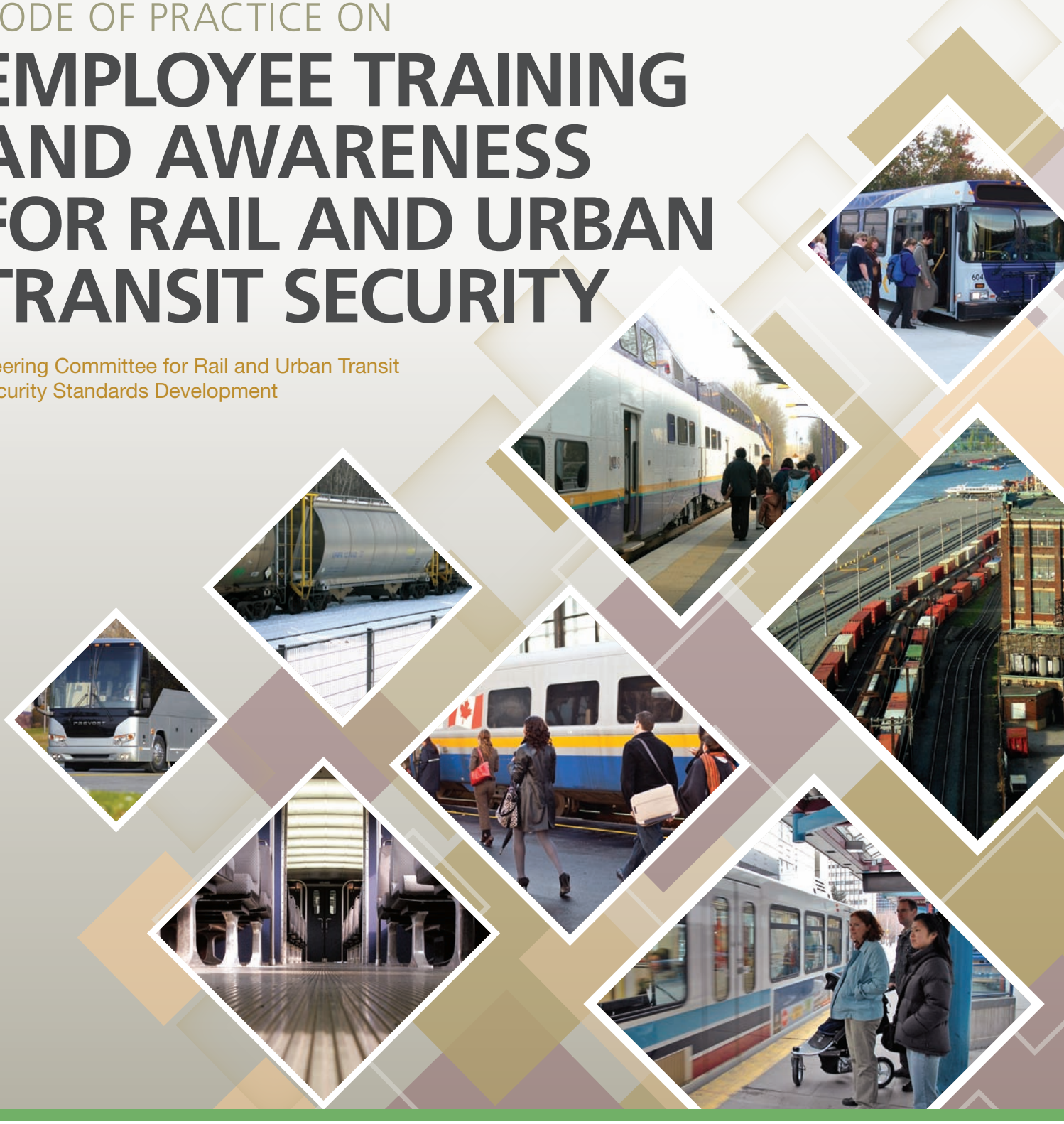
Transport Canada Transports Canada

TP 15121

CODE OF PRACTICE ON

EMPLOYEE TRAINING AND AWARENESS FOR RAIL AND URBAN TRANSIT SECURITY

Steering Committee for Rail and Urban Transit Security Standards Development



Canada

Preface

This Code of Practice is intended to assist rail and transit operators develop security training and awareness programs. The Code is one of a series being developed by Transport Canada, with support from rail and transit industry leaders and their primary associations (i.e., the Railway Association of Canada and the Canadian Urban Transit Association), via the industry-led Steering Committee for Rail and Urban Transit Security Standards Development. The material contained in these Codes of Practice is based on industry best practices, is for information only, is not exhaustive and is intended for voluntary adoption by all rail transit operators in Canada. Where applicable regulations exist, those regulations take precedence over the guidance material contained herein.

Canada shall not be held liable for any injury, including death, or for any loss or damage to property incurred or suffered in carrying out recommended actions set out in this guidance material.

For more information regarding this Code, or any other product of the Steering Committee, please contact Transport Canada or your industry association at the coordinates provided below.

Transport Canada
Surface and Intermodal Security Directorate (ABS)
330 Sparks Street
Place de Ville Tower C
Ottawa, ON, Canada, K1A 0N5
Tel: 613-998-6623 Fax: 613-990-2015
E-mail: sims-stti@tc.gc.ca
Website: http://www.tc.gc.ca/

Canadian Urban Transit Association
55 York Street, Suite 1401
Toronto, ON, Canada M5J 1R7
Tel: 416-365-9800 Fax: 416-365-1295
E-mail: communications@cutaactu.ca
Website: http://www.cutaactu.ca/

Railway Association of Canada
99 Bank Street, Suite 901
Ottawa, ON, Canada K1P 6B9
Tel: 613-567-8591 Fax: 613-567-6726
E-mail: rac@railcan.ca
Website: http://www.railcan.ca/

Acknowledgements

Transport Canada wishes to express sincere appreciation to the following organizations for their cooperation and contribution to this document as members or partners of the Steering Committee:

AMT – Agence métropolitaine de transport
Calgary Transit
Canadian National
Canadian Pacific
Canadian Urban Transit Association
Edmonton Transit System
GO Transit
Greyhound Canada
OC Transpo
Railway Association of Canada
STM – Société de transport de Montréal
South Coast British Columbia Transportation Authority (TransLink)
Toronto Transit Commission
VIA Rail Canada

TP 15121

Catalogue No. T33-26/2011E-PDF
ISBN: 978-1-100-18117-2

For additional copies of this publication, please visit http://transact-en.tc.gc.ca or contact Transport Canada's Publications Order Desk at 1-888-830-4911 — International at 613-991-4071.

For an accessible version of this publication, please contact Transport Canada's Publications Order Desk at 1-888-830-4911 — International at 613-991-4071.

An electronic version of this publication is available at http://transact-en.tc.gc.ca.

Table of Contents

1. Introduction 1

What is a Code of Practice (COP)? 1
Purpose, Scope and Benefits 1
How Operators Should Use this Code of Practice 1
What is Security Awareness? 2
What is Security Training? 2

2. Planning and Developing Security Training and Awareness Programs 3

Security Training and Awareness Objectives 3
Key Recommendations 3
Security Training and Awareness Program Development and Resources 4
The Five Phases of Developing a Security Training and Awareness Program 4
Consultations and Relevant Stakeholder Involvement 6

3. Training and Awareness Delivery Methods 7

Ways of Delivering Security Awareness Programming 7
Ways of Delivering Security Training Programming 7

4. Key Messages and Teaching Points for Security Training and Awareness 9

Baseline Security Information 9
Job-specific Security Information 9
Security Training and Awareness Gap Assessment 10
Information for Emergency Responders and Other Relevant Stakeholders 10

5. Management and Accountability 11

Ongoing Management of a Security Training and Awareness Program 11
Frequency 11
Review and Update Process 11
Security Training and Security Awareness Documentation and Records 11
Maintaining Confidentiality 12
Program Evaluation 12

Appendix A 13

Definitions 13

Appendix B 15

Resources 15

Appendix C 17

Security Training and Awareness Gap Assessment Grid 17
Sheet 1: Key Lesson Requirement Form 17
Sheet 2: Key Lesson Gap Analysis Form 22

1. Introduction

What is a Code of Practice (COP)?

A **Code of Practice (COP)** can be defined[1] as a set of recommended or best practices that are:

- Defined by one or more individuals or corporations;
- Designed to influence, shape, or benchmark behaviour; and
- Applied consistently by participants and/or reach a consistent outcome.

This Code of Practice is one of a series being developed by Transport Canada, in partnership with rail and transit industry leaders and their primary associations, the Railway Association of Canada and the Canadian Urban Transit Association, via the industry-led Steering Committee for Rail and Urban Transit Security Standards Development. These Codes of Practice are based on industry and international best practices and are intended for voluntary adoption by all rail and transit operators in Canada.[2]

Purpose, Scope and Benefits

This Code of Practice contains recommendations and guidance for **voluntary** actions. It does not set out mandatory requirements.

Canada's rail and transit systems are extensive, open systems that move high volumes of passengers and goods daily and as such, are targets for various acts of terrorism, crime and disorder. It is important that Canadian rail and transit operators put in place appropriate measures to enhance resilience by preventing, preparing for, responding to and recovering from any potential terrorist or security incident.

Training and awareness are key elements of an effective security program. Training and awareness programming is aimed at ensuring that all employees, contractors and relevant stakeholders are familiar with, and able to carry out the security responsibilities associated with their positions.

Training and awareness programming also contributes to the development of a strong security culture, where every employee understands and accepts their responsibility to enhance the system's security and security is integrated into an operator's day-to-day activities. A strong security culture helps to improve the security of both the operator's transportation network and Canada's rail and transit systems as a whole.

The purpose of this Code is to provide operators with guidance for developing training and awareness programs for their employees, contractors and relevant stakeholders based on the operator's security requirements (as determined by their Security Risk Assessment) and measures (as set out in their Security Plan). It also establishes a baseline of recommended best practices for various elements of an effective training and awareness program (e.g., frequency of training, record keeping, etc.).

How Operators Should Use this Code of Practice

Rail and transit operators of all sizes are encouraged to use this Code of Practice as a reference guide when developing security training and awareness programs for their organization. Operators may adapt aspects of the Code to best suit their particular security and operational needs.

1 For more definitions, please refer to Appendix A.

2 For details on other Codes available please contact Transport Canada, the Railway Association of Canada or the Canadian Urban Transit Association (see Preface for contact information).

What is Security Awareness?

Security awareness, for the purpose of this Code of Practice, refers to engaging employees, contractors and relevant stakeholders to make them more aware of their security roles and responsibilities in relation to security matters. This includes increasing their awareness of their surroundings and familiarity with security issues (e.g., the network's threat environment) and procedures (e.g., observing and reporting suspicious behaviour) and conveying basic information as to how employees, contractors and relevant stakeholders should respond to such situations. The goal of raising awareness is to reduce the risks, related to terrorist attacks or other security issues (e.g., crime and disorder).

What is Security Training?

Although some overlap exists between security training and security awareness, training typically fleshes out components included in security awareness campaigns and targets employees. Training involves increasing employees' familiarity with security issues, conveying specific information as to how to respond to these issues, teaching employees how to carry out specific tasks related to security and evaluating whether the information has been understood by those being trained.

2. Planning and Developing Security Training and Awareness Programs

Training and awareness are key elements of an effective security program. When developing a security training and awareness program an operator should identify and briefly describe its program objectives for its employees, contractors and relevant stakeholders.

Security training and awareness programs should be updated periodically to ensure they remain current and effective. Such programs should also include a regular evaluation of their successes, ongoing effectiveness and relevance. In addition, training and awareness programs should reflect operational needs, the operator's security context (as set out in its Security Risk Assessment) and the measures contained in its Security Plan.

A security training and awareness program may be stand-alone or integrated into an operator's other training and awareness programs (e.g., regarding safety). Integrating security training and awareness with existing programs could provide an operator with an efficient way to deliver such programming.

Security Training and Awareness Objectives

The purpose of all security training and awareness programming is to:

- Increase employee, contractor and stakeholder understanding of the potential threats to, and vulnerabilities within, the transportation network and what actions can be taken to eliminate, control, prepare for, or respond to, those threats and vulnerabilities (including to mitigate the impact of a security incident);
- Prepare employees for their security responsibilities;
- Increase the level of familiarity with security issues throughout the organization;
- Reinforce existing security policies and procedures (e.g., the preventive security measures set out in the operator's Security Plan);
- Maximize the involvement of the operator's employees, contractors and relevant stakeholders in the operator's security program;
- Introduce the following concepts: security awareness; prevention, mitigation, response and recovery; and,
- Raise awareness of relevant external stakeholder response plans.

Key Recommendations

A rail or transit operator should:

- Use this Code of Practice when developing its training and awareness program;
- Take into account the availability of resources for developing and implementing such programs; and,
- Evaluate the training and awareness program regularly.

The operator's security training and awareness program should:

- Reflect the guidelines contained in this Code of Practice;
- Be aimed at ensuring that employees, contractors and relevant stakeholders are able to fulfill the security-related responsibilities of their positions;
- Be endorsed by appropriate management;
- Address the security controls set out in the operator's current Security Plan;
- Address both initial security training for new employees and refresher training for existing employees;
- Outline the frequency of refresher security training (e.g., every three years) and security awareness programming (e.g., when new messages and/or objectives are developed);
- Respond to requirements for added security training and security awareness programming, for example when:
  - New equipment, materials, or processes are introduced;
  - Security controls set out in the Security Plan or operating procedures have been updated or revised; or,
  - Exercises or incidents demonstrate that an employee's performance does not meet the desired level of readiness;

- Provide evaluation benchmarks to gauge participants' understanding once training is completed; and,
- Prescribe that records of all training, evaluations, and assessments conducted be kept.

Security Training and Awareness Program Development and Resources

Ideally, operators should develop, design and deliver security training and awareness programs that are relevant to their needs and reflect the availability of the operators' resources for developing and implementing such programs. A number of resources are available both domestically and internationally to facilitate the development of awareness sessions within an organization.

If the option of developing programs within the organization is not available, using security training and awareness programs from outside the organization is the best alternative. When choosing an external supplier for training or awareness programming, it is crucial that the operator consider the supplier's qualifications and experience. For convenience, links to additional resources on training and awareness are provided in Appendix B.

The Five Phases of Developing a Security Training and Awareness Program

Security training and awareness programs should, in general, be developed and conducted using a five-phase cycle:

1. Identifying needs and objectives;
2. Designing and developing the program;
3. Delivering the program;
4. Evaluating the program; and
5. Planning and implementing program improvements using the evaluation results.

As each phase informs and is linked to the phase that follows it, there is some degree of overlap between them. Each of these phases is briefly described below.

Phase One – Identifying Needs and Objectives
The first step in developing a security training and awareness program is to determine what training and awareness is required to ensure that employees are able to fulfill their security-related responsibilities. To do this, an operator should conduct a needs assessment, for example by:

a) Doing a security training and awareness gap analysis:

- Reviewing its Security Risk Assessment to ensure it is familiar with the risks and vulnerabilities facing its network;
- Reviewing its Security Plans, policies, procedures to identify the security related roles, responsibilities and tasks employees and contractors are expected to fulfill to mitigate the vulnerabilities and impacts identified in its Security Risk Assessment (see Section 4 for additional information); and,
- Reviewing its existing training and awareness programs (if any) to identify any gaps between the training and awareness employees and contractors currently receive and the security related tasks and responsibilities they are expected to fulfill.

b) Conducting a performance review to identify potential training or awareness shortcomings:

- Reviewing reports on security exercises or incidents to identify any shortcomings in employees' or contractors' performance during those accidents or incidents (e.g., did they fulfill their security-related roles and responsibilities); and,
- Reviewing security training and awareness records of the employees and contractors involved in those exercises or incidents to determine if there is a link between any identified performance shortcomings and the security training and awareness that those employees and contractors had received.

The results of the needs assessment is then used to establish objectives for the security training and awareness program. These objectives provide a framework for developing the program and serve as the basis for the evaluation criteria used to assess the program.

Appendix C contains a **Security Training and Awareness Gap Assessment Grid** to help operators evaluate their training and awareness needs and gaps.

Phase Two – Designing and Developing the Program
The design of an operator's training and awareness program should reflect the needs and objectives identified in Phase One. The design and development process should generally consist of the following tasks:

- Assembling a planning team;
- Developing training material and documentation;
- Identifying employees needing training and awareness and the relevant training to be provided;
- Determining what training or awareness information, if any, contractors, visitors and others accessing the operator's property need;
- Scheduling training and awareness sessions;
- Budgeting for training and awareness sessions;
- Developing assessment criteria and a method to confirm the effectiveness of the training received;
- Developing a method to track courses offered, participant attendance, frequency of refresher training courses, etc.;
- Identifying the training and awareness delivery methods that will be used;
- Identifying service providers if training and awareness is outsourced; and,
- Identifying an evaluation criteria and methodology for the training and awareness program.

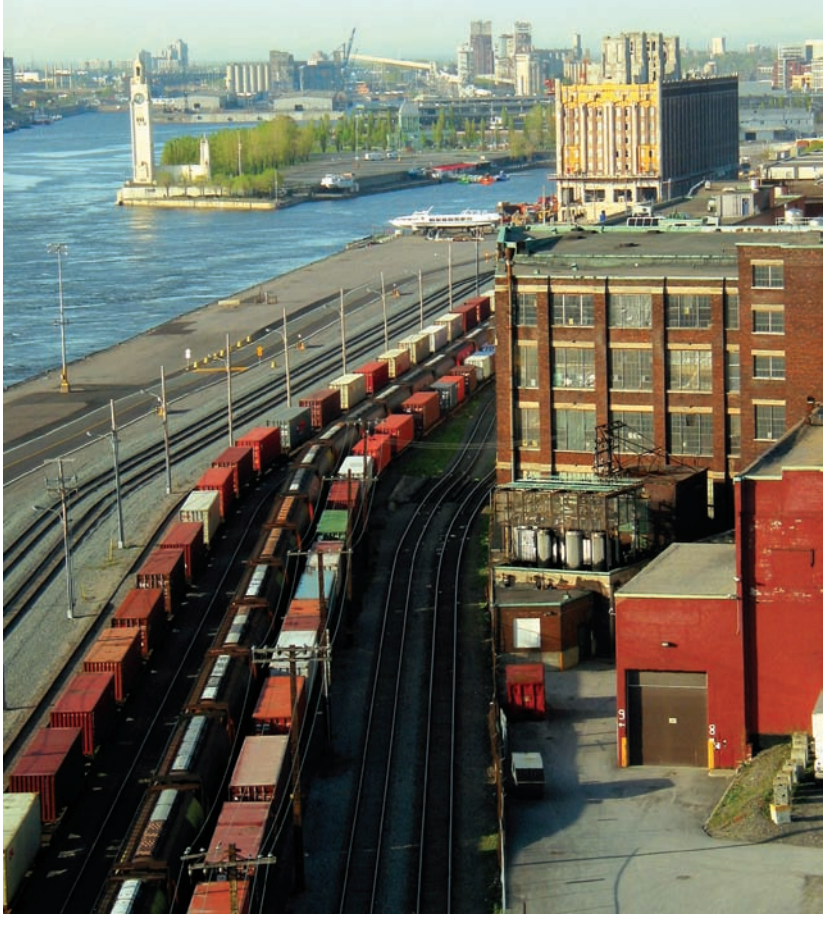
Phase Three – Delivering the Program
Once the security training and awareness programming has been developed, delivery may take place using a variety of formats. Please refer to Section 3 of this Code for some options. An operator may wish to consider integrating its security training and awareness program with existing training and awareness programs in order to benefit from investments previously made in those programs.

Phase Four – Evaluating Training and Awareness
Security training or awareness programs should include an application component (e.g., via an exercise or test) to provide relevant employees the opportunity to "learn by doing". This will help employees understand their security responsibilities more thoroughly and help operators verify employees' familiarity with the content of the security training or awareness material received.

Using the evaluation criteria created in Phase Two, operators should periodically evaluate the results of their security training or awareness program to see if objectives were met. Lessons learned while delivering their training and awareness programming should be exploited to improve program effectiveness and inform the next iteration of the program-planning phase.

Phase Five – Planning and Implementing Program Improvements

After evaluating the results of the security training or awareness program, operators should determine how they will address shortcomings and build on successes. Operators should use the evaluation criteria to determine which training or awareness competencies require improvement. This information would feed into an improvement plan.



Consultations and Relevant Stakeholder Involvement

When developing security training or awareness programs, an operator should consult with relevant stakeholders, which could include:

- Employees (including security staff, front line service providers and equipment operations employees);
- Law enforcement and intelligence officials;
- Emergency responders;
- Companies contracted to provide security services for the operator;
- Transportation Security Inspectors;
- Experts and/or safety/security inspectors of provincial or territorial transportation departments concerned, if any;
- Operators of interconnected transportation systems;
- Relevant industry associations;
- Managers of facilities (e.g., stations) used, occupied or shared; and
- Individuals/organizations with whom the operator shares a facility (e.g., tenants, user groups).

Such consultations should help the operator develop security training and security awareness material that promotes interoperability with its stakeholders.

3. Training and Awareness Delivery Methods

When selecting a delivery method for either security training or security awareness, consideration should be given to factors such as: the availability of internal resources, objectives, costs, participants, frequency, geography and the nature of messages (e.g., detailed procedures vs. basic information). There are many delivery methods available to operators, several of which are described in the following sections.

Regardless of the delivery method that is selected, operators should seek to incorporate their success stories and other positive examples into their security training and awareness programming. Such examples help to:

- Validate the effectiveness of the operator's security program by showing employees that the operator's security controls work; and,
- Demonstrate to employees that they play an integral role in keeping the operator's transportation network secure.

Ways of Delivering Security Awareness Programming

Orientation sessions
An orientation session serves to introduce employees to their working environment and outlines their responsibilities. Such sessions usually take place at the beginning of the employee's employment period.

Videos
Videos provide a learning tool for participants. Videos can be used as a primary medium for raising awareness.

Printed Material
Printed material such as posters, fliers, or newsletters may serve as primary awareness raising techniques. It is easy to create and distribute printed material to employees; however, these materials should be clear and all messaging should be well communicated.

Ways of Delivering Security Training Programming

On-the-Job Training
On-the-job training (OJT) is a common means of training or retraining workers and requires more thought and preparation than simply having someone follow an experienced worker around and watch what they are doing. It is only through planning a structured OJT program that consistency can be created and maintained. To establish a structured program, a plan must be developed regarding issues such as who will conduct the training, what material will be covered, and how long training will last. In addition, the following topics should be considered:

- Selecting and preparing OJT trainers/coaches;
- Working with supervisors for successful implementation;
- Developing and/or selecting training materials;
- Setting trainee prerequisites;
- Evaluating performance;
- Granting company certification to trainers/coaches and trainees; and,
- Evaluating the program.

It is important to have some system in place to determine whether trainees have gained the knowledge and skills required to do the new job. Such a system should be thorough enough to gauge trainee success accurately, but not too cumbersome to use with ease. One method is to design checklists including each important task and/or subtask that should be reviewed. Checklists can be compiled while training content is being defined. It can be used as a guide to key points to be made during training, as well as an evaluation tool as training progresses.

Classroom Instruction
Classroom style training typically involves a combination of lecture, participant discussion and facilitation of practical exercises and activities to reinforce new and existing concepts and skills. This training medium provides training that can be easily modified for the target audience in order to increase its relevance. It allows participants instant feedback to their questions, as well as the opportunity to learn from peers.

Computer-Based Training (CBT)
Computer-based training is an e-learning program uploaded to the computer that individual employees can complete at their own pace and at any time. It usually provides activities meant to provide content knowledge.

Workshops
Workshops are classroom-style training with scenario-based activities and hands-on skill enhancement exercises. Workshops tend to be clearly focused on a particular topic and may last a few days.

Videos
Videos can be used to supplement or enhance other forms of security training delivery methods previously described.

4. Key Messages and Teaching Points for Security Training and Awareness

In general, there are two categories of information that should be included in any security training and awareness program:

- **Baseline security information** that should be provided to all employees; and,
- **Job-specific security information** that should be tailored for, and delivered to, particular employee groups (e.g., employees that deal with the public).

When developing its security training and awareness program, an operator should determine what mix of training and awareness programming is required to transmit the baseline and job-specific security information and ensure that employees are able to fulfill their security-related responsibilities. When deciding on this mix, however, it is important to remember that awareness programming seeks to increase an employee's familiarity with security issues and practices, while training builds on awareness principles and instructs employees on how to carry out their assigned security tasks.

Baseline Security Information

At a minimum, an operator should provide all of its employees with the following messages and information via its security training and awareness program:

General Messages

- Security is everyone's business; all employees contribute to an organization's security;
- Following the operator's security policies and procedures (e.g., identification, access control, etc.) is important and helps to protect the lives and livelihoods of employees, customers and the public;
- It is crucial that employees be aware of and familiar with:
  - The potential threat scenarios facing the network as well as its current threat level; and
  - Their surroundings and watch for potential security threats (e.g., by acting as "eyes and ears" in the field).

Roles and Responsibilities

- The employee's own security related responsibilities;
- The employee's role in relation to contractors, visitors and other external parties (e.g., escorting them in secure areas, providing them with security briefings, challenging their right to access secure areas); and
- The employee's role in relation to coordination of security activities (e.g., public announcements, evacuations, etc.).

Detecting, Reporting and Responding

- How to **detect** and identify:
  - Potential security threats (e.g., unauthorized persons in restricted areas);
  - Suspicious behaviour (e.g., terrorist pre-attack indicators) and articles (e.g., using the HOT principle – Hidden, Obviously suspicious, not Typical); and,
  - Security incidents.
- How to **report** on security threats, suspicious behaviour or articles and security incidents, including:
  - Who to contact and how to contact them (e.g., using emergency hotlines);
  - What key information should be reported (e.g., the Who, What, Where, When, Why, and How and the details of persons, objects or vehicles involved).
- How to **respond** to potential security threats, suspicious behaviour or articles and security incidents, for example:
  - Following emergency response procedures, including with respect to: evacuating and exit points; using emergency equipment; isolating dangerous areas; and, seeking assistance.

Job-specific Security Information

In addition to baseline security information, certain categories of employees likely require additional security information that is tailored to their particular roles, responsibilities, location or environment. For example, the security responsibilities of a

train or bus operator could differ from those of a mechanic, office-worker or security official. In the latter case, a security official might require training to carry out tasks such as:

- Security sweeps and inspections;
- Perimeter checks;
- Surveillance;
- Security response; and,
- Access control.

Security Training and Awareness Gap Assessment

When developing or evaluating its security training and awareness program, an operator should determine what types of security information its various categories of employees require (e.g., via a needs assessment and gap analysis process), and what mix of training or awareness programming is required to ensure that they are able to fulfill their security-related responsibilities.

When performing a gap assessment an operator should:

- Identify its various employee categories (and other audiences) and list potential teaching points for each category.
- Assess:
  - Whether potential teaching points are required for employees in that category to fulfill their security-related roles and responsibilities;
  - Whether that teaching point is already being met via its existing security training and awareness program, and if so, via what delivery method(s) (e.g., classroom instruction and orientation sessions);
  - Whether an information gap exists; and,
  - What security training and awareness delivery method(s) the operator intends to use to address that gap (e.g., on-the-job training and printed materials).

Appendix C contains a **Security Training and Awareness Gap Assessment Grid** to help operators with this task.

Information for Emergency Responders and Other Relevant Stakeholders

When developing its security training and awareness program, an operator should determine what types of security information it needs to provide local emergency responders (e.g., fire and police services) and other stakeholders (e.g., other operators with interlinking systems), and what mix of delivery methods will be used to do so. At a minimum, an operator should seek to familiarize local emergency responders and key stakeholders with select components of its Security Plan, including: its operating environment(s) and related safety hazards; its facilities; and its equipment functions.

5. Management and Accountability

Ongoing Management of a Security Training and Awareness Program

The operator should designate one or more individuals to be responsible for:

- Developing, reviewing and updating the security training and awareness program;
- Determining how the security training and awareness program fits within the organization's security planning activities;
- Managing the implementation of the security training and awareness program;
- Evaluating the effectiveness of the security training and security awareness program; and,
- Ensuring appropriate management is involved in, and endorses, the training and security awareness program.

Frequency

Initial Training and Awareness for New Employees
New employees, regardless of their security responsibilities, should receive basic security training or awareness programming as soon as practicable and preferably:

- Within 90 days of commencing employment; or,
- Prior to taking up any duties with security implications, should this exceed 90 days (e.g., no access to security-sensitive documents without the adequate training).

Training for Employees
All employees with security responsibilities should be trained appropriately prior to assuming their security-related responsibilities.

Ongoing Training and Awareness
Security training should be refreshed on a regular basis. The operator should set out a training schedule for each training program (e.g., security personnel shall undergo refresher training annually). Awareness information needs to be updated and presented to employees as necessary to ensure that employees are familiar with the operator's key security messages (e.g., how to identify and report on security threats or incidents).

In addition, all employees should receive additional training as required to ensure skills and competencies remain sufficient for carrying out their security responsibilities, as outlined in the most up-to-date version of the operator's Security Plan (e.g., to account for changes in procedures, etc.)

If concerns/issues have been raised or identified with regards to employee competencies, operators should determine what additional training might be required and the appropriate frequency of such training by using techniques such as: gap analysis; skill or knowledge testing; or, other forms of assessments.

Review and Update Process

An operator should review and, if necessary, modify its security training and awareness program as required, to reflect changes in its operations or Security Plan. This will ensure messages and lessons reflect the operator's changing security environment, operations, capabilities and risk context and ensure its training and awareness program remain relevant.

Security Training and Security Awareness Documentation and Records

Both security training and awareness programs should be clearly documented and conveyed to those responsible for implementing the programs. Security training and awareness reference materials such as guides, handbooks, laminated reference cards, or checklists should be made available or provided to employees as required.

Operators should maintain records of their security training and awareness program.

Training records should include the following details:

- Name of employee/contractor;
- Type of training and title of course;
- Training objectives;
- Date and location of training;
- Name of trainer; and,
- Evidence of employee/security contractors' understanding.

Awareness records should include the following:

- Communication/delivery method used;
- The dates when the awareness information was delivered;
- A sample of the awareness information provided (e.g., if a flyer was used), or a description of the information provided (e.g., if an oral briefing was used); and,
- A description or list of the audience(s) that received the awareness information (e.g., all employees, employees that interact with the public, etc.).

The importance of tracking the delivery of security training and awareness (e.g., by keeping records in an archive) cannot be overemphasized. Tracking security training and awareness delivery has several key benefits:

- It helps create a culture of accountability;
- It enables operators to follow and evaluate employee performance;
- It helps operators to assess the actions it took during an exercise or incident (e.g., to determine whether existing training and awareness programs were sufficient).

Records of training and awareness programs should be held for a period as prescribed by law, or for a minimum of six (6) years to allow for adequate training program reviews. The operator's record-keeping and document tracking procedure should be referenced in the operator's Security Plan.

Maintaining Confidentiality

All documentation produced for the purposes of training and awareness should be reviewed to determine its security-sensitivity, and handled in accordance with the operator's document classification policy.[3]

The following document control steps are recommended for documents deemed to be security-sensitive:

- All copies of relevant documents should be stored in a secure location; and,
- Each operator should determine who "needs to know" about these materials such as appropriate management and those responsible for implementing training and awareness sessions.

Program Evaluation

The operator's security training and awareness program should be evaluated to confirm its effectiveness. It is recommended that evaluation take place every three years.

Examples of baseline measures that could help evaluate the effectiveness and relevance of the security training and awareness provided to employees without specific security duties, consist of the following:

- Employees can define suspicious behaviour and know what to do when suspicious behaviour is identified;
- Employees can define suspicious objects and know what to do when suspicious objects are identified; and,
- Employees know how to report an incident or suspicious behaviour or objects.

Each employee with specific security duties should be able to describe or demonstrate how to conduct these as per the operator's standard operating procedures.

3 Refer to section 1.3.10 of the Code of Practice on Security Plans for more information on maintaining the confidentiality of security-sensitive documents.

Appendix A

Definitions

Attack – A malicious action with the intent of inflicting harm or damage upon a system, such as critical infrastructure to destroy or incapacitate.

Mitigation and Prevention – To eliminate or reduce the impacts and risks of hazards through pro-active measures taken before an emergency or disaster occurs, for example threat risk assessment, personnel security, public education and protective structures such as target hardening. Prevention and mitigation may be considered independently or one may include the other.

Recovery – Actions taken after a security incident to repair or restore conditions to a functional level. Examples of such actions include: business continuity planning; managing network closure and pre-planning reopening of transport network; pre-planned response co-ordination; and roles and responsibilities.

Response – Actions during or immediately after a security incident to manage its consequences. Examples of such actions include: emergency public communication; search and rescue; emergency medical assistance; and evacuation to minimize suffering and losses.

Risk – The likelihood of injury or loss measured as a function of threat, consequence, and vulnerability (R=T x C x V). Indicates likelihood of adverse effect on health, property, the environment or other things of value.

Security Awareness – Refers to engaging employees, contractors and relevant stakeholders to become more aware of their surroundings while working/using the operator's transportation network. This implies increasing their familiarity with security issues (e.g., observing and reporting suspicious behaviour) and conveying basic information as to the manner employees and the riding public are to respond to such situations. The goal of raising awareness consists of reducing the risk of terrorist attacks, other criminal activity or safety concerns.

Security Incident – An event that could have or has resulted in death, injury, significant property damage or serious disruption to operations, works or equipment as a result of an intentional act by a person or persons.

Security Plan – A strategic and confidential document that:

- Sets security goals and objectives based on a security threat risk assessment (SRA);
- Establishes a framework, reflecting the full security "spectrum" (Prevention, Mitigation, Response and Recovery), for addressing security threats and risks;
- Reflects a coordinated approach to the security of an operator's system that integrates available resources to provide enhanced protection from potential security incidents;
- Identifies key assets that require protection;
- Sets out the measures to be implemented to address risks identified in a SRA, including mitigation measures applicable at each alert level (e.g., low, medium, high);
- Clearly identifies related plans (e.g., Emergency Management, and Business Recovery Plan) procedures, protocols and responsibilities to complete a security program;
- Identifies an action plan to introduce measures that are required to address priority risks (interim and long-term measures); and,
- Gives full consideration to actions or resources required to support the implementation of the measures it contains (e.g., training, IT requirements, documentation).

Security Training – Training involves increasing employees' familiarity with security issues, conveying specific information as to how to respond to these issues, training employees on how to carry out specific tasks related to security and evaluating whether the information has been understood by those being trained. Although some overlap exists between security training and security awareness, training typically fleshes out components included in security awareness campaigns and targets employees.

Suspicious Behaviour – Behaviour that causes increased suspicion. Increased suspicion is more than a hunch, but less than reasonable suspicion required to detain a person or group. It should be noted that increased suspicion should be based on suspicious behaviour and not profiling.

Suspicious Incidents – A **verified suspicious incident** is one that has been investigated by operator security staff or law enforcement and confirmed as being a possible indicator of terrorist activity. An **unverified suspicious incident** is one that has been reported, but has not been investigated, or has been investigated but no conclusion was reached about whether it represented a possible indicator of terrorist activity.

Terrorist Activity – An act that is committed in whole or in part for a political, religious or ideological purpose, objective or cause, with the intention of intimidating the public (with regard to its security), or compelling a person/government/organization to do or to refrain from doing any act, by intentionally causing death or serious bodily harm to persons by the use of violence, causing serious risk to the health or safety of the public, causing substantial property damage, or interference/disruption of an essential service/facility/system, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in harm (Synopsis of a definition from the *Anti-Terrorism Act*).

Threat – The likelihood or probability of a terrorist activity taking place that could cause mass casualties, damage to critical assets or operational disruption. Canada's intelligence community usually measures threat by assessing the intent and capability of individuals or groups to carry out an attack.

Appendix B

Please note that these resources are included for information only. Except for the Transport Canada Codes of Practice, these resources have not been reviewed nor endorsed by the Steering Committee for Rail and Urban Transit Security Standards Development.

Resources

Canadian Resources:
Canadian Emergency Management College
http://www.publicsafety.gc.ca/prg/em/cemc/index-eng.aspx

Canadian Police Knowledge Network
http://www.cpkn.ca/

CBRNE First Responder Training Program –
Public Safety Canada:
http://www.publicsafety.gc.ca/prg/em/cemc/04pgc_02-eng.aspx

Federal Association of Security Officials – Training Programs
http://www.faso-afrs.ca/

Government of Canada Security Training and Awareness listing – Treasury Board Secretariat of Canada
http://www.tbs-sct.gc.ca/gs-sg/sectrain_e.asp

IT Security Learning Centre – Communications Security Establishment Canada
http://www.cse-cst.gc.ca/its-sti/training-formation/index-eng.html

National Security Criminal Investigations Unit - RCMP
http://www.rcmp-grc.gc.ca/nsci-ecsn/nat-secur-eng.htm

Transport Canada's (TC) Rail and Urban Transit Security page:
http://www.tc.gc.ca/eng/railsecurity/pruts-menu.htm

Codes of Practices:
Transport Canada, **Code of Practice on Developing and Maintaining Security Plans For Rail and Transit Operators**, 2009.

Transport Canada, **Code of Practice on Conducting Security Risk Assessments of Rail and Transit Operations**, 2010.

Transport Canada, **Code of Practice on Security Exercises for Rail and Transit Operations**, 2011.

Best Practices by Canadian Transit Operators:
GO Transit
http://www.gotransit.com/publicroot/en/default.aspx

OC Transpo
http://www.octranspo1.com/travel-tips

Société de transport de Montréal (STM)
http://www.stm.info/English/info/a-securite.htm

Toronto Transit Commission (TTC)
http://www3.ttc.ca/Riding_the_TTC/Safety_and_Security/index.jsp

TransLink
http://www.translink.ca/en/Rider-Info/Safety-and-Security.aspx

Union Station
http://www.toronto.ca/union_station/security.htm

American Resources:
American Public Transportation Association (APTA) Standards
http://www.aptastandards.com/

ASIS International – Security Toolkit
http://www.asisonline.org/toolkit/toolkit.xml

Federal Transit Administration (FTA)
http://www.fta.dot.gov/
Calendar of Events:
http://www.fta.dot.gov/news/news_events_415.html

Massachusetts Bay Transportation Authority Transit Police Department
http://mbta.com/transitpolice/

National Institute for Occupational Health and Safety (Worker Training in a New Era: Responding to New Threats)
http://www.cdc.gov/niosh/docs/2004-173/

National Transit Institute
http://www.ntionline.com

Transportation Research Board
http://www.trb.org
TRB Report on Public Transport Security:
http://www.trb.org/publications/tcrp/tcrp_rpt_86v5.pdf

Transportation Security Administration (TSA)
http://www.tsa.gov/

Australian Resources:
Human Factors for Transport Safety Investigators (course)
http://www.atsb.gov.au/about_atsb/training/training.aspx

National Security Public Information Campaign
http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/

National Security Website
http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/

Appendix C: Security Training and Awareness Gap Assessment Grid – *Sheet 1: Key Lesson Requirement Form*

Introduction

Security training and awareness programming should be tailored to an employee's particular roles and responsibilities. In addition to the recommended baseline security information teaching points, this chart provides examples of key lessons that could be transmitted to various employee audiences via the operator's security training and awareness programs. Some of the teaching points listed below could contribute to an operator's safety preparedness as well as its security preparedness. Integrating such teaching points into existing safety or security training and awareness programs could therefore have co-benefits.

How to Use This Form

1. Review the list of audience categories and teaching points and modify as appropriate for your organization.
2. Review the modified list of teaching points and determine whether each teaching point is required for the modified audience categories (i.e., various employee types; contractors; and, other stakeholders, such as law enforcement, operators with connecting services or facility/infrastructure owners).
3. If the teaching point is required for that category of employee (or contractor, etc.) to fulfill their security roles and responsibilities (i.e., as set out in the operator's Security Plan), then the operator inserts a "Y" for "Yes" in the appropriate box. If the teaching point is not required, then the operator inserts an "N" for "No".

NOTE: It is recommended that all categories of employees receive the baseline security information via the operators security training and awareness program. Therefore, "Y"s have already been inserted into those boxes.

4. Use the results to help fill in the Key Lesson Gap Analysis Form.

Key Lessons for Security Training and Awareness Audiences		Employees – General	Employees Who Interact With the Public	Maintenance Employees	Employees – Security Personnel	Management	Contractors	Other Stake-holders/ Group(s)?
Category	**Teaching Point**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**
Baseline security information	1. Security is everybody's business	Y	Y	Y	Y	Y		
	2. Why it is important to follow the operator's security procedures	Y	Y	Y	Y	Y		
	3. The importance of being aware of your surroundings and of watching for potential security threats	Y	Y	Y	Y	Y		
	4. How to **detect** potential security threats, suspicious behaviour or articles and security incidents	Y	Y	Y	Y	Y		
	5. How to **report** potential security threats, suspicious behaviour or articles and security incidents	Y	Y	Y	Y	Y		
	5. A) Who to contact and how to contact them (e.g., using emergency hotlines)	Y	Y	Y	Y	Y		
	5. B) Key information to report when communicating suspicious or actual incidents (e.g., Who, What, Where, When, Why, How)	Y	Y	Y	Y	Y		
	6. How to respond to potential security threats, suspicious behaviour or articles and security incidents	Y	Y	Y	Y	Y		
	6. A) How to follow emergency response procedures, including with respect to: evacuating and exit points; using emergency equipment (e.g., alarm systems, communication devices, etc.); isolating dangerous areas; and, seeking assistance	Y	Y	Y	Y	Y		
	7. Employee's own security-related responsibilities	Y	Y	Y	Y	Y		
	8. Employee's role in relation to contractors, visitors and other external parties (e.g., providing escorts and security briefings, challenging right of access)	Y	Y	Y	Y	Y		
	9. The employee's role in relation to the coordination of security activities (e.g., public announce-ments, evaculation, etc.)	Y	Y	Y	Y	Y		

Key Lessons for Security Training and Awareness Audiences		Employees – General	Employees Who Interact With the Public	Maintenance Employees	Employees – Security Personnel	Management	Contractors	Other Stake-holders/ Group(s)?
Category	**Teaching Point**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**
Job specific information: General Skills	How to deal with victims of crime/ sensitivity training							
	How to deal with difficult customers and various security incidents							
	Tactical communication and conflict resolution strategies							
	How to respond to public reports relating to security concerns							
	Situational assessment (assess, plan, act)							
	Employee specific emergency equipment operations (e.g., duress alarms, communication devices)							
	Incident management basics (e.g., the steps to be taken to secure or cordon off the affected work environment)							
	Security incident/emergency/loss reporting procedures (e.g., who to contact and how)							
	How to document a security incident (e.g., report writing)							
	How to communicate with dis-patcher/rail traffic control on security matters							
Roles and responsibili-ties and program knowledge	Role of local law enforcement							
	Role of operator police/security personnel and how they are organized							
	Role of communications/control centre							
	System Security Plan/Program							
	Associated plans and programs (e.g., Emergency Response Plan/Program; Business Continuity Plan/Program)							
	Roles and responsibilities of emergency responders and the operator's role when interacting/ working with them							

Key Lessons for Security Training and Awareness Audiences		Employees – General	Employees Who Interact With the Public	Maintenance Employees	Employees – Security Personnel	Management	Contractors	Other Stake-holders/ Group(s)?
Category	**Teaching Point**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**
Roles and responsibilities and program knowledge *(continued)*	Roles and responsibilities of employees related to security incidents, employee/customer safety and asset protection							
	Managers' security responsibilities and accountabilities							
	How the operator's security program is coordinated and managed							
	General security/emergency policies and procedures applicable to all employees (e.g., fire evacuation, bomb threat procedures, workplace violence/harassment)							
	How system emergencies are managed (e.g., Emergency Plan, Emergency Operations Centre, Corporate Security Escalation Plan/ Security Alert Levels, role of emergency agencies and first responders)							
	Mechanisms to coordinate activities with relevant stakeholders (e.g., first responders, Municipal and Provincial emergency management, local government, etc.) in the development of Security Plans and management of day-to-day operations and during incidents							
	Organization of operator's security department							
	Interagency coordination, information sharing							
	Regulatory framework							
	Overview of employees' security responsibilities							

Key Lessons for Security Training and Awareness Audiences		Employees – General	Employees Who Interact With the Public	Maintenance Employees	Employees – Security Personnel	Management	Contractors	Other Stake-holders/ Group(s)?
Category	**Teaching Point**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**	**Req'd? (Y/N)**
Procedures	Security/emergency procedures (e.g., regarding: following incident command; suspicious packages; unattended items; bomb threats; fire/ smoke; assaults in progress; fare disputes; disorderly behaviour; evacuation, etc.)							
	How to conduct security inspections and sweeps for suspicious objects and signs of tampering (buses, trains, infrastructure)							
	How to conduct assigned security duties (e.g., perimeter checks, access control, security response)							
	How to conduct assigned law enforcement duties (e.g., suspicious package response)							
	Crime scene management							
	Media relations protocol							
	Crisis management							
	Business continuity procedures							
	Incident command training							

Sheet 2: Key Lesson Gap Analysis Form

How to use this Form:

1. Review the list of audience categories and teaching points and modify as appropriate for your organization.
2. Review the modified list of teaching points and determine whether each teaching point is required for the modified audience categories (i.e., various employee types; contractors; and, other stakeholders/groups, such as law enforcement, operators with connecting services or facility/infrastructure owners).
3. If the teaching point is required for that category of employee (or contractor, etc.) to fulfill their security roles and responsibilities (i.e., as set out in the operator's Security Plan), then the operator inserts a "Y" for "Yes" in the appropriate box of the "Req'd" column. If the teaching point is not required, then the operator inserts an "N" for "No".

NOTE: It is recommended that all categories of employees receive the baseline security information via the operator's security training and awareness program. Therefore, "Y"s have already been inserted into those boxes.

4. Determine whether each required teaching point is already being delivered to that category of employee via the operator's existing security training and awareness program.
   a) If the teaching point is being delivered, then enter a "Y" in the appropriate box of the "Req't met" column and record in the "Gap Analysis" column what delivery mechanism is being used (e.g., classroom instruction, orientation sessions, etc.).
   b) If the teaching point is not being delivered, then enter an "N" in the appropriate box of the "Req't met column" and record in the "Gap Analysis" column what training and awareness delivery method(s) will be used to address the gap (e.g., on-the-job training, printed materials, etc.).

Key Lessons for Security Training and Awareness Audiences		EMPLOYEES – GENERAL			Employees Who Inter-act with the Public			Maintenance Employees			Employees – Security Personnel			Management			Contractors			Other Stakeholders/ Groups?		
Category	Teaching Point	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis
Baseline security information	1. Security is everybody's business	Y		If Requirement Not Met: Indicate what training and awareness method(s) will be used to address the gap (e.g., on-the-job training, printed materials, etc.)	Y			Y			Y			Y								
	2. Why it is important to follow the operator's security procedures	Y			Y			Y			Y			Y								
	3. The importance of being aware of your surroundings and of watching for potential security threats	Y			Y			Y			Y			Y								
	4. How to **detect** potential security threats, suspicious behaviour or articles and security incidents	Y			Y			Y			Y			Y								
	5. How to **report** potential security threats, suspicious behaviour or articles and security incidents	Y			Y			Y			Y			Y								
	5. A) Who to contact and how to contact them (e.g., using emergency hotlines)	Y			Y			Y			Y			Y								
	5. B) Key information to report when communicating suspicious or actual incidents (e.g., Who, What, Where, When, Why, How)	Y			Y			Y			Y			Y								
	6. How to respond to potential security threats, suspicious behaviour or articles and security incidents	Y			Y			Y			Y			Y								
	6. A) How to follow emergency response procedures, including with respect to: evacuating and exit points; using emergency equipment (e.g., alarm systems, communication devices, etc.); isolating dangerous areas; and, seeking assistance	Y			Y			Y			Y			Y								
	7. Employee's own security-related responsibilities	Y			Y			Y			Y			Y								
	8. Employee's role in relation to contractors, visitors and other external parties (e.g., providing escorts and security briefings, challenging right of access)	Y			Y			Y			Y			Y								
	9. The employee's role in relation to the coordination of security activities (e.g., public announcements, evacuation, etc.)	Y			Y			Y			Y			Y								
Job specific information: General Skills	How to deal with victims of crime/sensitivity training																					
	How to deal with difficult customers and various security incidents																					
	Tactical communication and conflict resolution strategies																					
	How to respond to public reports relating to security concerns																					
	Situational assessment (assess, plan, act)																					
	Employee specific emergency equipment operations (e.g., duress alarms, communication devices)																					
	Incident management basics (e.g., the steps to be taken to secure or cordon off the affected work environment)																					
	Security incident/emergency/loss reporting procedures (e.g., who to contact and how)																					
	How to document a security incident (e.g., report writing)																					
	How to communicate with dispatcher/rail traffic control on security matters																					

Key Lessons for Security Training and Awareness Audiences		EMPLOYEES – GENERAL			Employees Who Interact with the Public			Maintenance Employees			Employees – Security Personnel			Management			Contractors			Other Stakeholders/ Groups?		
Category	Teaching Point	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis	Req'd? (Y/N)	Req't Met? (Y/N)	Gap Analysis
Roles and responsibilities and program knowledge	Role of local law enforcement																					
	Role of operator police/security personnel and how they are organized																					
	Role of communications/control centre																					
	System Security Plan/Program																					
	Associated plans and programs (e.g., Emergency Response Plan/ Program; Business Continuity Plan/Program)																					
	Roles and responsibilities of emergency responders and the operator's role when interacting/working with them																					
	Roles and responsibilities of employees related to security incidents, employee/customer safety and asset protection																					
	Managers' security responsibilities and accountabilities																					
	How the operator's security program is coordinated and managed																					
	General security/emergency policies and procedures applicable to all employees (e.g., fire evacuation, bomb threat procedures, workplace violence/harassment)																					
	How system emergencies are managed (e.g., Emergency Plan, Emergency Operations Centre, Corporate Security Escalation Plan/ Security Alert Levels, role of emergency agencies and first responders)																					
	Mechanisms to coordinate activities with relevant stakeholders (e.g., first responders, Municipal and Provincial emergency management, local government, etc.) in the development of Security Plans and management of day-to-day operations and during incidents																					
	Organization of operator's security department																					
	Interagency coordination, information sharing																					
	Regulatory framework																					
	Overview of employees' security responsibilities																					
Procedures	Security/emergency procedures (e.g., regarding: following incident command; suspicious packages; unattended items; bomb threats; fire/ smoke; assaults in progress; fare disputes; disorderly behaviour; evacuation, etc.)																					
	How to conduct security inspections and sweeps for suspicious objects and signs of tampering (buses, trains, infrastructure)																					
	How to conduct assigned security duties (e.g., perimeter checks, access control, security response)																					
	How to conduct assigned law enforcement duties (e.g., suspicious package response)																					
	Crime scene management																					
	Media relations protocol																					
	Crisis management																					
	Business continuity procedures																					
	Incident command training																					