



Tel: 519-326-0101 Fax: 519-326-0204
www.bonneaufreight.com

CARRIER SECURITY QUESTIONNAIRE

COMPANY INFORMATION

| | |
|--------------------------------------|--|
| LEGAL NAME OF COMPANY | |
| TRADE NAME (if different than above) | |

| | PHYSICAL ADDRESS | MAILING | Same as physical address |
|-------------|------------------|----------|--------------------------|
| STREET: | | | |
| CITY, PROV. | | | |
| POSTAL CODE | | | |
| NAME: | | TITLE: | |
| PHONE: | | FAX: | |
| E-MAIL: | | WEBSITE: | |

CERTIFICATIONS

Please specify your participation in any Canadian or US Customs Partnership programs and attach certificates where applicable:

| | YES | NO | APPLICATION IN PROGRESS | ESTIMATED DATE OF APPROVAL | NO PLANS TO APPLY |
|--------|-----|----|-------------------------|----------------------------|-------------------|
| FAST | | | | | |
| CSA | | | | | |
| PIP | | | | | |
| C-TPAT | | | | | |

If C-TPAT certified, please e-mail your SVI to admin@bonneaufreight.com through the CBP portal.

SECURITY QUESTIONS

Do you have documented Security Procedures in place that are comparable to the attached Security Recommendations?

| | SECTION | YES | NO |
|----|--|-----|----|
| 1. | Business Partners Requirements | | |
| 2. | Conveyance/Container Security | | |
| 3. | Physical Access Controls | | |
| 4. | Personnel Security | | |
| 5. | Procedural Security | | |
| 6. | Physical Security | | |
| 7. | Security Training and Threat Awareness | | |
| 8. | Information and Technology Security | | |

AUTHORIZED PERSON: _____
(SIGNATURE) (PRINTED NAME / TITLE) (DATE)



CARRIER SECURITY QUESTIONNAIRE

Business Partner Requirements

Highway carriers must have written and verifiable processes for the screening of business partners, including carrier's agents, sub-contracted highway carriers, and service providers, as well as screening procedures for new customers, beyond financial soundness issues to include security indicators, such as business references and professional associations.

Conveyance Security

Conveyance (tractor and trailer) integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material. Conveyance security procedures should include the physical examination of all readily accessible areas, securing all internal/external compartments and panels, and procedures for reporting cases in which unmanifested or non-reported material, or signs of tampering are discovered.

Physical Access Controls

Access controls prevent unauthorized entry to trucks, trailers and facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, service providers, and vendors at all points of entry. Employees and service providers should only have access to those areas of a facility where they have legitimate business.

Personnel Security

Written and verifiable processes must be in place to screen prospective employees and to periodically check current employees including:

- Pre-Employment Verification
- Background Checks/Investigations
- Personnel Termination Procedures

Procedural Security

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 supply chain. Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to the conveyance including concealment in trailers. Procedures must include a system for verifying seals on containers and trailers as well as a system for detecting and reporting overages and shortages.

Physical Security

Procedures must be in place to prevent, detect, or deter unmanifested material and unauthorized personnel from gaining access to conveyance, including concealment in trailers. Cargo handling and storage facilities, trailer yards, etc., must have physical barriers and deterrents that guard against unauthorized access.

Security Training and Threat Awareness

A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by drug smugglers and terrorists at each point in the supply chain. Employees must be made aware of the procedures the highway carrier has in place to address a situation and how to report it.

Information & Technology Security

Measures should be taken to protect electronic assets, including advising employees of the need to protect passwords and computer access. A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. Transponders or any technology provided to the highway carrier by U.S. Customs and Border Protection to utilize the Free and Secure Trade (FAST) program must be protected against misuse, compromise, theft, tampering, altering or duplication.