

General Operating Instructions (GOI)

Section 11

Security

TABLE OF CONTENTS

1.0	General Security	150
2.0	Security Alert Levels	150
3.0	Suspicious Objects	150
4.0	Persons on CP Property	151
5.0	Persons Riding Trains	151
6.0	Employee Identification	151
7.0	Disclosure of Sensitive Information	152
8.0	Border Crossing	152

1.0 General Security

1.1 Train crews must immediately report to the RTC or CP Police any security concern, security incident, criminal activity (known or suspected), suspicious activities, suspicious persons on or near Company property, and any other near miss or possible security threats. They should also be alert for signs of theft or vandalism of critical safety devices.

Note: More information on CP's Security Plan and Programs can be found on **RailCity**.

CP Police Communication Centre

1 – 800 – 716 – 9132

2.0 Security Alert Levels

2.1 CP's security program has 4 Alert Levels which incorporates all actions from the preceding levels:

- Level 1 – Normal Day-to-Day Operations
- Level 2 – Heightened Security Awareness
- Level 3 – Credible Threat
- Level 4 – Confirmed Threat

If there is a reason to change CP's Alert Level, RTC's will receive specific information on actions to be taken. Train crews will receive instructions by bulletin and/or from the RTC.

2.2 At Alert Level 3, Alert Trains will be identified, and the RTC notified of their status. The **RTC** must confirm the location of all Alert Trains in dark territory on a regular basis, at least every 60 minutes, and record this information.

ALERT TRAINS are trains carrying certain Dangerous Goods. The message "This is an Alert Train" will appear on the train consist in the header message area. Alternatively, you may be notified by the RTC while en-route that your train is an Alert Train.

2.3 At Alert Level 3, train crews must notify the RTC immediately of unusual or unexpected stops (e.g.: red signals, defect detectors, undesired brake emergencies, etc.), BEFORE they exit the locomotive for any reason, including to inspect the train. While occupied, locomotive cab doors should be kept locked.

3.0 Suspicious Objects

3.1 Employees should be alert for any suspicious or dangerous objects on trains or CP property, including items which may be attached to or adjacent to tracks, switches, signals, or on the right-of-way.

These objects can come in many different forms and may appear ordinary. Examples of what to look for are:

- Unusual items, such as Improvised Explosive Devices (IED), on or attached to cars, especially placarded tank cars.
- Apparent signs of tampering, sabotage, contraband or other unusual or prohibited items
- Loaded cars with broken door seals and/or partially open doors
- Hidden or abandoned bags, boxes or parcels,
- Objects emitting an unusual sound, odour, mist, gas or vapour.

3.2 Remote Monitoring Equipment (RME), such as GPS (Global Positioning System) devices are commonly being installed on highway trailers, railroad freight & tank cars and are not dangerous objects. Per AAR Standard S-2045, they are:

- Identified by a sticker, label or stencil:
 - At least 2" X 3"
 - In a highly visible bright yellow or orange with black lettering
 - Located within 12 inches of the sensor
 - With information describing the device indicating it's function and providing a phone number for information related to the device.
- Located in various locations on rail cars.
- Identified in UMLER if the RME is permanently mounted

3.3 If a suspicious object is found:

1	Do not attempt to move or touch it.
2	Stay clear of the area and keep others clear of the area.
3	If the object is a possible explosive: <ul style="list-style-type: none"> do not use your radio or cellular phone unless you are at least 300 feet away from the object, and instruct all personnel to evacuate the area.
4	Take note of any suspicious vehicles or people in the area
5	Immediately notify the RTC, your supervisor, or CP Police.

3.4 Definitions:

Improvised Explosive Device (IED) – is a device fabricated in an improvised manner incorporating explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design. This device generally includes a power supply, a switch or time, and a detonator or initiator.

Remote Monitoring Equipment (RME) applies to any device applied to a railcar or its lading that transmits a signal or records data that can be received by a remote receiver or retrieved at a later time by a carrier, shipper or other entity.

4.0 Persons on CP Property

Note: Employees should not approach or confront unknown persons on or near CP property or railway tracks if they appear threatening, upset, depressed, or intoxicated. Reasonable efforts should be made to keep them under observation from a safe distance until CP or local police can respond. Do not place yourself at risk. If you feel threatened back off and call the police.

3.1 Remain alert for:

- Individuals illegally riding in locomotives and on trains
- Strangers or visitors on CP property.

3.2 If it is safe, approach strangers or visitors on the property and determine if they have a business need to be there. Check credentials and photo ID for individuals, including those identifying

themselves as working for any government agency such as Transport Canada, or the Transportation Safety Board.

3.2 Immediately, report any suspicious or unauthorized people to the RTC, your Supervisor or CP Police who can arrange to have them escorted off the property. Be prepared to provide details such as descriptions of the individual and/ or vehicles.

5.0 Persons Riding Trains

5.1 The conductor or other employee in charge must immediately report to the RTC whenever there are other persons riding in locomotives or other non-passenger rail equipment, excluding assigned crew members and managers / supervisors performing their duties.

Managers must notify the Corridor Manager NMC, when they will be riding.

5.2 This report should identify the individual(s) name and what authorization they have for accompanying the train or equipment, including:

- a company employee who is performing normal duties and has company ID
- a company employee who possesses a signed access pass and has company ID
- a non-employee who possesses a signed pass, photo ID and has completed a liability waiver form.

5.3 If there are unauthorized persons riding on the train, the train crew should:

- not proceed, or stop at the next available location, AND
- notify the RTC or CP Police.

6.0 Employee Identification

Employee identification cards are issued to all CP employees.

Employee identification cards include the employee’s name, employee number and a phone number that can be used to confirm employment or obtain emergency contact information. The cards must be signed and carried along with valid photo ID by all employees on duty, and both pieces of identification must be presented for on-demand checks by a Company officer or by a customer while at a customer site. The employee identification cards do not replace location-

specific access cards which must continue to be used as well.

Employee identification cards are non-transferable, and are the responsibility of each employee. If an employee's card is incorrect, irreparably damaged, lost or stolen, the employee must contact the Human Resources Service Centre at 1-866-319-3900 (CAN) or 1-800-234-0013 (US) to arrange replacement. These contact numbers, or HR Self Service on RailCity, must also be used to ensure emergency contact information is up-to-date.

7.0 Disclosure of Sensitive Information

- 7.1 Be aware of personal conversations with others off the property concerning your job and workplace. Unusual interest in technical details should be reported to your supervisor and CP Police.
- 7.2 The heightened need for increased public security and for terrorist threat countermeasure planning by emergency responders has resulted in an increase in requests for information about our railway operations. Much of the attention is focused on the transportation of dangerous goods.

Anyone receiving a request for dangerous goods information or other suspicious questions regarding rail operations or critical infrastructures should ascertain as much detail as possible about the individual making the request, the organization he or she represents, and the intended use of any material that we might supply. Forward all such requests to the Public Affairs Department for co-ordination of the appropriate response.

NOTE: All CP employees are prohibited from providing any outside third party with information regarding dangerous goods movements, routing, volumes or storage.

8.0 Border Crossing

- 8.1 All employees crossing the border must comply with all requirements and requests from both the U.S. Customs and Border Patrol and Customs and Immigration Canada officials.

Unless otherwise instructed, you must check in with border officials each time you cross, regardless of why or the duration. It is illegal to cross the border with firearms, explosives, drugs, other banned substances or goods that may be subject to any form of import duty.