GUIDELINES FOR TRANSPORTATION SECURITY

November 2024

DISCLAIMER

This document is intended for information only and sets out guidelines concerning the main security risks involved in transporting and associated storage, loading, or unloading chemicals. The information contained in these guidelines is provided in good faith, and while it is accurate as far as the authors are aware, no representations or warranties are made regarding its completeness. It is not intended to be a comprehensive guide to all detailed aspects of the transportation of chemicals.

TABLE OF CONTENTS

INTRODUCTION

The transportation of chemicals, particularly dangerous goods, poses significant security risks that must be managed effectively to ensure the safety of people, property, and the environment. The guidelines provided in this document are designed to address these risks and offer a framework for mitigating and managing them within the chemical supply chain. It is important to understand and implement these guidelines to prevent potential risks.

These guidelines are intended for chemical companies, transport companies, and other logistics service providers involved in the transportation and associated storage, loading, or unloading of chemicals. They focus on the main security risks associated with transporting chemicals. While not attempting to provide a comprehensive overview of all security issues, they concentrate on the most critical aspects that must be addressed to ensure safe and secure transportation.

By adhering to these guidelines, stakeholders can work together to ensure the safe and secure transportation of chemicals, thereby protecting people, property, and the environment from potential harm.

1. OBJECTIVES AND SCOPE

1.1 OBJECTIVES

The primary objective of these guidelines is to provide comprehensive guidance on mitigating and managing the risks associated with transportation security within the chemical supply chain. This includes:

- Conducting comprehensive risk assessments to identify potential security threats.
- Implementing safe work systems based on risk assessment, risk management, and appropriate procedures.
- Ensuring compliance with relevant regulations and adherence to industry standards.
- Promoting a culture of security awareness and responsibility among all stakeholders transporting chemicals.

The potential negative outcomes from a security incident, as listed in the table below, highlight the importance of transport security management.

Risk Category	Examples
Litigation/lawsuits	Legal actions by victims, authorities, or other stakeholders following a chemical accident or incident.
Undesirable regulations	New or stricter rules imposed by governments or regulators to prevent or mitigate chemical risks, which may increase costs or reduce operational flexibility.
Harm to infrastructure	Damage to roads, bridges, railways, pipelines, terminals, or vehicles caused by chemical spills, fires, explosions, or collisions.
Community impacts	Negative effects on the health, safety, environment, or quality of life of the local population due to chemical exposure, noise, traffic disruption, or evacuation.
Cost to repair	Expenses incurred to restore the normal functioning of the affected infrastructure, equipment, or services after a chemical event.

Source: Chemical Transportation Security Handbook OPCW

1.2 SCOPE

These guidelines address the main security risks related to the transportation, intermediate storage, loading, or unloading of chemicals. The scope includes:

- In-transit security while transporting dangerous goods, focusing on measures to prevent theft, tampering, and other security breaches.
- Security on loading and unloading locations and intermediate storage facilities (warehouses)
- Providing a framework for selecting, controlling, and sub-contracting logistic service providers (LSPs)

By following these guidelines, stakeholders can work together to ensure the safe and secure transportation of chemicals, thereby protecting people, property, and the environment from potential harm.

2. DEFINITIONS

Consequences
In the context of security, the outcome of an unwanted event is commonly measured in four ways—human, economic, operational, and psychological—but may also include other factors such as impact on the environment or reputation.

Cybersecurity Risks
The potential for unauthorized access or attacks on digital systems, potentially leading to data breaches, operational disruptions, or vehicle manipulations.

Dangerous Goods
Substances and chemicals listed in the UNRTDG Dangerous Goods List or in the international dangerous goods regulations (ADR/RID/AND/IMDG-Code/IATA-DGR) and by your national authority.

Geopolitical Risks
Risks arising from political instability or conflict in regions that may affect the supply chain or transportation routes.

High Consequences Dangerous Goods
Those goods which have the potential for misuse in a terrorist event and which may, as a result, produce serious consequences such as mass casualties, mass destruction, or, particularly for Class 7 (Radioactive Substances), mass socio-economic disruption.[1]

Incident
An unplanned or unexpected event which typically results in property damage or people injury.

Hazard
A process, phenomenon, or human activity that may cause loss of life, injury or other health impacts, property damage, social or economic disruption, or environmental degradation.

Physical Security
Lock technologies (typical securement methods) are used to secure hazardous materials during transport (see also Chapter 6.).

Risk

[1] Recommendations on the Transport of Dangerous Goods – Model Regulations (Rev.22), 1.4.3.1.1 the indicative list can be found in 1.4.3.1.2

A security risk is the probability or likelihood that a threat will exploit vulnerabilities and cause harm, loss, damage, or disruption.

Threat
any action, indication, circumstance, or event with the potential to cause bodily harm, death, damage to property, injury, or loss or damage to assets.

Transportation Security
Measures or precautions to be taken to minimize theft or misuse of dangerous goods that may endanger persons and properties[2]

Vulnerabilities:
Weaknesses that a threat can exploit to gain access to an asset include building characteristics, equipment properties, personnel behavior, personnel locations, equipment, or operational and personnel practices.

3. SECURITY DURING TRANSPORT OF DANGEROUS GOODS

Companies involved in the transportation of dangerous goods by all modes of transport should take into account the security provisions stated in Chapter 1.4 of the UN Recommendations on the Transport of Dangerous Goods. Additionally, the modal security provisions in UN Chapter 7.2 should be considered for transporting dangerous goods by road, rail, and inland waterways.
The security provisions outlined in the modal regulations for transporting dangerous goods (ADR, RID, ADN, ICAO, IMO) must be implemented upon their entry into force.

Companies that are engaged in the transportation of High Consequence Dangerous Goods (as defined in Table 1.4.1 of the UN Recommendations) by all modes of transport should also develop a Security Plan that addresses at least the elements specified in Section 1.4.3.2.2 of the UN Recommendations.
To assist companies in implementing the necessary components for the Security Plan related to the transportation of High Consequence Dangerous Goods, the following guidance is provided:

3.1. RESPONSIBLE PERSONS

The company should designate an individual responsible for security, either an employee or external expert, who has the necessary qualifications and competence. This person will advise management on strategies and measures to reduce security risks. This person should relay all security recommendations and information from employees to management and ensure that relevant information is communicated to employees involved in activities related to high-consequence dangerous goods.

3.2. RECORD-KEEPING

The company is required to maintain records of the transportation of various types of high-consequence dangerous goods for a period of five years and provide them to the authorities on request. These data should be incorporated into the annual report prepared by the Safety Advisor under section 1.8.3 of ADR.

3.3. REVIEW OF OPERATIONS

Security measures should be an integral part of every company's safety and quality management system when transporting dangerous goods.

[2] Recommendations on the Transport of Dangerous Goods – Model Regulations (Rev.22), 1.4, NOTE 2

When establishing the Security Plan, management should review all current operations regarding the storage, handling, and transportation of High Consequence Dangerous Goods. At regular intervals, a general review of the operations from a security perspective should be conducted in cooperation between management and the person responsible for security. The outcome of this review should be used to take the necessary measures to prevent or reduce security risks.
Annex 1 contains the Transport Security Vehicle Checklist Template, which may be used in transport operations.

Although the recommendations above primarily focus on High-Consequence Dangerous Goods, companies should also consider integrating elements of the security plan into their operations for all dangerous goods. Incorporating these security practices can help mitigate risks, protect assets, and improve overall safety during transportation. Enhancing security across all categories of dangerous goods strengthens the company's resilience against potential threats and ensures a higher standard of protection for people, property, and the environment.

3.4. TRAINING

Every employee involved in activities related to dangerous goods should receive security awareness training, as part of their existing training programs. When they take on functions associated with High-Consequence Dangerous Goods, such employees should also receive clear information from the responsible person about the security prevention measures.
In addition to theoretical training, companies should conduct periodic **emergency response drills** simulating various security incidents, such as cargo theft, cyberattacks, or terrorism. These drills will ensure all employees are familiar with response procedures and can act quickly in case of emergencies.

3.5. REPORTING OF THREATS, BREACHES OR INCIDENTS

Every employee involved in activities related to dangerous goods should report to management and/or the person responsible for security any threat, breach, or incident observed concerning security. When a security incident happens, the company should activate the transport security plan. This plan should outline the procedures for:

1. Escalating the incident to management and notifying relevant authorities.
2. Communicating the breach to affected stakeholders, including customers and transport partners.
3. Conducting a post-incident analysis to identify root causes and prevent recurrence.

When a security breach occurs, it is crucial to have a **communication protocol** in place. This protocol should define:

1. The stakeholders (e.g., authorities, customers, suppliers) to be notified immediately.
2. The designated spokesperson within the company.
3. Timelines for communication and follow-up to ensure transparency.

3.6. SECURITY OF INFORMATION

All employees involved in activities related to High-Consequence Dangerous Goods must be instructed to refrain from disclosing information about the type of goods transported and handled by the company and its clients. Exceptions to this confidentiality requirement include situations where disclosure is necessary according to other regulations (e.g., information required in transport and customs documents) or when demanded by the authorities.
Employees are also required to maintain confidentiality of security measures and the contents of the Security Plan. For communication between the Logistic Service Provider (LSP) and the driver, systems must be implemented to ensure that information received is from a known and reliable source. The chosen method should sufficiently guarantee the secure identification of the information source.

3.7. ADDITIONAL MEASURES

In addition to the measures described above, each company should evaluate if their own or their customers' infrastructure and operations require additional actions to mitigate security risks.

4. SECURITY AT CHEMICAL SITES

The following guidelines are intended for all chemical sites involved in the transportation and associated storage, loading, or unloading of goods.

4.1. SITE SECURITY MANAGEMENT SYSTEM

To minimize security risks at chemical sites, chemical companies should establish a comprehensive written management system as part of their overall risk management strategy. This system should address security risks related to transport operations and encompass processes for identifying, evaluating, and managing security risks to people, property, information, and reputation. Line management should be responsible for the implementation of this security management system. Accordingly, a security policy should be established, security roles clearly defined and adequately resourced, and the lines of communication explicitly outlined.
This security management system should incorporate the following components:

- Procedural security measures: these are measures to be taken concerning personnel, budgets, and procedures.
- Constructional (physical) security measures: these measures provide physical barriers against unauthorized access to sites, buildings, rooms, and information.
- Electronic security measures: these are electronic, electrotechnical, and optical security measures that offer information, detection, warning and observation capabilities, facilitating an appropriate and timely response when necessary.

4.2. SELECTION, CONTROL AND SUBCONTRACTING OF LOGISTIC SERVICE PROVIDERS (LSP)

The following guidelines should be considered with for the selection and control of logistics service providers (LSP) by chemical companies:

- Every LSP should be assessed using the SQAS questions related to security. Companies should evaluate this assessment, as part of their LSP selection process;
- A security clause should be included in the contractual agreements with the LSPs, which refers to the company's security management system.
- Transit control procedures, site control procedures, and sub-contracting requirements should be communicated by the chemical company to the LSP and implemented by the LSP.

The following guidelines should be taken into account in case of subcontracting by the contracted LSP:

- Subcontractors must operate under the responsibility, management, and operational system of the contracted LSP and adhere to their procedures. The contracted LSP remains accountable to the chemical company.
- The contracted LSP is responsible for assessing and training their subcontractors, ensuring full integration into their management and operational system.
- The contracted LSP should compile and maintain a list of their approved subcontractors and provide this list to the chemical company for approval.
- Chemical companies have the right to reject sub-contractors from the list if they do not meet the chemical company's assessment criteria.
- Subcontractors are prohibited from further subcontracting (sub-subcontracting).

4.3. TRANSPORT OPERATIONS NOT CONTRACTED BY THE CHEMICAL COMPANY

If the chemical company is not the contracting party for the transport operation (e.g. in case of raw materials purchased on a delivered basis or in case of customer pick-ups), it should contrually require its suppliers or customers to implement measures ensuring secure loading/unloading at the chemical companies' site. The chemical company should particularly focus on vehicle and driver access control when entering the chemical site, as well as monitoring the movements and operations of the vehicles and drivers on-site.

5. SECURITY DURING TRANSPORT

There are several methods and technologies available to protect vehicles and equipment (trailers, containers) from tampering or theft when securing dangerous goods during transport.
Some methods for ensuring physical security are:

- Generic methods like key locks, bolts, strikes and latches, seals, and high-security seals (for High Consequences Dangerous Goods)
- Steering wheel and brake pedal locks
- GPS alarm system
- Anti-theft systems
- Onboard cameras (truck)

For high-risk scenarios involving High Consequence Dangerous Goods (HCDG), the following additional measures may be implemented:

1. **Escort vehicles** for high-value or high-risk goods during transit.
2. Use **secured parking areas** that are monitored and have restricted access.
3. **Driver identification** using biometric or GPS technology to ensure that the vehicle is operated by authorized personnel.

6. RISK MITIGATION

In the context of security, minimizing risk when transporting dangerous goods is essential to prevent accidents, damage, and misuse. Here are some measures that contribute to risk mitigation:

- Risk analysis: conduct a risk analysis to identify potential hazards and vulnerabilities risks and take appropriate measures to minimize risk.
- Training and awareness: train all employees involved in transporting dangerous goods to identify and minimize risks.
- Route planning: plan the transport route carefully to minimize risks such as accidents, traffic congestion, and environmental hazards.
- Emergency planning: develop an emergency plan that covers all possible scenarios to ensure a quick and effective response during incidents.
- Monitoring: continuously monitor the transport of dangerous goods to ensure compliance with all regulations
- Control: regularly check compliance with regulations and risk mitigation measures to ensure their practicality and adjust them if necessary.

Track and trace systems are essential for transport security, facilitating continuous monitoring and tracking of goods and commodities. By using RFID or barcode technology, transport companies, logistics service providers, and chemical companies can monitor and track the real-time location and condition of goods. This enables swift responses to unforeseen events such as delays, losses, or thefts. Moreover, tracking dangerous goods helps identify and mitigate potential security risks, such as smuggling or terrorism. Additionally, track-and-trace systems enhance the efficiency and

productivity of transportation and logistics processes by optimizing shipment planning and control and reducing delivery times. Companies may also consider integrating additional technological tools such as:

- **Geofencing**: To automatically issue alerts when vehicles deviate from designated routes, or send confirmation messages when planned (transit) locations are reached.
- **Driver communication systems**: To maintain constant contact with drivers during high-risk transports.
- **Autonomous surveillance systems**: To monitor for suspicious activity around vehicles or in storage areas

Conducting a thorough risk assessment involves identifying and analyzing vulnerabilities, evaluating the potential impact of different threats, and rating risks according to their likelihood and severity. Organizations should use a structured approach, such as a risk matrix, to prioritize security measures based on the assessed risks.

In addition to conventional security risks, organizations must stay alert to emerging challenges, such as cyberattacks targeting transportation networks and disruptions resulting from geopolitical instability. Regular security audits, encompassing both physical and cyber aspects, are recommended to maintain readiness against evolving threats.

7. EMERGING CYBER SECURITY RISKS

Transportation security and cybercrime are closely interrelated. As transportation and logistics systems become increasingly digitalized and interconnected, companies and service providers are more vulnerable to cyberattacks. These attacks can lead to serious issues, such as data theft and vehicle manipulation, potentially disrupting transport processes.
Companies must take proactive measures to ensure transportation security. This includes implementing security protocols, training staff on cybersecurity, and regularly updating security measures. Industry-wide collaboration is essential to strengthen the security and integrity of global transport and logistics systems.

7.1. Impact of Cybercrime on the Transportation Industry

Cybercrime can have a considerable impact on shipping companies and other entities in the transportation sector. Examples of such impact include:

- **Theft of Data:** Cybercriminals can breach shipping company systems, accessing confidential information for criminal activities like identity theft or extortion.
- **Disruption of Transport Processes:** Cyberattacks can disrupt IT systems, causing delays in goods delivery and damaging the company's reputation.
- **Manipulation of Vehicles:** Criminals may infiltrate and manipulate vehicle systems, risking safety by tampering with navigation or control systems.
- **Financial Losses:** Cyberattacks can result in theft of funds, reputational damage, or business opportunity losses due to delivery delays.

7.2. Recommendations for Cybersecurity

To mitigate risks and impacts, stakeholders in the transportation sector should consider the following cybersecurity practices:

- **Strong Password Policy:** Implement robust password policies, avoid weak or identical passwords, and use password vaults for secure storage.
- **Multi-Factor Authentication (MFA):** Enable MFA on all accounts for added security, ensuring MFA devices are separate from login devices.
- **Security Awareness Training:** Provide regular training to identify phishing attempts and malicious communications.

- **Utilize Trusted Vendors:** Download software only from trusted sources and restrict access using the “principle of least privilege”. This ensures that a user or entity has only access to the specific data, resources and applications needed to complete a required task
- **Threat Actor Monitoring:** Reduce exploitation risks by continuously monitoring ransomware groups targeting the sector, implementing mitigation measures, and by staying updated on Tactics, Techniques, and Procedures (TTPs) of cybercriminals to develop and engage in cyberattacks.
- **Maintain Regular Backups:** Follow the three, two, one backup rule, storing 3 copies of the data on 2 different media types with one copy in a secure off-site location for disaster recovery.

In addition to general cybersecurity practices, companies should implement specific protocols to safeguard logistics systems:

1. **Securing IoT devices**: Ensure all tracking devices, sensors, and onboard systems are equipped with the latest security patches.
2. **Data encryption**: Encrypt all data transmitted between vehicles, drivers, and control centers to prevent interception.
3. **Regular cybersecurity audits**: Conduct routine IT system audits to identify and address vulnerabilities proactively.

By implementing these practices, transportation entities can improve their cybersecurity measures and protect against digital threats.

Robert Schmidkunz
Vice President - Head of Logistics Safety
robert.schmidkunz@evonik.com

Steven Rowland
ECTA Responsible Care Director

steve.rowland@ecta.com

Gerhard Albrecht
Responsible Care & Logistics Manager
gah@fecc.org

Laercio de Oliveira
Transportation Safety and Security Leader
Dow – Latin America
looliveira1@dow.com

Jos Hamers
Specialist, EHSS & Sustain Solids, Global Supply Chain Petrochemicals
Jos.Hamers@SABIC.com

Imre Elek
Transport & Logistics Safety Manager

iel@cefic.be

Annex 1: Transport Security Vehicle Checklist Template

Pre-Departure Checklist	Yes (✓)	No (X)
Verify driver's ID and qualifications (licenses, certifications)		
Ensure driver has undergone security awareness training		
Inspect all locks (steering wheel, brake pedals) and ensure anti-theft devices are functioning		
Check if tamper-proof seals are in place and intact		
Verify GPS tracking system is active and functional		
Ensure vehicle doors, compartments, and containers are secured properly		
Confirm transport documents are complete, accurate, and secure		
Ensure emergency contact details and response procedures are available in the vehicle.		
Verify that route planning is completed with security in mind		
Check if emergency equipment (fire extinguisher, first aid kit) is available and functioning		
Ensure the vehicle has an emergency communication system installed		

In-Transit instructions
Confirm that the driver regularly checks in with the base via secure communication channels
Use geofencing to ensure the vehicle stays within designated routes
Ensure all doors, seals, and locks are checked during rest stops
Park only in secure, pre-approved areas with monitored surveillance
Report any suspicious behavior or vehicles following the transport

Post-Delivery instructions
Inspect the vehicle for any signs of tampering after unloading
Check locks, seals, and security systems again before returning the vehicle
Confirm delivery documentation is complete and accurately signed by all parties
Report any security incidents (if any) immediately to relevant authorities and the company's security manager
Schedule any necessary maintenance or repairs for locks, tracking systems, or alarms as soon as possible

Driver Signature: _____ **Date:** _____

Security Officer Signature: _____ **Date:** _____