Industry Guidance for Implementing a Security Plan and Developing Security Plan Training under the *Transportation of Dangerous Goods by Rail Security Regulations*

February 6, 2020

This document is intended for information and guidance purposes only. It describes the objectives and purpose of security plans and security plan training as required by the *Transportation of Dangerous by Rail Security Regulations* (Regulations), and provides explanations and guidance to assist railway carriers or railway loaders in meeting the regulatory requirements for developing and implementing a security plan and security plan training.

The regulatory requirements outlined in the Regulations supersede what is written in this guidance document. As such, this document does not change, create, amend or permit deviations from the regulatory requirements.

Table of Contents

Introduction

The *Transportation of Dangerous Goods by Rail Security Regulations* (Regulations) apply to railway carriers or railway loaders who offers for transport, handles or transports any of the security-sensitive dangerous goods outlined in Schedule 1 of the Regulations and requires companies to develop and implement individualized security plans specific to their particular security environment.

What is a security plan?

A security plan should document a company's security goals and objectives, and is based on the company's security risk assessment. A security plan is part of a holistic approach to security that establishes a framework for addressing security risks, and reflects the range of prevention, mitigation, response and recovery from a threat or security concern.

What is the purpose of a security plan?

The purpose of a security plan is to enhance and maintain the security of an organization by assessing security risks, reinforcing existing security policies and procedures, and developing and documenting measures to address security risks.

Overview of the Security Plan Requirement

Refer to sections 8 through 11 of the Regulations for the complete regulatory text of the Security Plan requirement. This provision comes into force for railway carriers on February 6, 2020 and for railway loaders on May 6, 2020.

As stipulated in sections 33 and 34 of the Regulations future amendments will include the addition of railway loaders:

33 Section 9 of the Regulations is replaced by the following:

Application – Security-sensitive Dangerous Goods

9 (1) Sections 10 to 13 apply only to railway carriers that transport and railway loaders that offer for transport or handle any security-sensitive dangerous goods set out in Schedule 1.

34 Sections 10 to 15 of the Regulations will be amended by replacing "railway carrier" and railway carrier's with railway carrier or railway loader and "railway carrier's or railway loader's", respectively.

Scope of Application

Which companies need to meet this requirement?

The requirement to develop and implement a security plan applies to **railway carriers that transport and railway loaders** that offer for transport or handle any of the security-sensitive dangerous goods, outlined in Schedule 1 of the Regulations. As defined in the Regulations:

Railway carrier means a person who has possession of dangerous goods for the purposes of transportation by railway vehicle on a main railway line, or for the purposes of storing them in the course of such transportation.

Railway loader means

(a) any person that operates a handling site*, or

(b) any manufacturer or producer of dangerous goods that has possession of dangerous goods at a handling site for the purposes of loading them prior to, or unloading them after, transportation by rail.

***Handling site** means a facility connected to a railway line where a railway vehicle is placed for the loading or unloading of dangerous goods.

What are security-sensitive dangerous goods?

Security-sensitive dangerous goods are dangerous goods that are set in Schedule 1 of the Regulations and that could pose a security concern. Please refer Schedule 1 for the complete list of classes and quantities of these dangerous goods. Additionally, please refer to Part 4 of the Regulations for Exemptions that pertain to *the Transportation of Dangerous Goods by Rail Security Regulations.*

Developing and Implementing a Security Plan

Paragraphs 10(1)(a) through (m) of the Regulations provide the elements required in a security plan. Paragraph 10(1)(g) does not apply to railway loaders.

What must be included in a security plan?

A railway carrier or railway loader is required to implement a security plan that:

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
Companies must read the Regulations in concert with the *Transportation of Dangerous Goods Act, 1992,* 7.3(2) stipulates: ***Security Plans*** ***The plan shall, in accordance with the regulations, set out measures to prevent the dangerous goods from being stolen or otherwise unlawfully interfered with in the course of the importing, offering for transport, handling or transporting".***	Your security plan must set out measures to prevent dangerous goods from being stolen or otherwise unlawfully interfered with in the course of the importing, offering for transport, handling, or transporting. The security plan must have measures to address the identified security risks associated with the shipments of the security-sensitive dangerous goods while they are en route. Examples of potential measures are communication protocols, and vigilance programs.
(a) is in writing;	A security plan must be a written document that includes processes, measures and detailed information specific to the company's security operations. This information may reference other plans or procedures such as a Business Continuity Plan, a Fire Evacuation Plan, and an Information Management Plan. The security plan may be stored electronically or by hard copy.
(b) identifies, by job title, a senior manager responsible for the plan's overall development and implementation;	For railway carriers, this person could be the Rail Security Coordinator or the key person responsible for the development and implementation of the security plan. For railway loaders, this person could be the key person responsible for the development and implementation of the security plan.
(c) describes the railway carrier's or railway loader's organizational structure, identifies the departments that	In addition to the organizational structure and identifying responsibilities, a security plan could also, as a best practice, include the: • Company legal name;

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
are responsible for implementing the plan or any portion of it and identifies every position whose incumbent is responsible for implementing the plan or any portion of it;	• Operating name (if different from legal name); • Company headquarter address (including city, province, country and postal code); • Company telephone number, fax number and email address.
(d) describes the security duties of each identified department and position;	The security plan must identify the duties of personnel who have responsibilities with respect to security. Examples of such security-related duties could include, but are not limited to: • Personnel involved in developing and implementing the security plan, in response to security emergencies, such as security staff (employees or contracted staff), rail security coordinator, railway police.
(e) sets out a process for notifying each person in a position referred to in paragraph (b) or (c) and who is responsible for implementing the plan or any portion of it that the plan or that portion of it must be implemented;	This process may be established through any means that is practical and sustainable for the company's operations. An example could be internal communications within the company (e.g. instructions or bulletins).
(f) includes an assessment of the security risks associated with the offering for transport, handling or transport of the dangerous goods set out in Schedule 1 that the railway carrier/railway loader offers for transport, handles or transports;	A security risk assessment is the basis for its security plan. Security risks can take many forms and could have major impacts on a company's operations and the surrounding environment. Identifying these risks and planning to mitigate their potential impact is vital for companies involved in the transportation of security-sensitive dangerous goods. A security risk assessment should help to identify, evaluate and prioritize the security risks facing a company's operations. Security risk assessment methodologies may vary based on the size and scope of a company and its operations. There are many different methodologies with most using mathematical formulas to calculate risk through threat, probability, vulnerability and impact. Risk methodologies can also be scenario-based taking into account incidents which would compromise the security of a company's operations. See more detailed information in Annex A concerning the assessment of security risks associated with the offering for transport, handling or transporting security-sensitive dangerous

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
	goods.
(g) sets out a process for security inspections in section 7 , including ***(i) a procedure for conducting security inspections,*** ***(ii) a method for determining whether security has been compromised,*** ***(iii) a method for determining whether additional security inspections are necessary when, given the circumstances, security could be compromised, and*** ***(iv) a method for addressing the situation, if it is determined that security has been compromised.***	***Note: This paragraph applies to railway carriers only.** The security plan must address how the security inspections are conducted. If a company already has a set process in place, company instructions or procedures may be referenced in the security plan. If a company is developing this process, railway carriers could consider the following: • Where are the security inspections going to take place? Are there specific locations, yards or sites? • When are these inspections going to take place? • How will they be conducted? Is there one or more methods that may be used? • Will this requirement be added to existing operational procedures? • Who will be responsible for carrying out security inspections? • Will there be a process for recording that the inspection has taken place? For more detailed guidance, please refer to Transport Canada's guidance on Security Inspections. This document is not available on our website but a copy may be requested from Transport Canada at TC.Railsecurity-sureteferroviaire.TC@tc.gc.ca.
(h) sets out measures to prevent access by unauthorized persons to the dangerous goods set out in Schedule 1 and to the railway vehicles used to transport those dangerous goods;	The security plan must identify and briefly describe the security measures in place that could mitigate against unauthorized access, its impact and to facilitate a response to unauthorized access. Some measures that could be considered to limit access by unauthorized persons include: • A component in security training programs; • Fencing, barricades and/or bollards; • Perimeter trip alarms, building alarms, video surveillance (e.g. CCTV); • On-site security personnel; • Coded key pads on doors or gates; • Swipe cards or assigned keys; • An identification card/pass/photo ID; and • Distinctive clothing for company employees and contractors.
(i) sets out measures to verify information provided by	A candidate means any person or company who is applying for a position with a railway carrier or railway loader that will be working

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
candidates for positions that involve access to the dangerous goods set out in Schedule 1;	with security-sensitive dangerous goods, as outlined in Schedule 1 of the Regulations. These measures must be documented in the security plan and will vary based on the size and complexity of the company's operations, the commodity and the identified risks. It is recommended that consideration be given to each position based on the individual's duties when determining the level of security clearance or personal verification required. Measures for verifying candidate information could include, but are not limited to: • A reference check; or • A police background check
(j) sets out a policy on limiting access to security-sensitive information and sets out measures for the sharing, storing and destruction of that information;	Security-sensitive information refers to information that relates to the offering for transport, handling, or transporting of Schedule 1 dangerous goods as defined in the Regulations that, if publicly released, would be detrimental to transportation security. The security plan must identify and describe measures and/or technologies in place to protect, store, safely share, limit access to and destroy security-sensitive documents. Examples of such measures could include, but are not limited to: • Storage in a secure location such as password-protected computers, or locked cabinets and offices; • Use of encrypted e-mail; • Use of an industrial shredder; or • A process in place for restricted access to those positions requiring access to security-sensitive information. Policies should be reflective of a company's size and operations. Positions that have responsibilities that involve access to or handling of security-sensitive information should be identified in the security plan and receive the appropriate training to understand their special obligations to protect this information from unauthorized disclosure.
(k) sets out measures to address other security risks identified in the assessment referred to in paragraph (f);	"Other security risks" are the risks that are identified in the security risk assessment process set out in paragraph 10(1)(f) but have not been addressed in this provision. The security plan must include measures to address other security risks. These could vary from company to company. The following are some examples that may be considered other

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
	security risks: • Physical security measures for critical infrastructure including the yards/sites; • Company profile (high profile for environmental or political reasons); and • Site proximity to critical infrastructure, major venues with a high concentration of people (i.e. stadiums), or major transportation routes/facilities.
(l) sets out a program for the security awareness training required under section 14 and the security plan training required under section 11; and	Training programs may be stand-alone or integrated into a company's other training and awareness programs. Training programs should be updated periodically to ensure they remain current and effective. Such programs should also include a regular evaluation of its effectiveness and relevance. In addition, security awareness training programs should reflect operational needs, the company's security environment and the measures contained in the security plan. The security plan should explain that a security awareness and security plan training program exists and is implemented. It is suggested that details in the security plan include: • Who or what department is responsible for the training programs; • Which positions are required to receive training, and identify the particular training required; • An assessment of security training needs for current company personnel, including the assessment of the provisions of training in subsections 11(2),(3) and 14(3), 4) of the Regulations; • The method by which the training will be carried out (e.g. classroom style, online, etc.), including verification of the required knowledge obtained; and • The method by which training records will be retained.
(m) sets out measures to respond to a security incident and for reporting it.	The security plan must address company protocols for responding and reporting security incidents. Some elements to consider when setting out these measures include: • Who is required/responsible to report a security incident? • Who do they report it to? • What is the reporting structure and timeframe(s) for reporting? • How do they report the incident? • What information do they have to report? • What response measures will be taken?

Please note that examples provided below are for guidance purposes only.	
Required Elements	**Additional Guidance**
	• Will records be kept and for how long?

In addition to the requirements above, additional guidance on developing a security plan is included in Annex A.

Who must have access to the security plan?

A railway carrier or railway loader must make the most recent version of the security plan or any portion of it available to each person who is responsible for implementing the plan or that portion of it.

How often does the security plan have to be reviewed?

The security plan must be reviewed, and if necessary, revised once a year. A change in circumstance that is likely to affect the security risks that were identified in the assessment, may trigger a review of the security plan. Such circumstances may refer to, but are not limited to, major operational changes (e.g. changes in commodity, increase or decrease of operations, physical expansion of site, etc.), current events (increase in threat level, environmental protests, political summits or a major events) internal security breaches, or recent security incidents.

The appropriate persons must be notified without delay of any significant revisions to the plan. Such persons are those who are responsible for implementing the plan or that portion of it.

What level of security classification should be used for the security plan?

It is recommended that railway carriers or railway loaders classify and treat their security plan as a security-sensitive document. Companies are encouraged to mark all pages with a document classification appropriate to the level of sensitivity and the railway carrier's or railway loader's classification policy. The railway carrier or railway loader should limit and control the distribution of its security plan (e.g. using numbered copies, requiring that older versions be returned when new versions are distributed) and ensure that copies of the plan are stored in a secure location. Transport Canada will classify all security plans as Protected B which requires the department to adhere to information security standards as it relates to the handling of security-sensitive documents.

Is there a requirement to submit the security plan to Transport Canada?

A copy of a railway carrier or railway loader's security plan must be made available to the Minister of Transport upon his or her request. Once a copy of a security plan has been submitted to Transport Canada, the department will take proper measures to protect this document in accordance with the Policy on Government Security.

Can a railway carrier or railway loader use an existing security plan to meet this requirement?

A railway carrier or railway loader may utilize an existing security plan if it meets the requirements stipulated in subsections 10(1) and (3) of the Regulations.

If a company operates multiple locations or sites, is a security plan required for each site?

The Regulations require a railway carrier or railway loader to develop a security plan that is representative of its entire network and all operational sites in order to address the security risks associated with the transportation of the security-sensitive dangerous goods that the company offers for transport, handles or transports. The Regulations do not require a security plan for each site; however the security plan should take into account the company's unique operating environment and risk profile. As such, depending on the results of a company's security risk assessment, a company may be required to have specific measures for its high-risk operational locations, sites and yards to ensure the measures outlined in the security plan are commensurate (as per subsection 10(3) of the Regulations) with the security risks identified.

Companies are encouraged to reference or include its site-specific security plans in the corporate security plan, if applicable.

If a company already has site-specific security plans under other regulations, is an additional security plan required?

A railway carrier or railway loader may utilize an existing security plan only if it meets the requirements stipulated in subsections 10(1) and (3) of the Regulations.

The Regulations require railway carriers or railway loaders to develop a security plan that is representative of their entire network and all their operational sites. If a company has existing site-specific security plans, these may be referenced or included in the security plan, if applicable.

The term "indirectly" is intended to capture persons who are not direct employees of the company. This could include third party contractors who offers for transport, handles or transports dangerous goods for the railway carrier or railway loader.

Security Plan Training

Refer to sections 11, 12, 13 and 15 of the Regulations for the complete regulatory text of the Security Plan Training requirement.

The requirement to provide security plan training comes into force for railway carriers on February 6, 2020 and for railway loaders on May 6, 2020.

What is the objective of security plan training?

The objective of security plan training is to enhance the level of knowledge and understanding of the railway carrier or railway loader's security environment and its associated risks, and to elevate the security

posture of those persons who offers for transport, handles or transports security-sensitive dangerous goods, as well as those who are responsible for implementing or have a role in the development and implementation of the security plan.

Who is required to receive security plan training?

A person who is employed by or is acting directly or indirectly for a railway carrier or railway loader is required to receive security plan training if the person:

- Offers for transport, handles or transports security-sensitive dangerous goods (as set out in Schedule 1) by railway vehicle, in Canada; or
- Is responsible, in Canada for implementing the security plan or any portion of it but does not perform any of the duties referred to above. (Such persons could include, but are not limited to, the rail security coordinator, railway police, security guards, or security officers occupying a position in an office environment.)

It should be noted that only employees with the duties set out in subsection 11(1) of the Regulations are required to undergo security plan training.

When must security plan training be provided?

Railway carriers or railway loaders must ensure that training on the security plan is provided to the person:

- Before the person (referred to in paragraph 11(1)(a)) undertakes their security-related duties, unless the person has previously received equivalent training;
- Within six months of this requirement coming into force and before a person with duties described in paragraph 11(1)(b) undertakes security-related duties (unless the person has previously received equivalent training); and
- On a recurrent basis at least once every three years after the date the person previously completed their training, including any equivalent training received before the coming into force of this regulatory requirement.

All of the above requirements must meet the training topics requirement outlined in section 12 of the Regulations.

Note: Equivalent training may be assessed by Transport Canada on a case-by-case basis to determine whether the equivalent training meets the regulatory requirement.

What happens if an employee does not have the required training?

Supervision by a trained employee may be required if a person with the duties referred to in paragraph 11(1)(b) has not received security plan training. Until this person has received the training, they must perform their duties under the supervision of a person who has received that training.

What topics must security plan training cover?

The security plan must cover the following topics:

- The railway carrier's or railway loader's organizational structure with respect to security;
- The railway carrier's or railway loader's security procedures;
- The security duties of the person who is undergoing the training and any other security duties that are relevant to their duties; and
- The security plan measures that, in the event of a security incident, are relevant to the duties of the person undergoing the training.

Records

Do records of security plan training need to be maintained?

Yes. Railway carriers or railway loaders **must have a training record <u>for each person</u>** who has undergone security plan training.

Records may be kept electronically, in paper format such as a written log-book, or other such means or in combination and can be retained in any manner or in any location.

How long do records need to be maintained after an employee has left the organization?

Records must be retained for **at least two years** after the day on which the employee is no longer employed by or acting directly or indirectly for the railway carrier or railway loader.

What must the security plan training records include?

The security plan training record must include:

- The person's name and details of the most recent training session, that the person has received as well as the following information:
    - Date of the training;
    - Duration of the training;
    - Title of the course;
    - Delivery method;
    - Components of the security plan that were covered , if applicable; and
    - Name of the training provider.
        - The name of the training provider refers to the individual or company that provided the training. For example this could be an employee of the railway carrier or railway loader whose responsibility it is to provide training or a contracted entity or third party provider.
- The training record must also include the title and date of each training session that the person has received.

Where to find more information

For general information regarding Transport Canada's rail security program visit: https://www.tc.gc.ca/eng/railsecurity/menu.htm.

For general inquiries to headquarters email: TC.Railsecurity-sureteferroviaire.TC@tc.gc.ca.

Annex A: Assessment of Security Risks

The following steps could be considered when assessing security risks

STEP ONE: Identify Scope and Background

The first step in conducting a security risk assessment is to establish the company's security operating environment, or the security operating environment. This step will help to determine the scope of the assessment and define the level of detail to include in the security risk assessment.

It is recommended that companies start by providing background information on the company, such as various operations, corporate structure and ownership, infrastructure/facilities, and any business practices that are, or can be part of the dangerous goods operations. Existing safeguards should also be taken into consideration (e.g. training, reporting of security incidents, camera surveillance, security personnel, fencing, employee identification, restricted access zones, security threat protocols, etc.) that the company has in place to enhance security and reduce the risk of exposure. Documenting this type of information will help determine the context of the security risk assessment, and support the development of the security plan.

STEP TWO: Identifying and assessing critical assets and operations

The next step is to identify assets or operations that, if compromised, could result in a security incident. Examples of possible assets and operations could include:

- People (e.g. employees, contractors, clients, public or other stakeholders);
- Facilities (e.g. buildings, adjacent facilities, electrical systems, storage, site equipment and parking lots);
- Security devices (e.g. alarm systems, locks, access cards and cameras);
- Surveillance and monitoring equipment;
- Business/security processes (e.g.. access management, business continuity planning, codes of practice, emergency directives);
- Vehicles (e.g. locomotives, railway cars, construction equipment);
- Dangerous goods; and
- Transportation operations (packaging, temporary storage and movement).

STEP THREE: Setting the threat context

The security risk assessment should establish the level of potential threat to a company's dangerous goods operations from acts of violence, terrorism, insider threat, or criminal or malicious activities. A threat identifies the potential for a planned or premeditated act that could occur and may have an impact on critical assets or operations. Identifying the likelihood, impact and volatility of threat will help to determine the likelihood of a security incident occurring.

The threat level will set the overall tone of the security risk assessment and help determine the vulnerabilities or security weaknesses of the company's operations.

STEP FOUR: Identifying and assessing security vulnerabilities and analyzing existing safeguards

The next step is to identify and assess the company's security vulnerabilities. Vulnerabilities are weaknesses that make critical assets and operations susceptible to damage or attack. The company's vulnerabilities are the areas where security gaps should be identified.

The potential threat level that was established in the previous step would set the overall tone of the security risk assessment when a comparative analysis is performed against security vulnerabilities of the company's operations.

This step involves analyzing existing safeguards (identified in Step One) to determine how effective they are or would be in protecting the company's critical assets and operations. This will help to determine whether more robust security safeguards are necessary in order to prevent the compromise of these critical assets or operations. The final step in the security risk assessment process, is to develop an action plan that could help manage and address identified risks and vulnerabilities in a timely, efficient and sustainable manner.

If vulnerabilities have been identified through the security risk assessment, the potential impacts and consequences of those vulnerabilities should then be analyzed. From there, the company can begin to explore mitigation strategies for the company's identified security risks. Mitigation refers to actions that are taken to avoid or reduce the risks and impacts that are posed by a potential threat or security incident.

The security risk assessment process helps to identify the company's vulnerabilities and the possibility of these vulnerabilities being exploited. Once a railway carrier or railway loader conducts its risk assessment, this will help provide the company with the necessary information to develop and implement an appropriate security plan.

Annex B: Establishing Security Objectives

After the security risk assessment has been conducted and the company's vulnerabilities have been identified, the next step is to determine the company's security measures. It is recommended that at minimum, security measures be established for each component of the security plan (e.g. for personnel security, unauthorized access or en-route security

The next step is to assign mitigation measures to address vulnerabilities. After establishing the security objectives for each component of the security plan, identify mitigation measures that will be implemented to achieve each objective. Measures should be identified to address vulnerabilities that were identified in the company's security risk assessment. Included below are some examples of possible mitigation measures ***Examples of mitigation measures for personnel security objective:***

- Verify employee or applicant credentials and records where possible
- Confirm past employment (contact former employer)
- Have applicants provide additional references (personal and former employer)
- Implement random and reoccurring background checks for existing employees

Examples of mitigation measures for unauthorized access objective:

- Require employee photo identification badges
- Establish control and safekeeping procedures for badges
- Enforce the display of badges for employees and visitors
- Train employees to challenge persons without visible badges
- Install a fence around the facility and a security guard station at entrances

Examples of mitigation measures for en route security objective

- Install theft-protection devices to disable movement of goods (e.g., kill-switch)
- Secure cargo with specialized anti-theft locks/seals
- Inspect cargo manifests and verify cargo
- Conduct en route inspections to confirm that cargo has not been tampered with
- Enforce dwell time policies
- Verify identity of vehicle conductor/driver prior to any exchange of operation