"The project has received funding from the European Union's Internal Security Fund – Police under the grant agreement No 815347"

SHERPA

Deliverable D5.2

Executive Summary

Guidelines for railway management for handling and mitigating the risks coming from insider threats

July 2020

Project Details

Project acronym	SHERPA
Project full title	Shared and coHerent European Railway Protection Approach
Grant Agreement no.	815347
Call ID and Topic	ISFP-2017-AG-PROTECT, Topic ISFP-2017-AG-PROTECT Protection
Project Timeframe	01/11/2018 – 31/10/2020
Duration	24 months
Coordinator	UIC – Marie-Hélène Bonneau (bonneau@uic.org)

SHERPA

Document details

Title	Executive Summary of the guidelines for railway management for handling and mitigating the risks coming from insider threats
Work Package	WP5
Date of the document	01/07/2020
Responsible Partner	UIC
Reviewing Partner	All partners
Dissemination level	Public

Consortium – List of partners

Partner No	Short name	Name	Country
1	UIC	UNION INTERNATIONALE DES CHEMINS DE FER	France
2	DB	DEUTSCHE BAHN AG	Germany
3	FS SPA	FERROVIE DELLO STATO ITALIANE SPA	Italy
4	PKP S.A.	POLSKIE KOLEJE PANSTWOWE SPOLKA AKCYJNA	Poland
5	SNCB	SOCIÉTÉ NATIONALE DES CHEMINS DE FER BELGES	Belgium
6	SNCF	SNCF	France

INTRODUCTION

1. PROJECT OBJECTIVES

Terrorist attacks carried out in recent years show an alarming increase of indiscriminate violent actions carried out against civilians gathering in public spaces. Even though railway transport represents a critical infrastructure for all European countries, stations and trains can be essentially regarded as soft targets due to their inherently open system nature. Several initiatives aiming at increasing their protection from terrorist attacks were undertaken in the past years at various levels. Nevertheless, the knowledge about the phenomenon itself and possible countermeasures is still quite fragmented and presents many gaps.

The SHERPA project aims at improving the overall protection level for stations and trains in Europe against terrorist attacks by implementing multiple synergistic actions towards the relevant stakeholders, such as: providing and sharing an up-to-date, high-value knowledge base on threats and countermeasures (both technical and procedural); defining a coherent approach for risk assessment, risk management, crisis and disaster recovery management; strengthening co-operation among stakeholders through high-level international trainings and other practical tools; outlining needs and requirements for industry and research to focus on improving the ways in which railways cope with both present and future threats.

Five among the most relevant key-players in the European railway sector (DB, FS, PKP, SNCB, SNCF) take part as partners in the SHERPA project proposal: their joint participation brings the highest levels of credibility, representativeness and authoritativeness. Furthermore, the consortium itself is led by UIC, whose aggregative nature, together with its solid expertise and experience in participating and leading European projects, will facilitate synergies among the co-applicants and between them and police, first responders and other relevant stakeholders represented in the Advisory Board such as CER, COLPOFER, The French Ministry of Transport, RAILPOL, NS and SBB.

2. PURPOSE OF THE DELIVERABLE

The objective of these guidelines is to support the management of railway companies in developing coherent and holistic procedures for discovering, recognizing and dealing with insider threats.

However, it must always be beard in mind that the individual companies' obligations are defined by the respective national legislation with special reference to the Labour Statute regulations and the privacy provisions. The measures and instructions given in this guidance are therefore of a rather recommendatory and indicative nature. The depth and level of implementation in day-to-day operational life must recognise the factual and legal business surrounding of each individual railway company.

The document is organised in two main parts:

- Part A deals with "Recommendations for Rail Management". In addition to the legal framework, the main points that must be considered by the management and the question of how to detect an insider threat are described.
- Part B addresses some recent measures, on the organizational, technical, procedural and human-factor level. These are supplemented by recommendations on raising awareness and training on the topic of insider threat.

SHERPA

TERMINOLOGY AND ACRONYMS

Background check	A recorded check of a person's identity, including any criminal history (certified by a competent authority), as part of the assessment of an individual's suitability for unescorted access to security sensitive areas. (Source: RAILSEC WG2, DG Move; DG Home)
Ethical Code of Conduct	It outlines the ethical principles that govern decisions and behaviour at a company level. It give general outlines of how employees should behave, as well as specific guidance for handling issues like harassment, safety, security and conflicts of interest.
Criminal Record Certificate	A certificate about a person's criminal history that may be used by potential employers to assess the person's reliability
DPO	Data Protection Officer
HR	Human Ressources
Insider terrorism-related threats – types of	Employees, suppliers, contractors, ex-employees, third party employees who apply or applied in the past with: • the intent to commit a terrorist act or • who radicalize themselves, or • who are radicalized by outsiders after entering the company and then purposely have the intent to commit a terrorist act or who have the same intention after leaving the company but still having access to the company facilities.
Insider threat	Malicious threat to an organization that comes from people within the organization
Intrusion Detection System	IT: device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion or breach is usually reported to either an administrator or an event management system.
Security Check Act	It regulates the requirements and the procedure for checking a person who is to be entrusted or has already been entrusted with a security-sensitive position by the responsible authority. This is to ensure that information that is to be kept secret in the interests of the state is not made known to unauthorized persons. (Definition following Gabler Wirtschaftslexikon)
Security clearance	A statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to classified information or to restricted areas until a specified date; (Source: COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information)
Sensitive position	A sensitive position is: a) a position in which an employee is granted access to sensitive information b) a position requiring access to sensitive areas or assets c) a position that requires operations that present a high risk on security, health or safety, or d) a position that requires a high degree of confidence. (Source: RAILSEC WG2, DG Move; DG Home)
SPOC	Single Point of Contact
Two-Factor Authentication	Method to prevent unauthorized access to a system or confidential information. It requires a known information (password, PIN) and a special. The aim is to increase security because an unauthorized person has to get both to gain access
Vetting	A thorough investigation of a person, especially to ensure that it is suitable for work requiring secrecy, loyalty or trust, and to handle sensitive information. (Source: RAILSEC WG2, DG Move; DG Home)

SHERPA

EXECUTIVE SUMMARY

These guidelines aim at helping railway management handling and mitigating the risks coming from insider threats related to terrorism, and especially radicalization which could lead to violent acts.

The main challenge for railways when dealing with this type of insider threat is to take appropriate measures according to the legal framework of the country and the ethical rules of the company.

Radicalisation is seen as an increasing problem in some European countries; therefore, the legal framework has been adjusted in some countries to make it easier for the authorities to vet individuals for sensitive positions in railways companies even after the hiring process.

At the same time, within the current legal framework at EU level, few rail operators have more possibility to deal with responsibilities related to security issues concerning insider threats, since structured programme to mitigate this risk are conferred to National Law Enforcement Authorities.

Beside the national legal framework, an efficient company-wide insider threat strategy to prevent attacks against staff, customers and company assets should be defined in close collaboration with the authorities.

The following elements should be considered at company level:

- **Definition of a company-strategy to combat insider threat** by the members of the responsible steering board
  - An overall company approach needs to be taken: all business parts and the entire management level of the company (legal, HR, privacy, security, etc) should be involved in drafting an insider threat prevention strategy.
  - Clear definition of responsibilities: the roles and tasks of the involved company departments need to be clear and known.
  - Regular monitoring: the efficiency of the implemented processes need to be evaluated regularly; discovered weaknesses or new developments need to be reacted upon as soon as possible.
  - Procedures for the management of suspected staff: for the case of a finding in the process of screening for insider threats a clear reaction must be provided for which applies to the legal framework in place.

- **Ethical aspects**
  - Implementation of an Ethical Code of Conduct of the company.
  - Commitment of the employees to the ethical code of conduct.
  - Implementation of a system protecting the whistle-blowers.

- **Categorisation of employment positions**:
  - Reference to legally prescribed sensitive positions.

  - Definition and constant evaluation of sensitive positions within the company in addition to the legal requirements, including internal employees as well as external parties connected to the company's business.

- **Hiring process**
  - Knowledge of HR legal and privacy protection departments about what can and cannot be checked during a recruitment and hiring process, in accordance with relevant legal framework.
  - Definition of clear procedures for the recruitment and career development process (pre-employment).

- **End-of-position process (also: release / retirement / dismissal)**
  - Definition of clear procedures for the end of an employment.
  - Ensuring the return of all company access keys, badges and devices as well as uniforms.

- **Background checks for new and already operating railway employees**:
  - Strict compliance with the legal framework on security requirements for sensitive positions.

- **Building Awareness training for staff**
  - Development of dedicated training programmes, aimed at raising awareness among staff in handling suspicious behaviours and situations, in strict compliance with national and internal regulations.

- **Definition of clear procedures**
  - for the handling of sensitive information
  - for information security
  - for any kind of IT-based transfer of classified or confidential data
  - for the reporting processes and reporting channels
  - for access control to sensitive areas.

- **Mitigation procedures**:
  - Clear follow ups: in case of the detection of a threat.
  - Designation of a SPOC to coordinate with authorities if an insider threat is detected according privacy and security aspects.

- **Coordination with authorities**
  - Establishing a reliable data sharing network and partnership with authorities.
  - Ensuring a continuous exchange of information on new insider threat developments and potentially dangerous persons.

- **Cooperation between rail companies**
  - Consultation of existing insider threat initiatives and their degree of implementation, results, efficiency, evaluation, etc.

- Knowledge and best practice exchanges at international level using the existing network like Colpofer or UIC security platform.
- Exchange of information between companies should be possible, particularly with regard to the free movement of workers in the EU.

There are different kind of prevention measures that can be applied:

- **Organizational related measures**:
  - Cooperation within the company and its different departments, no matter if operative or corporate.
  - Background checks and staff vetting, in compliance with national regulations to find out as much as possible about employees or potential employees.
  - Means to report Insider Threat.

- **Technical related solutions**
  - Video surveillance on sensitive spots.
  - Access control to sensitive company buildings and premises.
  - IT security to prevent misuse by insiders, including e.g. a two-factor authentication as well as hardware-based solutions, and IT-security related awareness training.

- **Human factor related solutions**:
  The human factor plays an outstanding role in connection with insider threat as insider perpetrators are often present or former colleagues. This must be considered when implementing mitigation strategies.

Dealing with insider threats requires a comprehensive company approach. Essential components are the establishment of a governance model in order to guarantee prompt, company-wide reactions, in strict accordance with national regulations and public authorities' duties and responsibilities.

The cooperation of all stakeholders (board, HR, privacy law, compliance, law, business areas, IT, corporate security and others) is of fundamental importance. The goal is the company's ability to identify and mitigate insider threats. A strategy should be sought that can adequately respond to changes in risk, the emergence of new modes operandi and achieve also the desired level of maturity.

However, it should always be remembered that only the authorities are legally obliged to fight against insider terrorist related threat, the railway undertakings can only support by reporting findings made internally or by responding to information on insiders forwarded by the responsible authorities.

***