CBSA officer will conduct an on-site inspection of the

business' facilities to assess compliance with PIP MSRs. Businesses must respond within the specified timeframe to all validation requests made by the CBSA.

24. Should the business decide to hire a third party to represent them at site validations, and/or in any other interactions with the CBSA, they must provide the CBSA with a Third Party Authorization letter signed by an authorized officer (see "Definitions" for details) of the business. The letter of authorization should be printed on the business' letterhead and should follow the suggested format outlined in the Appendix of this memorandum. The business maintains full liability for all information provided to the CBSA by their representative.
25. If the business has a complex business structure with multiple lines of business, divisions and/or locations, the CBSA will validate each mode and reserves the right to visit as many facilities as deemed necessary in order to ensure a thorough validation of the business' entire supply chain. At the discretion of the CBSA, a site validation may be extended to include the business' supply chain partner(s).
26. Upon approval of PIP membership, the date of the site visit will become the membership's effective date. It is on this date that the countdown will begin for revalidation of PIP membership.

Site Revalidation

27. PIP program membership requires a renewed site visit no later than every four calendar years for revalidation of membership. For example, a business that became an approved PIP program member in August 2010 will be revalidated by, no later than, the end of 2014. Unless otherwise determined by the CBSA, membership will remain active throughout the revalidation process. Members will be notified when they are due for revalidation.

28. At the discretion of the CBSA, PIP program members are subject to periodic reviews and/or site visits at any time, outside the regular four-year revalidation cycle, in order to ensure compliance with MSRs.

Withdrawal

29. A PIP application or membership may be withdrawn by the applicant at any time. An application or membership that has been withdrawn will not be reinstated and a full reapplication will be required in order to be reconsidered for PIP membership.

Non-transfer of PIP Program Membership

30. Ongoing applications and approved memberships in Trusted Trader programs are not transferrable and cannot be sold, disposed of, or acquired through corporate amalgamation, change of legal entity, or sale of business.

31. PIP applicants or members that undergo any such changes will need to withdraw and reapply under their new corporate structure in order to be considered for continued participation in the PIP program.

PIP Program Membership List

32. As a service to our members, the CBSA publishes a list of approved PIP members on the CBSA website. The businesses listed are those that have consented to have their names posted and therefore may not comprise a complete list of all PIP-approved businesses.

Trusted Trader Program Email List

33. Businesses that are not in the PIP program but are interested in trade chain security may [send an email to PIP](#) with the subject line "Email List Request Form" in order to receive email communications from the CBSA's Trusted Trader Program, including program updates, newsletters, publications, invitations to special events, and other announcements.

34. Businesses that are on the Trusted Trader Program email list are not subject to a risk assessment or compliance with MSRs and their names are not posted on the CBSA website. Those on the list are responsible for keeping their contact information up-to-date and may be removed without notice if it is found to be invalid.

Action Plans

35. If vulnerabilities are identified in a business' supply chain, the CBSA may implement an action plan to outline the corrective measures necessary for compliance with MSRs. An action plan constitutes a mutual agreement between the business and the CBSA.
36. The business must agree to the terms and timeframe specified in the action plan. Failure to abide by the terms of an action plan within the specified timeframe may result in denial of an application or the suspension or cancellation of program membership.
37. At the discretion of the CBSA, a PIP program member may be suspended pending completion of an action plan depending on the nature of the identified security deficiencies.
38. The business will be notified when an action plan is required. Completion of an action plan must occur within 90 calendar days from the date of issuance.
39. If requested, an extension to the action plan timeframe may be granted at the discretion of the CBSA. Extension requests will be reviewed by the CBSA on a case-by-case basis and should not exceed six months.
40. A CBSA officer will follow up with the business upon completion of an action plan to verify that corrective measures have been implemented to the satisfaction of program requirements.

Denial of a PIP Program Application

41. Reasons for denial of a PIP program application may include, but are not limited to:
- (a) submission of false or misleading information;
 - (b) failure to respond to requests for additional or revised information within the specified timeframe; (c) failure to notify the CBSA of changes to the business as they occur, including any changes to the supply chain, business structure, security practices, location(s) of operations, or contact information; (d) failure to meet PIP program eligibility requirements or MSRs;
 - (e) failure to pass a risk assessment or site validation;
 - (f) refusal to undergo a site validation;
 - (g) failure to comply with the requirements of an action plan or to address security deficiencies in a satisfactory manner; and/or
 - (h) a security incident prior to program membership approval, such as an enforcement action at the border, a security breach involving cross-border freight, or an instance of cargo theft.
42. Applicants are required to respond within the specified timeframe to all requests from the CBSA regarding their PIP program status, including requests to confirm or update business or contact information, schedule an onsite validation or post-incident analysis, provide additional details on business or security practices, submit or verify information in the Trusted Trader Portal, etc. Failure to respond to a request from the CBSA may result in denial of an application.
43. A denial decision will be rendered by the CBSA after thorough consideration of the situation.
44. A letter of notification will be sent to the business following a denial decision. The letter will state the reason(s) for denial and will provide an effective date for the CBSA's decision. Denial of a PIP program application is subject to appeal.

Reapplication Following Denial

45. A moratorium on reapplication following a denial decision may be imposed at the discretion of the CBSA depending on the reason(s) for denial. The standard reapplication timeframe relating to application related issues is six months. However, the CBSA reserves the right to specify reapplication timeframes on a case-by-case basis, and to disallow reapplication indefinitely for serious cases.

Suspension or Cancellation of PIP Program Membership

46. Suspension of PIP program membership constitutes an interruption of all program-related benefits, including access to FAST lanes, and may result in removal of the business' name from the list of approved PIP program members on the CBSA website. A suspension can last up to 180 calendar days and will be reviewed by the CBSA within a minimum of every 60 calendar days. Suspension is intended to be a temporary status that will lead to either reinstatement or cancellation of program membership.
47. Cancellation of PIP program membership constitutes full cessation of all program-related benefits, including access to FAST lanes, dissolution of the Terms and Conditions, and termination of program membership. The business' name will be removed from the list of approved PIP program members on the CBSA website.
48. Reasons for suspension or cancellation of PIP program membership may include, but are not limited to: (a) submission of false or misleading information;
- (b) failure to respond to requests for additional or revised information within the specified timeframe; (c) failure to notify the CBSA of changes to the business as they occur, including any changes to the supply chain, business structure, security practices, location(s) of operations, or contact information;
- (d) failure to disclose information that directly impacts the member's security profile, including security-related incidents or breaches;
- (e) failure to abide by the obligations outlined in the Terms and Conditions of PIP membership;
- (f) failure to continue to meet PIP program eligibility criteria or MSRs;
- (g) failure to pass a site validation or renewed risk assessment;
- (h) refusal to undergo a site validation;
- (i) failure to submit updated security profile information for revalidation of PIP program membership;
- (j) failure to comply with the requirements of an action plan or to address security deficiencies in a satisfactory manner;
- (k) commission of an infraction under the [Customs Act](#) or any of its regulations, or under any legislation enforced by the CBSA or other international customs organization; and/or
- (l) lack of cooperation with the CBSA, such as repeatedly asking for extensions, neglecting to return phone or e-mail correspondence, failing to provide requested documentation, or refusing to grant access to the business' premises.
49. Members are required to respond within the specified timeframe to all requests from the CBSA regarding their PIP program status, including requests to confirm or update business or contact information, schedule an on-site validation or post-incident analysis, provide additional details on business or security practices, submit or verify information in the Trusted Trader Portal, etc. Failure to respond to a request from the CBSA may result in suspension or cancellation of membership.
50. A suspension or cancellation decision will be rendered by the CBSA after thorough consideration of the situation.
51. A letter of notification will be sent to the member following a CBSA decision to suspend or cancel program membership.. The letter will state the reason(s) for suspension or cancellation, provide an effective date for the decision, and specify the length of the suspension, if applicable. Suspension or cancellation of PIP program

membership is subject to appeal. **Note:** For information on appealing a CBSA decision refer to Appeals under “Suspension or Cancellation of PIP Program Membership”.

Reinstatement

52. The CBSA may reinstate program membership following an appeal of a suspension or cancellation decision, or following verification of corrective measures implemented to resolve security deficiencies identified by an action plan.

Appeals

53. An applicant or member that disagrees with a denial, suspension, or cancellation decision by the CBSA may submit an appeal electronically to: CBSA.Trusted_Trader-Negociants_dignes.ASFC@cbsa-asfc.gc.ca

54. Only one appeal will be considered by the CBSA for any particular decision. In order to be considered, the appeal must:

- (a) be submitted within 30 business days from the effective date of the decision being appealed;
- (b) clearly state the appellant’s PIP Membership Number and the reason(s) for appeal; and
- (c) include any supporting documentation.

55. The appellant’s ‘denied’, ‘suspended’, or ‘cancelled’ status will remain in effect throughout the duration of the appeal period. No further application processing or administration of program membership will occur until the CBSA has rendered a decision.

56. If the CBSA overturns a decision to deny a program application and accepts the appeal, then the application process will resume from the point at which it was interrupted. Conversely, if the CBSA upholds a decision to deny an application and rejects the appeal, then the denial will remain in effect and the business will be required to reapply following the expiration of any prescribed waiting period.

57. If the CBSA overturns a decision to suspend program membership and accepts the appeal, then either the suspension will end immediately and program membership will be reinstated, or the duration of the suspension will be reduced at the discretion of the CBSA. Conversely, if the CBSA upholds a decision to suspend program membership and rejects the appeal, then the suspension of membership will remain in effect.

58. If the CBSA overturns a decision to cancel program membership and accepts the appeal, then either the cancellation will end immediately and program membership will be reinstated, or the member will be placed under suspension for a specified duration pending corrective action. Conversely, if the CBSA upholds a decision to cancel program membership and rejects the appeal, then the cancellation of membership will remain in effect.

59. The CBSA will render a decision and a letter of notification will be sent to the business within 30 business days of receipt of the appeal, not including any period of time in which the application is held in abeyance pending the receipt of requested additional information or response from the business. The letter will state the CBSA’s decision and specify an effective date. All appeal decisions rendered by the CBSA are final. **Reapplication**

Following Cancellation

60. A moratorium on reapplication following a cancellation decision will be imposed at the discretion of the CBSA depending on the reason(s) for cancellation.

61. The CBSA reserves the right to specify reapplication timeframes on a case-by-case basis, and to disallow reapplication indefinitely for serious cases.

Post-incident Analysis

62. The CBSA may conduct a Post-Incident Analysis (PIA) following an incident or breach of supply chain security. A letter of notification will be sent to the program member when a PIA has been initiated. The letter will state the reason for the PIA and request the member's participation. The PIA will seek to:
- (a) identify the source of the incident;
 - (b) assess the member's response and cooperation with customs regulations and law enforcement (including self-reporting); and
 - (c) ensure the implementation of proactive measures to prevent future incidents.
63. The sole purpose of a PIA is to assess compliance with PIP program MSRs following a security-related incident. A PIA will not be conducted at the request of another program or agency without grounds directly rooted in PIP program policy.
64. Incidents that require a PIA may include, but are not limited to:
- (a) a violation of the [Customs Act](#) or any of its regulations, or of any legislation enforced by the CBSA or other international customs organization;
 - (b) a violation of the Terms and Conditions or of PIP program policies; or (c) a perceived weakness in a PIP program member's supply chain.
65. Incidents that require a PIA may be brought to the attention of the CBSA by means of:
- (a) voluntary disclosure by the business or its authorized representative, in accordance with the obligations set out in the Terms and Conditions of PIP program membership;
 - (b) communications with CBSA operations, including border services officers;
 - (c) exchange of information with the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) program, or any other AEO program under an established MRA;
 - (d) court decisions or legal publications; or
 - (e) information in news media or other open sources.
66. At the discretion of the CBSA, membership benefits, including access to FAST lanes entering Canada, may be maintained or suspended throughout the duration of a PIA depending on the severity of the incident.
67. The outcome of a PIA will be determined by the CBSA upon consideration of all findings and pertinent information. Should any indicators of criminal activity be discovered in the course of a PIA, the CBSA will refer the findings to the appropriate law enforcement authority.
68. The outcome of a PIA may consist of:
- (a) an awareness presentation or training session given by a CBSA officer to the business and its employees to promote greater understanding of security-related issues and vulnerabilities; (b) an action plan to outline corrective measures in response to the incident; and/or (c) suspension or cancellation of program membership.
69. If the program member gives an unsatisfactory explanation as to the possible cause(s) of the incident, fails to respond effectively to the incident, and/or is unwilling or unable to participate in a PIA, then program membership may be suspended or cancelled at the discretion of the CBSA.
70. A letter of notification will be sent to the program member when a PIA has been concluded. The letter will state the outcome of the PIA and will provide an effective date for the CBSA's decision. A CBSA decision affecting PIP program membership as a result of a PIA is subject to appeal.

Cargo Seal Requirements

71. All PIP program applicants and members must have a written seal policy in accordance with PIP program MSRs. This must include procedures for proper disposal of used seals in order to mitigate the risk of counterfeit seals.
72. PIP program members are responsible for monitoring their supply chains and ensuring seal integrity throughout the life cycle of a shipment of goods, including proper use of high-security seals, in accordance with PIP seal requirements.
73. The use of high-security seals is not required for CSA carriers; however, CSA program members that are also PIP program members must comply with PIP requirements, including the mandatory use of high-security seals.
74. To access FAST lanes into Canada, both PIP and CSA program requirements must be met, including the mandatory use of high-security seals as required by the PIP program. **Note:** For further information refer to the [Cargo Sealing Guidelines for PIP Members](#).

General Seal Requirements for all PIP Program Members

75. PIP program members must ensure that a high-security seal is affixed to all loaded containers and trailers that cross the border in either direction, including shipments that cross the border while in transit to a domestic location.
76. For PIP program purposes, high-security seals are classified as meeting or exceeding the ISO/PAS (International Organization for Standardization / Publicly Available Specification) 17712 standard for mechanical freight container seals.
77. PIP program members must:
 - (a) ensure that seals are affixed by an authorized individual who is appropriately trained in the proper application and use of high-security seals;
 - (b) acquire seals from a legitimate manufacturer and obtain the manufacturer's test report to be kept for future reference and verification that seals meet the ISO/PAS 17712 standard;
 - (c) safeguard the use of seals and maintain a record of all issued seal numbers. Seals must be controlled and secured by authorized personnel;
 - (d) inspect seals on all cargo-laden containers and trailers. The receiving party is responsible for verifying seal integrity at each transfer of custody;
 - (e) report any seal discrepancies or evidence of tampering to a border services officers at the point of entry into Canada, or to an appropriate law enforcement authority such as local police. All discrepancies and instances of tampering must be noted in the cargo documentation;
 - (f) oversee and advise their supply chain partners to ensure that pertinent security measures are in place, including proper use of high-security seals, from point of origin through to final destination;
 - (g) document all requirements they impose on their supply chain partners with regard to the application and verification of high-security seals.

Specific Seal Requirements by Line of Business

78. If a carrier in any mode takes possession of a container or trailer that has not been sealed, the onus shifts to the carrier to seal the container/trailer and to record the seal number on the bill of lading.
79. **Highway carriers** - responsible for inspecting the condition of seals and for comparing each seal number against the shipping documentation. If a seal has been broken, highway carriers must report to their dispatcher the name(s) of the person(s) responsible as well as the number of the new seal that is placed on the container/trailer. **Note:** In the highway mode, an empty container/trailer does not require a high-security seal to cross the border into

Canada. However, a container/trailer containing dunnage without cargo on board is not considered to be empty and therefore requires a high-security seal.

80. **Rail carriers** - responsible for affixing a high-security seal to all loaded rail cars and intermodal containers that are transported by rail and destined for Canada. Rail cars crossing the border into Canada must comply with seal verification rules and seal anomaly reporting requirements.

81. **Marine carriers** - responsible for inspecting seals and documenting their condition before containers are loaded onto a vessel. **Note:** In the marine mode, all containers bound for Canada must be visually inspected and sealed, even when empty.

82. **Air carriers** - responsible for overseeing all cargo loaded on board an aircraft in a manner pursuant to applicable laws and regulations. When an air carrier contracts supply chain partners to control a specific element of the cargo transportation service (such as an airport terminal, a unit load device, the direct handling of cargo containers, or any process subject to seal requirements), the air carrier must work with its supply chain partners to ensure that pertinent security measures are implemented and followed.

83. **Importers and warehouse operators** - must inspect all seals prior to removal and note any discrepancies between the seals and the information listed in the cargo documentation. Any indicators of illicit activity must be reported to the CBSA or an appropriate law enforcement agency.

84. **Exporters and freight forwarders** - responsible for sealing all containers/trailers until the carrier assumes control, and for ensuring that all seal numbers are recorded on the bill of lading.

Seal Exceptions, Replacements, and Noncompliance

85. Shipments that are **less-than-truck-load (LTL)** or **less-than-container-load (LCL)** may use high-security padlocks or similar locking devices instead of high-security seals when the pick-up or delivery of local freight involves multiple stops. However, all containers/trailers that cross the border must be secured with a high-security seal. In such cases, PIP program members must implement strict controls to limit access to padlock keys or combinations. **Note:** If a consolidation hub is used, the seal number(s) may be recorded on the consolidated lead sheet rather than the individual bills of lading. The seal number(s) should be listed on the documents presented to a border services officer.

86. Some commercial loads and conveyances are not suited to accommodate high-security seals or padlocks (e.g., tank trailers, bulk or open-top loads, dump trailers, tractors, open or van trailers, step decks, flatbeds, livestock trailers, and other types of open trailers or oversize loads for which a seal will not detect access). In such cases, PIP program members must demonstrate the use of other effective methods to ensure cargo integrity during transit. For example, cargo access could be detected by using tamper-evident tape or by undertaking more thorough and/or frequent documented inspections.

87. If a seal is removed while en route to the border, even by government officials, it is the carrier's responsibility to replace the seal and document its particulars, including the new seal number, on all pertinent cargo documentation. The carrier is not required to reseal loads examined by the CBSA if a border services officer affixes a high-security seal supplied by the CBSA after examination.

88. Depending on the frequency and/or severity of occurrence, noncompliance with PIP program seal requirements may result in:

- (a) placement on an action plan to address security deficiencies; and/or
- (b) suspension or cancellation of program membership. Before cancellation, a CBSA officer will conduct a follow-up to give the business an opportunity to rectify the situation.

Additional Information

89. For additional information or clarification on the PIP program, please e-mail PIP-PEP@cbsa-asfc.gc.ca or call the Border Information Service (BIS) line at **1-800-461-9999**. If you are calling from outside Canada, you can access BIS by calling 204-983-3500 or 506-636-5064 (long-distance charges will apply).

Appendix**Letter of Authorization**

Sample Only

Business Letter Head

Date

To: Canada Border Services Agency

Subject: Letter of Authorization This

is to advise you that:

Name of representative:

Address:

City/Province/State: Postal/Zip-code:

Is authorized by: Name

of business:

Address:

City/Province/State: Postal/Zip-code:

To provide information to the Canada Border Services Agency (CBSA) on behalf of the business as required in relation to the Partners in Protection (PIP) program.

(Business Name) acknowledges that by authorizing the above noted representative, it assumes full liability for all information provided to the CBSA by their representative.

This authorization is valid until further notice.

Authorized Signature:

Title:

Telephone Number:

References	
Issuing Office	Trusted Trader Programs Unit Commercial Program Directorate Programs Branch
Headquarters File	
Legislative References	<u>Customs Act Criminal Code</u>
Other References	<u>D1-8-1</u> , <u>D3-1-1</u> , <u>D17-4-0</u>
Superseded Memorandum D	N/A