

COMMENTS ON PROPOSED MINIMUM SECURITY CRITERIA (IMPORTERS/EXPORTERS)

January 17, 2008

| PIP REQUIREMENTS | COMMENTS |
|--|--|
| <p>GENERAL INFORMATION</p> <p>To be an eligible Importer/Exporter participant in Partners in Protection (PIP), your company must own or operate facilities in Canada directly involved in the importation or exportation of commercial goods.</p> <p>These security criteria are designed to ensure PIP program applicants implement effective security practices to secure its supply chain and mitigate the risk of contraband smuggling.</p> <p>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 flexibility and customization of security measures, within certain minimum criteria, based on the applicant’s business mode.</p> <p>Verifiable compliance with security requirements and standards set by other intergovernmental organizations, such as IMO, UNECE and ICAO, will be considered and may constitute partial or complete compliance with these security criteria.</p> | <p>Why are non-resident importers not eligible for the PIP program? It would appear preferable to include as many participants as possible. We note that under the C-TPAT program, non-resident importers and foreign manufacturers are allowed to join the program.</p> <p>What does CBSA mean by “the PIP Program allows for flexibility and customization of security measures, within certain minimum criteria...”? Is there flexibility in the application of the minimum criteria? If not, where is the flexibility?</p> <p>What does “mode” refer to? Is this a reference to the different categories or types of applicants, eg. importers, brokers, carriers, etc? The C-TPAT Agreement contemplates that within different categories of participants (importers, for example), companies may have different business “models”, which will affect their risk analysis, etc.? There should also be flexibility in application of the security measures based on such factors as the size of the company, the number of employees, the nature of the company’s business, the location of the company’s business, the activities carried out at a particular location, etc.</p> <p>Suggest providing full names rather than acronyms for IMO, etc.</p> <p>There are a number terms used throughout this document, including Supply Chain Security Profile, minimum security criteria, and Assessment Report, that should be defined in a separate Definitions section.</p> |

| | |
|---|---|
| <p>APPLICATION PROCESS</p> <p>1. The PIP application process has 3 stages:</p> <ul style="list-style-type: none"> (i) Completion of the Supply Chain Security Profile by the applicant. (ii) Completion of a security review and Assessment Report by the CBSA. (iii) Signing of a Memorandum of Understanding (MOU). | |
| <p>2. Upon receipt of a completed Supply Chain Security Profile, a security review will be undertaken by the CBSA to confirm the security measures detailed in the Security Profile. At the end of its security review, the CBSA will prepare an Assessment Report. A copy of this Report will be provided to the applicant.</p> | <p>What will the security review entail and how will it be conducted?</p> <p>Will CBSA conduct a security review of all of the facilities of the applicant before granting PIP? Clarification is required of what CBSA is expecting as a "Security Profile" for a company that has several locations. Different locations may have different activities and not all locations have the same level of risk.</p> <p>It is recommended that in general only those locations that are the point of first delivery for goods after importation and main offices should be subject to the PIP Security Criteria. Retail locations would not be covered, for example, unless imported goods were delivered directly to these locations following importation rather than going through distribution centres. There may be some exceptions. Some security measures may have to be company wide, such as those relating to data and documentation protection.</p> <p>Timeframes should be established for CBSA to complete its security review and to provide the applicant with a copy of the report. We suggest 30 days to respond to the initial application and 6 months to carry out the security review and provide the applicant with a copy of the report.</p> <p>A larger concern is whether CBSA will have sufficient qualified officers to review the applications and to conduct the security reviews. We suggest that CBSA adopt the approach followed under the C-TPAT program in the United States of approving participants and conducting the verifications within a specified timeframe after the application is approved. This approach has the advantage of allowing applicants time following</p> |

| | |
|--|---|
| | <p>acceptance into the program to implement some of the security measures that they propose to implement in their Supply Chain Security Profile before the verification is carried out by CBSA. However, even if CBSA follows the approach used in the United States, we still have serious concerns whether CBSA will have the necessary qualified personnel to review the applications and re-approve existing PIP members and process new members during a transition period. In addition, how does CBSA contemplate that it will sustain the program over the longer term?</p> |
| <p>3. In addition to the applicant being able to meet or exceed the minimum security criteria set out herein, the applicant must have both a good record of compliance with the CBSA, and its directors must all be of good character.</p> | <p>What constitutes "good" compliance? Is there a metric that will be used to determine the threshold of "good compliance"? If so, will the importer/exporter be made aware of this "compliance score"? How does one improve this score if required?</p> <p>For greater certainty, we recommend that CBSA substitute "members of the board of directors" for "directors."</p> <p>What is meant by "good character"? How will "good character" be determined? If one director is found not to be of good character, will the company be advised as to who that person is? Will the CBSA provide reasons and will there be an appeal process?</p> |
| <p>4. If the security review and Assessment Report of the CBSA conclude that the applicant's Security Profile meets or exceeds the minimum security criteria, the applicant will be notified and asked to sign two (2) original copies of the PIP MOU prepared by the CBSA and return both to the CBSA for its signature. The MOU sets out the roles and responsibilities of the applicant to maintain its status as an authorized participant in the PIP Program.</p> | <p>As noted above, timeframes should be established for CBSA to complete its security review and to provide the applicant with a copy of the report.</p> <p>How frequently does CBSA contemplate conducting follow up reviews once a company has been accepted into the PIP program?</p> |
| <p>5. Once the CBSA has signed both copies of the PIP MOU, one copy will be returned to the applicant. At this time, the applicant is considered to be an authorized PIP Participant.</p> | |
| <p>6. An application may be rejected for any omission or the submission of false information.</p> | <p>What recourse will be available where an application is rejected?</p> |
| <p>7. Should the security review and Assessment Report of the CBSA</p> | <p>Will the CBSA assessment report state exactly why the application was</p> |

| | |
|--|---|
| <p>conclude that the applicant's Security Profile 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 Assessment Report to the complete satisfaction of the CBSA.</p> | <p>denied? If an applicant is rejected, will the applicant have to go through the entire application process again? We suggest that the application be kept open and that the applicant be given the opportunity to respond to the report and provide additional information and/or correct any deficiencies.</p> |
| <p>APPLICATION INSTRUCTIONS:</p> <ol style="list-style-type: none"> 1. Complete Sections 1, 2 and 3 of the Supply Chain 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 4 – 11. 3. Send a copy of the completed Security Profile to the PIP Program, CBSA, 191 Laurier Avenue West, Ottawa, Ontario, K1A 0L8, or electronically by email to: PIP@cbsa-asfc.gc.ca 4. An incomplete Security Profile will not be processed. <p>Direct any questions about this Security Profile to the CBSA through the PIP e-mail address: PIP-PEP@cbsa-asfc.gc.ca</p> | <p>There is concern about the security of applications submitted electronically by email, as well as those submitted in hard copy by mail or courier.</p> <p>The expectation is that CBSA will in the relatively near future create a Web portal for the PIP program. We recognize, however, that this Web portal will not be in place in time for the re-launch of the PIP program. In the meantime, appropriate access and security controls must be put in place to protect data privacy whether documentation is submitted electronically or in hard copy. Among other things, the name of the CBSA official designated to receive the applications should be provided, and an acknowledgement process should be established.</p> <p>Also given the potential size of some of the documents being requested (eg. site maps), there is concern about the ability to transmit these documents electronically and the capacity of CBSA's system to receive them.</p> |
| <p>ADDITIONAL SECURITY REQUIREMENTS (If Applicant accepted into PIP Program)</p> <ol style="list-style-type: none"> 1. Notification in writing of any changes to the company information contained in Sections 1, 2 and 3 must be provided to the CBSA within 30 days of such change. | <p>Some of the company information requested, such as number of employees, will change frequently and it will not be practical to update them. We suggest that CBSA identify those fields of information that it considers necessary to be updated within 30 days, with the remainder being updated annually.</p> |
| <ol style="list-style-type: none"> 2. When changes occur and/or when the company makes security improvements, an updated Supply Chain Security Profile must be provided to the CBSA. In all other cases, an updated Security Profile must be provided to the CBSA no later than three (3) years from the date of this Security Profile. | <p>What would CBSA consider to be a "change" or "improvement" for purposes of this section? Would the holding of a training session or issuance of written communications constitute an improvement, for example? It would not appear to be practical for the Security Profile to be updated every time there is a change or improvement, especially if CBSA will not have a Web portal that can be used to notify CBSA. Presumably CBSA's interest is in ensuring that there is no significant</p> |

| | |
|---|--|
| | <p>decline in the level of supply chain security and receiving communications about any changes that would impact CBSA’s assessment of whether the minimum security criteria are still being met. In addition, if a Participant is making improvements to its security processes and procedures in accordance with a plan set out in its Security Profile, it is reasonable to expect that the Participant would advise CBSA as it implements these improvements. Otherwise, it should be possible to provide information with respect to changes or improvements with the update required every three years.</p> |
| <p>SECTION 1: COMPANY INFORMATION</p> <p>[Form omitted]</p> | <p>Under subsection 1.4, not all companies will have a Dun and Bradstreet number. It is important to ensure that leaving this field blank will not cause the application to be rejected.</p> <p>Under subsection 1.5 Criminal Offences, in the first question, suggest substituting “convicted of any offence under any” for “found in violation of.” Presumably a company that merely receives an AMPS penalty could be considered to have been in violation of the law.</p> <p>We suggest providing a timeframe for checking into criminal offences, ie. five years, which the period usually covered in criminal background checks,</p> <p>Under subsection 1.10, does “participant” mean fully approved and live on a program or at some stage of the application process of a program?</p> <p>Under subsection 1.13, does a signing officer need to sign this field or any level of employee?</p> <p>For obvious reasons, there is serious concern about the confidentiality of information provided by applicants to the PIP program. With respect to subsection 1.14 Privacy Statement, there does not appear to be a legal basis for stating that the information provided in the security profile and other supporting documentation is “collected under the Customs Act (Canada), and is ‘customs information’ as that information is defined therein” as the PIP program is not provided for under the Customs Act. This means that the disclosure provisions of the <i>Customs Act</i> would not</p> |

| | |
|--|--|
| <p>SECTION 2: COMPANY CONTACT INFORMATION</p> <p>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 responsible for the security commitments within the company.</p> <p>[Table omitted]</p> | <p>apply.</p> |
| <p>Complete Sections 3 to 11 by describing in detail, your company’s policies, practices and procedures, etc. to demonstrate how the minimum- security criteria are met. In the text box for each section, you must 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 you feel it does not apply to your company. Each response should make reference to the section number.</p> <p>Acceptance of your company in the Partners in Protection (PIP) program is dependant on the responses provided in this profile. Inadequate or incomplete responses will result in the application being rejected.</p> | |
| <p>Section 3. Company Site Map</p> <p>A site map will assist in the review and approval of your application.</p> | <p>This requirement raises a number of questions. For example, for which locations will site maps be required? Are satellite sales offices required to provide maps of their offices and to what detail? It is recommended that site maps only be required for those locations that are the point of first delivery of the Participant for goods after importation and for main offices. Retail locations would not be covered, for example, unless imported goods were delivered directly to these locations following importation rather than going through a distribution centre.</p> |

| | |
|--|--|
| | <p>Providing site maps will raise serious concerns for large and small companies. Given the sensitivity of the information contained in a site map, it is recommended that site maps not be submitted to CBSA but rather be made available to CBSA officers at the time that the verification visits are made.</p> |
| <p>3.1 Site location details</p> <p>The site plan should be to scale and clearly identify a company’s site boundaries, the various buildings within the site and also the usage of any open areas. Entry points to the site and the buildings within the site must be clearly indicated and labeled. The company should also include the positions of the lighting (flood lights, emergency lights, etc.), CCTV’s and any other security equipment in the company’s premises. The site plan must be dated and identified with the name and address of the site.</p> <p>Include map (clearly labeled) when submitting the application.</p> | |
| <p>Section 4: Physical security and access controls</p> <p>Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.</p> <p>Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets.</p> | <p>What is the purpose of the “preamble” to each section? Is the preamble intended to establish requirements and obligations, or simply to introduce or explain the specific requirements and obligations contained in the subsections that follow?</p> |
| <p>4.1 Facilities</p> <p>Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.</p> <p>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.</p> | <p>Applicants may not be owners of the property and may not have control over gates and fences. It is not clear how a fence would be secured with a locking device. It is recommended that the reference to gates and fences be removed from this section and the reference to locking devices on gates moved to subsection 4.8.</p> |

| | |
|--|---|
| <p>4.2 Key Control</p> <p>Management or security personnel must control the issuance of all locks and keys</p> | |
| <p>4.3 Lighting</p> <p>Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.</p> | <p>Applicants may not be owners of the property and may not have control over lighting outside the facility. It will also not be practical or feasible to light fence lines if there is extensive fencing. It is recommended that “must” be substituted with “should.”</p> |
| <p>4.4 Communications</p> <p>Communications systems must be in place to contact internal security personnel or local law enforcement officials.</p> | |
| <p>4.5 Parking</p> <p>Private passenger vehicles for visitors and employees should be prohibited from parking in or adjacent to cargo handling and storage areas.</p> | <p>As applicants may not be owners of the property and may share parking with other companies, we support the use of “should” rather than “must” in this subsection.</p> |
| <p>4.6 Fencing</p> <p>Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All fencing must be regularly inspected for integrity and damage.</p> | <p>We support the use of “should” rather than “must” in this section. Most companies will not have perimeter fencing. It would not be practical or cost effective to have fencing around the perimeter, especially for small importers. This is also a concern where importers share common facilities such as at an industrial park.</p> <p>It is also not always feasible for companies to segregate cargo inside their facilities due to lack of space and personnel. For certain types of cargo, such as hazardous material, segregation is required under existing regulations. Satisfying those regulations should be sufficient.</p> |
| <p>4.7 Signage</p> <p>Signage should exist directing conveyances and persons to appropriate areas. Signage should exist to prevent unauthorized personnel access to restricted areas and/or premises.</p> | <p>In the second sentence, substitute “deter” for “prevent.”</p> |
| <p>4.8 Gates and Gate Houses</p> <p>Gates through which vehicles and/or personnel enter or exit must be</p> | <p>Applicants may not be owners of the property and may not have control over gates and gate houses. Recommend substituting “should” for “must” in the first sentence. Further to comment to subsection 4.1, suggest</p> |

| | |
|--|---|
| <p>manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.</p> | <p>adding the following at the end of the second sentence “and all gates should be secured with locking devices when not being monitored.”</p> |
| <p>4.9 Alarm Systems & Video Surveillance</p> <p>Alarm systems and video surveillance should be utilized 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.</p> | |
| <p>4. 10 After- Hours Access</p> <p>For company’s operations that do not operate 24/7, provide details of after-hours access.</p> | |
| <p>4.11 Physical Access Controls</p> <p>Access controls prevent unauthorized entry to 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 the shipping, loading dock and cargo areas must be prohibited.</p> | <p>What is meant by “positive” identification? Does this necessarily mean photo identification? Will blank access cards or simple recognition of employees (eg. at small locations with less than 10 employees) be acceptable? If photo identification will be required, we recommend an exception for employees at small locations (eg. under 10 employees).</p> |
| <p>4.12 Employees</p> <p>An employee identification system must be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed in the performance of their duties.</p> <p>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, key cards etc.) must be documented.</p> | <p>See comments to subsection 4.11 regarding employees.</p> <p>As the first sentence of the second paragraph is not restricted to employees, we suggest that this sentence be moved to subsection 4.11.</p> |

| | |
|---|--|
| <p>4.13 Visitors</p> <p>Visitors must present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification.</p> | <p>What does “for documentation purposes” mean? Is this a reference to a visitor log?</p> <p>Some visitors may be known to employees of the company. It is recommended that the following be inserted after “must” and before “present”: “be positively identified by an employees of the PIP Participant or.”</p> |
| <p>4.14 Challenging and Removing Unauthorized Persons or Vehicles</p> <p>Procedures must be in place to identify, challenge and address unauthorized/unidentified persons or vehicles.</p> | |
| <p>4.15 Deliveries (including mail)</p> <p>Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail should be periodically screened before being disseminated.</p> | <p>Will PIP participants be required to keep a record of all visitors including validation of identification (i.e., a log)? What type of screening will be required for arriving packages on a periodic basis?</p> |
| <p>Section 5. Procedural Security</p> <p>Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the secure supply chain. Importers must ensure business partners develop security processes and procedures consistent with the PIP security criteria to enhance the integrity of the shipment at point of origin. Periodic reviews of business partners’ processes and facilities should be conducted based on risk and should maintain the security standards required by the importer.</p> | <p>To what extent does CBSA expect importers to ensure that their business partners develop security processes and procedures consistent with PIP? Which business partners? All vendors, carriers, warehouses, freight brokers, forwarders? Some importers have thousands of suppliers of goods and services. Most importers will not be in a position to impose requirements on their suppliers to implement security processes and procedures as a condition of their contracts. A risk based approach needs to be adopted not only with respect to conducting reviews of business partners but also with respect to which business partners (eg. key or strategic partners) should be required to implement security processes and procedures.</p> <p>If importers cannot ensure that business partners develop security processes and procedures, the PIP participant can mitigate the risk by following tighter security procedures when dealing with that supplier, such as subjecting merchandise received from that business partner to greater inspections.</p> |

| | |
|--|--|
| | <p>What if there is an incident involving a "partner"? Is the importer going to be implicated as well? Many companies use the same foreign partners. Are all importers known to use this supplier implicated in the case of an incident?</p> <p>Finally, see the comments to section 10. It is recommended that all the provisions with respect to business partners be consolidated under that section to avoid confusion, especially since none of the requirements in the subsections to section 5 relate specifically to business partners. The last two sentences, starting with "Importers must ensure.." are almost identical to subsection 10.3.</p> |
| <p>5.1 Process Mapping</p> <p>Map your process illustrating the flow of goods and documentation/information through your international supply chain.</p> | <p>To what level of detail are these process maps required to be created and maintained? Process maps have different levels of detail and are constantly updated, tweaked and modified to improve operations. Would every revision have to be sent to CBSA?</p> <p>More fundamentally, what is the purpose of this requirement? Not all companies prepare process maps. This should not be a mandatory requirement.</p> <p>We also suggest that where an applicant is prepared to provide process maps voluntarily this type of information be provided at the time of the site visit rather than being submitted with the application.</p> |
| <p>5.2 Shipping and Receiving (Drivers)</p> <p>Drivers delivering or receiving cargo must be positively identified before cargo is received or released. A designated security representative should supervise the introduction/removal of cargo.</p> | <p>We support the use of "should" rather than "must" in this section as it may be difficult or burdensome for small companies to have a designated security representative at cargo loading areas.</p> <p>We recommend that "security representative" be substituted with "designated employee."</p> |
| <p>5.3 Cargo Tracking</p> <p>Measures should be in place to track the timely movement of incoming and outgoing cargo.</p> | |

| | |
|--|---|
| <p>5.4 Cargo Reconciliation</p> <p>Arriving cargo must be reconciled against information on the cargo manifest. Measures must be in place to detect and report cargo shortages and overages. The cargo should be accurately described and the weights, labels, marks and piece count indicated and verified.</p> | <p>We support the use of “should” rather than “must” in the last sentence of this subsection as it is expensive and burdensome to weigh inbound containers for validating weights. Generally companies only weigh inbound containers when there is reason to suspect a problem.</p> |
| <p>5.5 Security Sweeps</p> <p>Random, unannounced security assessments of areas in your company’s control within the supply chain should be conducted.</p> | |
| <p>5.6 Reporting of Anomalies or Suspicious Cargo Activity</p> <p>In cases where anomalies or illegal activities are detected or suspected by the company, the CBSA and/or other law enforcement agencies must be notified, as appropriate.</p> | <p>Consistency in the terminology used and clarity with respect to what is expected is needed. In the title, we have “anomalies or “suspicious cargo activity.” In the body, there is reference to “anomalies or illegal activities.” In subsection 5.7, “illegal or suspicious activities” is used.</p> <p>“Anomalies” and “suspicious activities” are too broad. We recommend restricting this requirement to illegal or suspected illegal activities.</p> <p>What does “as appropriate” refer to, the appropriate authorities?</p> |
| <p>5.7 Cargo Documentation Processing</p> <p>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.</p> <p>To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and timely.</p> <p>All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. CBSA and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected – as appropriate.</p> | <p>With respect to the last sentence of the third paragraph, see comments to Subsection 5.6 above.</p> |
| <p>Section 6: Container, Trailer and Rail Car Security</p> | |

| | |
|--|--|
| <p>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, procedures must be in place to properly seal and maintain the integrity of the shipping container, trailer or rail car.</p> <p>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.</p> | |
| <p>6.1 Cargo Integrity</p> <p>Procedures should be in place for affixing, replacing, recording, tracking, and verifying seals on containers, trailers, and railcars. Describe the security measures your company uses with respect to containers, trailers and rail cars used in the transport of international cargo.</p> | <p>There appears to be inconsistency between this subsection 6.1 and the preamble to section 6. The preamble states that “procedures must be in place to properly seal and maintain the integrity of the shipping container...” Subsection 6.1 states that “[p]rocedures should be in place for affixing, replacing, recording, ... seals on containers...” Are seals mandatory on all containers or not?</p> <p>More generally, what is the purpose of the “preamble” to each section? Is the preamble intended to establish requirements and obligations, or simply to introduce or explain the specific requirements and obligations contained in the subsections that follow? If there is inconsistency between the preamble and the wording of a subsection, as in this case, which prevails?</p> |
| <p>6.2 Container, Trailer and Rail Car Inspection</p> <p>Procedures must be in place to verify the physical integrity of the container structure, trailer and rail car prior to stuffing, to include the reliability of the locking mechanisms of the doors and search for signs of tampering.</p> | <p>We suggest combining subsections 6.2 and 6.5.</p> |
| <p>6.3 Container, Trailer and Rail Car Seals</p> <p>Foreign business partners should have documented procedures that set forth their internal policy regarding the affixing and processing of cargo and containers that employ high-security seals that meet or exceed the current ISO standard and/or other devices that are designed to prevent tampering with cargo.</p> | <p>“Meet” should be “meet.”</p> <p>See comments to subsection 6.1 above.</p> |

| | |
|---|---|
| <p>6.4 Container, Trailer and Rail Car Storage</p> <p>Containers, trailers and rail cars must be properly stored to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers, storage areas, trailers and rail cars.</p> | |
| <p>6.5 Container Inspection</p> <p>Procedures must be in place to verify the physical integrity of the container structure, trailer and rail car prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers:</p> <ul style="list-style-type: none"> • Front wall • Left side • Right side • Floor • Ceiling/Roof • Inside/Outside doors • Outside/Undercarriage | <p>See comment to subsection 6.2. If subsections 6.2 and 6.5 are not combined, this subsection should also make reference to searching for signs of tampering as in subsection 6.2.</p> |
| <p>Section 7: Data and Documentation Protection</p> <p>A well defined physical security policy and system controlling the access to any office or secure areas must be in place to ensure 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.</p> | |
| <p>7.1 Cargo Manifests/Forms</p> <p>Your company must have procedures to secure the storage of used and unused forms and related cargo documentation, to prevent the loss or unauthorized use of such documentation.</p> | |
| <p>7.2 Information Technology (IT) Security</p> <p>Automated systems must use individually assigned accounts that</p> | |

| | |
|---|--|
| <p>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.</p> <p>Procedures and standards must be in place and provided to employees in the form of training to protect against unauthorized access to and misuse of information.</p> | |
| <p>7.3 Company policies on IT Violations</p> <p>A process must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions for abuse.</p> | |
| <p>Section 8: Personnel Security</p> <p>Personnel security programs must incorporate screening of employees and prospective employees. These programs should include periodic background checks on employees working in security-sensitive positions, noting unusual changes in an employee's apparent social and economic situation.</p> | |
| <p>8.1 Pre-Employment Application Verification</p> <p>Application information, such as employment history and references must be verified prior to employment.</p> | |
| <p>8.2 Employee Background Checks</p> <p>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</p> | <p>How frequently is "periodic"? Would all employees have to undergo periodic checks and reinvestigations? Most companies generally only screen prospective employees upon hiring and after hiring only if there is cause. They do not have the funds or manpower to do "periodic" checks of all employees. We recommend inserting "where needed" at the end of the second sentence.</p> |
| <p>8.3 Terminated/Departing Employees</p> <p>Companies must have procedures in place to remove identification, facility and system access for terminated and departing employees and ensure that all company property is returned.</p> | |
| <p>Section 9 : Security Training and Awareness</p> | |

| | |
|---|---|
| <p>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, maintaining product integrity and foster awareness of the threat posed by the criminal and terrorist element at each point in the supply chain.</p> | |
| <p>9.1 Corporate Security Policies</p> <p>Companies are encouraged to enhance border security by establishing threat awareness programs to ensure that security threats such as contraband smuggling, human smuggling, terrorism, etc., are recognized at each point in the supply chain.</p> | |
| <p>9.2 Security Awareness</p> <p>Employees must be made aware of the procedures the company has in place to address a situation and how to report it. Programs should encourage active employee participation in security controls. Records should be maintained of employee attendance at security meetings.</p> | <p>Not all security training will be conducted face to face. There may be electronic education, posters, notices, bulletins, etc. It is recommended that companies should track and monitor all forms of training, including monitoring how training is being incorporated into operations and improving security and whether the appropriate people are receiving the appropriate training.</p> |
| <p>9.3 Security Policy Manual</p> <p>The company should develop and maintain a security policy manual that contains detailed guidelines of efforts to secure cargo within their control.</p> | |
| <p>Section 10: Business Partner Requirements</p> <p>Where a company contracts out elements of their international supply chain, it is vital the company work with their business partners to ensure sound security measures are in place and adhered to, to achieve an effective secure supply chain globally.</p> | <p>See comments to section 5 with respect to business partners.</p> <p>There is overlap between sections 5 and 10 and some inconsistency in the language used. In the case of section 5, only the preamble contains reference to business partners raising confusion again about the purpose of the preamble. To avoid confusion, we recommend that all provisions relating to business partners be consolidated under this section 10.</p> |

| | |
|---|---|
| <p>Based upon a documented risk assessment process, business partners not eligible for PIP must be subject to verification of compliance with PIP security criteria by the company.</p> | <p>What does “not eligible” mean in this context? We assume that it refers to their eligibility to apply for the program as opposed to their ability to qualify for acceptance into the program. We recommend substituting “not eligible for PIP” with “that are not PIP participants or participants in another country’s supply chain security program.”</p> <p>What does “must be subject to verification of compliance” mean? Does this mean that verifications must be conducted of all business partners that are not PIP approved? This would be inconsistent with subsection 10.3 which states that periodic reviews “should” be conducted.</p> |
| <p>10.1 Selection Criteria</p> <p>Companies must have written and verifiable processes for the selection of business partners including manufacturers, product suppliers, vendors and carriers.</p> | <p>What will the CBSA accept as a “verifiable” process?</p> |
| <p>10.2 Satisfying the business partner security requirements.</p> <p>International supply chain business partners must demonstrate they are meeting your company’s supply chain security obligations.</p> <p>Businesses that are not eligible for PIP, can demonstrate they are meeting these security criteria in a number of ways.</p> <ul style="list-style-type: none"> • written or electronic confirmation, or • contractual obligations, or • a letter from a senior business partner officer attesting to compliance, or • a written statement from the business partner demonstrating their compliance with these criteria or another countries (sic) supply chain security criteria, e.g. U.S. Customs Trade Partnership Against Terrorism (C-TPAT) or an equivalent WCO accredited security program administered by a foreign customs authority (e.g. Authorized Economic Operator – AEO), or • by providing a completed supply chain security profile. | <p>See comment to section 10 regarding “Businesses that are not eligible for PIP.” We recommend substituting this language with “Businesses that are not PIP participants.”</p> <p>In the fourth bullet point, “countries” should be “country’s”.</p> <p>Will the WCO be accrediting security programs?</p> |

| | |
|--|--|
| <p>10.3 Business partners – Point of Origin</p> <p>Companies must ensure foreign business partners develop security processes and procedures consistent with these security criteria to enhance the integrity of the shipment at the point of origin. Periodic reviews of your business partner’s processes and facilities should be conducted based on risk and should maintain the security standards required by your company.</p> | <p>See comments to section 5 above.</p> <p>The language in this section 10.3 is almost identical to the language in the last two sentences of the preamble to section 5. However, subsection 10.3 refers to “foreign” business partners, although both deal with the “integrity of the shipment at the point of origin.” Is CBSA making a distinction between foreign and domestic business partners?</p> <p>It may not be practical to do periodic reviews of ALL business partner processes and facilities if there are thousands used globally. Is it sufficient to do a combination of electronic questionnaires and onsite assessments for higher risk areas or strategic partners?</p> |
| <p>10.4 Business Partner - Other Internal Selection Criteria</p> <p>Using a risk based approach, 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.</p> | <p>What is the alternative for the Participant if the Supplier does not meet the security criteria? As discussed in the comments to section 5, could the Participant put additional security measures in place at its end of the supply chain?</p> |
| <p>Section 11: Supply Chain Security Planning</p> <p>Policies and procedures should be in place for the company to undertake a risk assessment of their supply chain, identifying gaps and weaknesses and implement strategies to mitigate those risks.</p> | |
| <p>11.1 Determining Risks</p> <p>Your company should have measures to identify, analyse and mitigate supply chain security risks.</p> | |
| <p>11.2 Compliance with Security Profile</p> <p>Procedures should be in place to ensure regular re-assessment of and compliance with the company’s Security Profile.</p> | <p>What does “regular” mean in this context?</p> |
| <p>11.3 Contingency Planning</p> <p>Periodic training of employees and testing of emergency contingency</p> | |

| | |
|---|--|
| <p>plans should be in place to ensure continuation of trade in the event of an emergency/security situation. Describe what contingency plans your company has in place.</p> | |
| <p>Section 12 : Other</p> <p>Your company may have security measures for the protection of the international supply chain that have not been previously described in other sections of this profile.</p> | |