TRANSPORT SECURITY GUIDANCE FOR AIGA MEMBERS

AIGA 043/15

Revision of AIGA 043/07

Asia Industrial Gases Association

3 HarbourFront Place, #09-04 HarbourFront Tower 2, Singapore 099254
Tel : +65 6276 0160 • Fax : +65 6274 9379
Internet : http://www.asiaiga.org

AIGA 043/15

TRANSPORT SECURITY GUIDANCE FOR AIGA MEMBERS

Disclaimer

All publications of AIGA or bearing AIGA's name contain information, including Codes of Practice, safety procedures and other technical information that were obtained from sources believed by AIGA to be reliable and/ or based on technical information and experience currently available from members of AIGA and others at the date of the publication. As such, we do not make any representation or warranty nor accept any liability as to the accuracy, completeness or correctness of the information contained in these publications.

While AIGA recommends that its members refer to or use its publications, such reference to or use thereof by its members or third parties is purely voluntary and not binding.

AIGA or its members make no guarantee of the results and assume no liability or responsibility in connection with the reference to or use of information or suggestions contained in AIGA's publications.

AIGA has no control whatsoever as regards, performance or non performance, misinterpretation, proper or improper use of any information or suggestions contained in AIGA's publications by any person or entity (including AIGA members) and AIGA expressly disclaims any liability in connection thereto.

AIGA's publications are subject to periodic review and users are cautioned to obtain the latest edition.

ASIA INDUSTRIAL GASES ASSOCIATION
3 HarbourFront Place, #09-04 HarbourFront Tower 2, Singapore 099254
Tel: +65 62760160 Fax: +65 62749379
Internet: http://www.asiaiga.org

Acknowledgement

This document is adopted from the European Industrial Gases Association document 913/13 – Transport Security Guidelines for EIGA Members. Thanks and acknowledgement are hereby given to EIGA for permission granted for the use of their document.

Table of Contents

Amendments to AIGA 043/07

Section	Change
	Revised for updating to latest version of EIGA 913/13 – Transport Security Guidelines for EIGA Members

1 Introduction

Security measures improve the safe transportation of all materials, in particular those that are hazardous, by reducing the risks from a wide range of threats. Concerns about terrorism, sabotage, theft, illicit drugs, or intentional product contamination for example giving companies that transport materials a compelling reason to implement security measures for transportation of their products. Security measures, like safety measures, protect the general public and the environment as well the compressed gas industry and its employees.

Whilst this document has not been harmonized with other gas associations it has taken account other material including the Compressed Gases Association (CGA) standard P-51 Transportation Security Standard for the Compressed Gas industry [1] and AIGA thanks CGA for permission to reproduce parts of P-51 in this document

2 Scope and purpose

2.1 Scope

This document contains tools and resources that maybe used when assessing security issues related to the transportation of materials and products.

The implementation of the information contained in this document, plus the specific ways of managing security and risks will vary when taking into account the raw materials and products being transported, the mode and route of transportation and the vulnerability/risk profile. For example, the measures taken by a company located in a residential area or adjacent to a strategic transport corridor could be very different to one located or operating in open country.

2.2 Purpose

This document is intended for management personnel, transportation/logistics specialists, and all other personnel that are responsible for the safe and secure transportation of all raw materials and products by roads/highway, rail, inland waterways and pipeline.

3 Definitions

For the purpose of this publication, the following definitions apply.

3.1 Asset

Person, environment, facility, material, information, intellectual property, business reputation or an activity that has a value to a business

Note: An asset can have value to an adversary as well as a business, although the nature and magnitude of those values can differ. Assets included in a security vulnerability assessment include the community and the environment surrounding a site.

3.2 Bulk

Container having a water capacity greater than 1000 litre

Note: Includes tube trailers, cargo tanks, ISO containers, etc.

3.3 Consequence

Amount of loss or damage

Note: Loss may be monetary but may also include political, morale, operational effectiveness, or other impacts. The impact of security events that should be considered only includes those that are extremely severe. Examples of relevant consequences considered in a security vulnerability analysis include injury or death; large-scale disruption to public, private, or company operations; large-scale environmental damage; large-scale financial loss; loss of critical data; and loss of reputation whether resulting from an attack or any other unlawful activity.

3.4 Countermeasure

Measure (physical, organizational) put in place to reduce or eliminate vulnerabilities.

3.5 High consequence dangerous goods

Those with the potential for misuse in a terrorist incident and which may, as a result, produce serious consequences such as mass casualties or mass destruction.

Note: There is a list of high consequence dangerous goods in table format within AIGA 003/14, Site Security Guidelines

3.6 Mitigation

Action that causes a consequence to be less severe

3.7 Risk

Potential for damage to or loss of an asset.

Note: For example (but not limited to an intentional release of hazardous materials to the atmosphere, theft of chemicals that could later be used as weapons or for other criminal activities, the contamination of chemicals that may later harm the public, or the economic costs of the damage or disruption of a chemical process.

3.8 Risk assessment

A process of predicting the likelihood of an adversary successfully exploiting a vulnerability and the resulting degree of consequences.

Note: A risk assessment provides the basis for rank ordering of risks and thus establishes priorities for the application of countermeasures.

3.9 Seal

Device used as tamperproof identification or securing device.

Note: ISO/PAS 17712, *Freight containers–Mechanical seals* is a standard that describes security seals used in international shipments [5]. Some countries may have their own specific product security seal requirements.

3.10 Security

The measures or precautions taken to minimise the theft and or misuse of raw material, industrial gases products, and includes those that may endanger persons, property or the environment.

Note: Security issues may arise from errors, malicious, criminal and or hostile activities or through unsafe acts and or a lack of understanding by employees or third parties

3.11 Security awareness training

This is training on “the nature of risks, recognizing security risks, methods to address and reduce such risks and actions to be taken in the event of a security risk”.

3.12 Security plan

Document describing a plan that addresses security issues and related events, including a security assessment and mitigation options. An example layout is at Appendix A;

Note: A security plan include security alert levels and response measures.

3.13 Security vulnerability /risk assessment (SVA)

Evaluation of the possibility of an adversary successfully exploiting a company's vulnerability and the degree of damage or impact that can result.

Note: SVAs are not a quantitative risk analysis; they are qualitative, using the best judgment of security and safety professionals. The determination of risk (qualitatively) is the desired outcome of the SVA. It provides the basis for rank ordering the security-related risks to establish priorities for the application of countermeasures.

3.14 Terrorism

Unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof to further their political or social objectives.

3.15 Threat

Indication, circumstance, or event that if pursued by an adversary can cause loss of or damage to an asset

3.16 Transportation

Includes receiving raw materials and dangerous goods / products onto members' premises and the whole process of supplying dangerous goods to customers by road, rail, inland waterway and pipeline. It includes security during the whole time that the goods are on route including when held in temporary storage.

3.17 Vulnerability

Weakness that can be exploited by an adversary to damage a company or gain access to its assets (especially hazardous material in transit).

Note: Vulnerabilities can include but are not limited to equipment, personnel practices and behaviours, locations of people, equipment, buildings, or operational practices.

3.18 Weapons of mass destruction (WMD) (see list of Chemicals of Concern in AIGA 091/14 appendix B)

Weapon designed or intended to:

- cause death or serious bodily injury through the release, dissemination, or impact of toxic/poisonous chemicals or their precursors;
- release radiation or radioactivity at a level dangerous to human life;
- deliver a disease organism; or
- deliver an explosive incendiary, poison gas, bomb, grenade, or rocket.

4 Staff employment

Get documentary evidence of background and experience for all potential employees to ensure they and their background is suitable for the role under consideration. Insist on original documents to check identity and qualifications and wherever possible get a continuous record of the applicant's education and employment history covering at least the previous five years.

Check that staff hold verifiable:

- licences, certificates and operating documents where applicable; and
- permission to work in the country of operation.

Warn applicants that giving false information, or failing to disclose material information, would be grounds for a refusal to interview or, if employed dismissal.

Companies should also verify at regular intervals any licences, certificates and operating documents that staff may need to do their job and that they comply with any local laws and regulations.

5 Selecting contractors

Businesses use contractors or agencies to provide a range of services. However contractors may create new vulnerabilities and could expose businesses to 'insider' threats.

Contractors or agencies need to be rigorous in their selection procedures. It is therefore good practice to ensure that contractors and agents undertake the same pre-employment screening process as for your own employees, particularly if they are involved in the transport of dangerous goods.

Responsibility for implementing such checks should rest with the supplying company. The user company should ask them to demonstrate, from their records, that they have carried out these checks. If they fail to do so, the employing company should consider using a different contractor.

Organisations shall ensure that there are appropriate checks or screening of contractors or sub-contractors or agency staff employed in key positions, such as security guards at site access points, drivers, dispatchers, route planners, and handling and filling staff.

It is also good practice is to ensure that you have procedures to confirm that a person sent by a contractor or agency is the individual who turns up.

6 Security road/highway transportation

6.1 Transportation security plan

It is good practice and a requirement in many Countries that companies transporting hazardous materials (by road/highway) have a written transportation security plan.

A transportation security plan shall address relative risks associated with the transportation of hazardous materials. Using risk assessment methodology, a company should select an appropriate level of detail for its security plan based on the risks associated with the material being transported. Factors that may be considered are:

- type of materials transported;
- area from which the material is shipped;
- destination facility or area; and
- mode of transportation.

A transportation security plan shall contain the following:

- method(s) for confirming information provided by applicants, including internal applicants, for jobs that involve access to or handling of the hazardous materials covered by the plan;
- method(s) to address the possibility that unauthorized persons may attempt to gain access to hazardous materials or transport vehicles that are being prepared for hazardous materials transportation; and
- method(s) to address security while a shipment of hazardous materials is in transit from one destination to its final destination including any storage incidental to transport.

A security plan is acceptable if it includes the minimum requirements outlined in this document. If National agencies mandate additional requirements then those requirements shall be implemented.

When developing a written security plan, transporters should assess their internal practices and staff behaviour to ensure the safe transportation of hazardous materials. Considerations should include:

- Technology—Transporters may use technological solutions to enhance security. These can include communication systems, tracking systems, inventory controls, sensors, and vehicle access control systems;
- Event monitoring, reporting, and analysis. Records of security incidents should be kept. Reviewing these incidents can help identify trends and potential vulnerabilities while ensuring that carriers are handling hazardous products properly.
- Risk management is the key to an effective transportation security program. Transportation security risk management programs should include the following components:
    - Risk assessment evaluation of all hazardous materials transportation risks;
    - Risk reduction identification, development, and implementation of risk reduction measures that are appropriate for the level of risk.

The written transportation security plan should be periodically reviewed and updated.

Note: All parties in the transportation chain should have a security plan. Some may benefit from a joint plan. See Appendix A for an outline that can be used to help develop a transportation security plan

6.2 Security co-ordinator

It is good practice to have one person to be accountable at a site or process level for the whole security planning process.

This person should have sufficient authority to direct the response to security threats. They should also be involved in the planning and design of the site's exterior security, access control and so on.

If a company has several sites you may wish to appoint one person with overall accountability for security but also several site-based security co-ordinators.

Whilst such a person is accountable, all staff are responsible for helping to maintain industrial gas product security of on a daily basis.

6.3 Security training

Security training shall comply with all relevant regulation.

Companies (including contractors) should provide security awareness training periodically, supplement by refresher training. The training should deal with:

- the nature of security risks;
- recognising security risks;
- company security objectives, specific security procedures and employee responsibilities;
- how they can help minimise security risks; and
- what to do in the event of a security breach.

Some staff may also require awareness of those parts of any security plan that they 'need to know'. This should be at a level appropriate to the responsibilities of individuals and their part in implementing security plans.

Drivers and crew members should also be trained/advised on what to do in the event of hijack or criminal attack. It must be emphasised that they must not put themselves at risk in an attempt to protect the vehicle and or load.

The depth and regularity of training will depend upon the type of goods being carried and the outcome of any risk / vulnerability assessment unless specific timeframes are set down by Regulation (for example ADR and individual country requirements).

Each employee shall complete function specific security training and testing to ensure proper skills and knowledge. Copies of tests taken during this training shall be retained.

The employer should record all security training and testing shall be retained. Records should be made available to the employee upon request.

It is important that security is seen as a normal, daily routine, in the workplace.

6.4 Communication

To prevent transportation security incidents, effective communication methods should be established. Carriers, shippers, and customers should have a process in place to communicate information on events, patterns, technologies, security plans, modifications, and discrepancies such as improper driver identification, incomplete bills of lading, etc. Tracking and communicating information about incidents such as tampering with security seals or equipment enables the early identification of trends.

Communication methods can include e-mail, PDAs fax, cell phones, satellite phones, global positioning satellites, etc.

Vehicles should be fitted with mobile telephones or some other means of two-way communications between the driver and the base to aid emergency and other essential communication.

6.5 Vehicle security

All vehicles (power units, including but not limited to tractors, rigid units, pickups, etc) shall be secured (engine off, keys removed, doors locked, windows closed) when unattended on or off sites.

All product compartment doors shall be locked when not in use for loading, unloading, or maintenance procedures.

Tail lift/lift platform shall be secured when not in use.

Where fork lift trucks are part of the vehicle unit the fork lift truck ignition key shall be removed when not in use.

Consider additional security measures based both on their feasibility and the vulnerability / risk assessment. Measures such as:

- Anti-theft equipment
- High security locks
- Security Grilles/Mesh
- Fuel valve immobilisers
- Starter motor immobilisation
- Immobilisation of braking systems

- Wheel clamps
- GPS and other tracking systems

6.6 Trailer security

All product compartment doors shall be secured when not in use during loading, unloading, or maintenance procedures.

Tail gates/platforms shall be properly secured when not in use.

Secondary locks including trailer pneumatic locking devices (glad hand locks), king pin locks, or an approved internal lockout control process shall be in place when a trailer is left unattended or unhooked in an unsecured location.

6.7 Cylinder security

Members companies should consider the risk and vulnerabilities of the raw materials and hazardous products they are transporting in order to decide on the level of security that needs to be applied. Hazardous materials with an LC_{50} less than 200ppm shall be transported in a secured vehicle, for example:

- open vehicle—transport in a security cage;
- a suitably ventilated enclosed trailer/vehicle that is designed to prevent any gas leak in the load compartment from entering the cab; or
- transport with secured access.

This is unless an assessment of the transportation risks indicates that a lower level of security could be deployed

6.8 Tamper detection

Carriers, shippers, and customers should implement procedures that help to determine whether a product and container have been tampered with. This can include using seals, closures, or shrink wrap on cylinder valves.

6.9 Transporter qualification

All Transporters that transport raw material and hazardous products should be pre-qualified by the contracting company. The qualification should include a review of their transportation security plan and pre-employment screening process.

The contracting company should also consider the regular auditing of security procedures adopted by any contractor they engage to carry dangerous goods.

6.10 Inbound shipments/truck arrivals

Do not allow a vehicles to have access to a facility unless the shipment is expected, the driver and crews paperwork, and the delivered material is acceptable.

The authorisation process may include the verification of:

- The shipment is due or expected
- The names of the shipper and carrier on the delivery paperwork for materials are correct; and
- The shipment's content, quantity, and condition:
- The quantity shipped is the quantity received. If there is a discrepancy, investigate immediately.

Notify the appropriate management representative of any shortages not immediately resolved; and check for discrepancies such as evidence of tampering with the container, improper /incorrect transportation documents, or improper identification of product.

Where required a process should be put in place to allow pre-authorisation for entry to a site without human intervention (electronic pass, tag or key).This is of particular relevance to unmanned sites.

If any shipment is unreasonable delayed then an explanation for late delivery should be investigated. If the reasons unsatisfactory then consider with management whether the shipment should be received, for example the delay may have been to enable someone to interfere with the integrity of the load.

6.11 Driver and truck monitoring

Drivers, plus any crew, should be monitored while entering and when on site. They must be restricted to appropriate areas whilst driving on site and during loading and unloading. Unauthorized drivers/crews must be denied entry into a facility.

A driver's commercial driver's license should be verified by checking the photograph, expiration date, and valid hazardous materials endorsement if applicable. If there are team drivers, this verification applies to both drivers

6.12 Shipment preparation

Inspect all transportation vehicles and the load to ensure they are ready for loading and that there is no evidence of tampering or interference.

Follow all company procedures and local and national regulations as applicable for labelling, loading, placarding, and securing shipments.

Report any unusual activity such as “unusual interest in vehicles or sites” to local management.

6.13 Outbound shipments

Do not allow a truck to leave a facility until the driver’s paperwork for the outbound material is determined to be acceptable.

If adequate paperwork is not available, then contact the plant traffic/shipping department for authorization before allowing a truck to leave the facility.

Where there has been pre-authorisation for exit from a site without human intervention (electronic pass tag or key), a process should be put in place to verify the load, for example electronic monitoring of loading, use of camera technology.

Where ever possible shipments should avoid overnight or other extended stop but where this is not possible this should be in a secure parking area

If the outbound shipment is going to be delayed in arriving at the customer or other facility then steps should be taken to notify the recipient of that fact and the reasons why.

6.14 Security on the road

The best and safest routes are not necessarily always the shortest. It is good practice to plan routes where there may be security risk that are of concern. This is so that neither drivers nor the public are put at additional risk no matter what the load. Where route planning is deemed appropriate the following should be considered:

- Routes should be based on the assessment of the security and safety risks.
- Appropriate measures should be taken to mitigate risks as far as possible – this should start at the initial sale contact point.
- Route / instruction cards (or their equivalent) should be used as a safety tool. Their content should details the hazard or risks and the action required by the driver in order to reduce a security/safety risks happening on a journey.
- Drivers should be instructed to follow the routes/directions that appear on the trip instructions or route card.
- Where a driver has concerns about his/her personal safety these should discuss with their line supervisor / manager
- Drivers have valuable information on route risks – look to gather and make use of that intelligence

Always using the same route at the same time of the day can put vulnerable loads at risk. Periodically reassess to reject, modify, or downgrade any route or other restrictions that have been put in place.

Routes that should never be used are described as those that are:

- Physically impossible to drive the vehicle on.
- Too dangerous (safety/security) to drive a vehicle on the route.
- National or local legislation restrictions prevent use.

Routes that may have temporarily safety/security restrictions and or are operated under special instructions / restriction may involve the following factors:

- Seasonal weather conditions and or other issues that add to the risks of any journey.
- Travelling in cities and or other populated areas during night or daytime.
- Increase in criminality (including hijackings, robberies and abductions)
- Increase in other risks due to ‘time bound’ events such as protests, demonstrations, etc.
- Unsafe routes for lone workers but consider safe if more than one worker is present.

Route compliance can provides an indication of the driver's general location if a driver fails to arrive at a location. In particular drivers involved in any incident (as a crime victim, accidents or breakdowns) on route will be easier to locate.

Manager should continuously seek and evaluate information/intelligence about route risks from a variety of sources such as police, contractors and drivers. This is an on-going process.

Many drivers are lone worker for most of the day; it is good practice to plan routes that do not place them at additional risk

Drivers should only be permitted to deviate from their designated route if specifically instructed by the emergency services; e.g. an official diversion following an on-road incident. If this occurs, the driver should return to the designated route as soon as is practicable and advise their Transport Manager/Supervisor of the deviation when safe to do so.

Drivers and crew should report anything unusual to the relevant manager as soon as possible.

Whether route planning is conducted or not drivers should also:

- carry out a walk-around security check of the vehicle before departing a company site or customer facility. This includes stops where the vehicle is left unattended during rest/break periods;
- remove and secure the ignition keys, lock the cab doors, tail gate, secure any folk lift, and switch on any alarm or immobiliser whenever they have to leave the vehicle unattended, even when going to pay for fuel or making a delivery;
- avoid stopping for any reason not to do with their work, such as shopping for personal items;

- never carry unauthorised passengers;
- try to keep the vehicle in sight and be able to return to it quickly, if it must be left unattended;
- never leave windows open when away from the vehicle and if they are permitted at any time to sleep in their cabs then they must lock all doors while sleeping;
- contact their operating base whenever they encounter any significant delay, problem or change in consignment details. The driver should not change the pre-agreed routing without prior confirmation from their base

6.15 Overnight parking

It is always better to move hazardous goods so that overnight parking (off site) is not required. If there is a need to park a loaded vehicle overnight transporters should only use pre-planned, secure and approved overnight parking facilities wherever possible.

7 Security for pipeline operations

Where there are National requirements regarding the security of pipelines then gas companies should follow these.

A Security Vulnerability/Risk Assessment (SVA) should be conducted for the transport of product by pipelines starting with the most critical in accordance with the principles set out in AIGA 003/14 Site Security Guidelines[2].

By developing a security plan operators can improve the security of pipeline systems and develop the knowledge and processes for making security related decisions.

Pipeline operators need to:

- Identify and analyse actual and potential events that could result in pipeline security related incidents
- Identify the likelihood and consequence of such events
- Examining and evaluating risks and selecting risk reduction actions
- Establish security conditions and specific protective measures based on the threat level
- Establish and track the security plan effectiveness

The following should be considered as part of the risk assessment process:

- control room access controlled to restrict unauthorized access to the operating controls, related products, and proprietary customer information;
- control and valve stations/ pipeline interconnections / metering stations secured to prevent unauthorized access (examples for an unmanned site include perimeter fence, signage, secured access);
- valves locked to prevent tampering;
- internal and external pipeline bridge crossings - ensure that supports are protected from damage;
- internal and external above ground piping – it is good practice that all pipeline supports and bridge crossing should be provided with anti-climbing devices e.g. spikes, barbed wire, ;
- underground piping – it is good practice to consider use of pipe monitoring equipment (for example, including fibre optics and ground disturbance) particularly when laying new pipes. Some pipes may need CCTV coverage dependent upon the product;
- low temperature protection devices – to ensure they are protected against interference;
- products and other materials imported or exported by pipelines, and
- secondary risks on customer sites caused by supply interruption (e.g. nitrogen supply pipe damaged by intruders)

8 Rail security

It is important to ensure those who transport product by rail on behalf of member companies understand the security issues and risks associated with any product and that they maintain the security of the product in accordance with any legal/regulatory requirements and any additional company requirement.

Due to the risk associated with large quantities of hazardous materials (bulk shipment) the following security procedures shall be followed:

- securement—cargo compartments shall be properly secured;
- inspection—railcars shall be inspected for proper cargo securement and for unknown/suspicious object(s) upon arrival or departure from a facility; and

incident reporting—unusual or suspicious activity shall be reported immediately

Those that provide or use rail as a mean of the shipment of industrial gases products must also comply with the previous sections within this document where they are relevant,

9 Inland water (rivers and canals) security

It is important to ensure those who transport product by water (rivers and canals only, not by sea) on behalf of member companies understand the security issues/risks associated with any product and that they maintain the security of the product in accordance with any legal/regulatory requirements and any additional company requirement.

- Those that provide or use inland waterways as a mean of the shipment of industrial gases products must also comply with the previous sections within this document where they are relevant

10 Vulnerability / Risk assessment

A vulnerability / risk assessment considers the characteristics of a shipment that may cause it to be vulnerable to deliberate attacks, acts of sabotage, theft, or product contamination. Examples of characteristics to consider in a vulnerability assessment include:

- ease of access to shipment by unauthorized persons;
- equipment design, for example, covered trailer;
- size of containers involved and ease of theft;

11 Exposure risk

The member company sending the goods should rank the potential effects of exposure to hazardous materials in transit on the public and the environment, focusing on shipments that may be prone to deliberate acts of sabotage, terrorism, theft, diversion or product contamination.

Factors to consider in ranking possible exposure effects include the following:

- volume of shipment;
- proximity to public events;
- proximity to high population areas;
- proximity to significant landmarks;
- predictability of shipments;
- number of trips;
- trip distance;
- bulk vs. non-bulk; and

- private carrier versus or contract carrier.
- communication mechanisms between carrier, shipper, and customer;
- route selection;
- security trends for mode, carrier, or route used; and
- security procedures of the carrier.
- potential value and or desirability
- employees training, experience, back ground and suitability for position

12 Security documents (electronic or paper) – Good practice

12.1 Markings

Markings shall be applied to security related documents to protect the confidentiality of security measures.

12.2 Applicability

Security information includes:

- security vulnerability and risk assessments (actual assessments, security measures, etc.);
- security plans (policies and procedures);
- training programs (documentation related to training if security information is included); and
- security audits, incident records, related findings, and corrective actions.

12.3 Control of access to security documents

Security documents shall be accessible only to those who have a legitimate need to know.

In order to prevent unauthorized access to security documents, they should be stored in secure location such as locked cupboard, restricted access room or strongbox. Access to these documents should also be tracked and/or recorded.

Electronic security information shall be stored on a secure server and access shall only be allowed to authorised personnel and access to the server shall be password protected.

12.4 Chemicals of concern / hazardous material

Shippers should compile a secure list of transported materials that may be subject to attacks, sabotage, theft, diversion or contamination. Special attention should be given to hazardous products, e.g., materials that are poisonous (toxic), flammable, or explosive.

Refer to Appendix B in AIGA 091/14, Guidance for Qualifying Customers Purchasing Compressed Gases [3] that lists materials classified as chemicals of concern by various organizations.

13 Security incident reporting procedures

All persons should immediately contact their supervisor/management to report any suspicious activity associated with a member companies business.

Local, regulatory agencies and or police should be contacted (following company procedures) of any of the following (this list is not exhausted):

- High-jacking
- Robbery
- Theft of load, part of the load or sensitive documentation;

- Tampering with product, load, security device (broken seal), or load documentation;
- Missing or shortage of freight/product.

14 References

Unless otherwise specified, the latest edition shall apply.

[1] Compressed Gases Association (CGA) standard P-51 Transportation Security Standard for the Compressed Gas industry www.cganet.com]

[2] AIGA003/14 Site Security Guidelines

[3] AIGA 091/14 Guidance for Qualifying Customers Purchasing Compressed Gases

Appendix A Transportation Security Plan (Informative Example)

The following is an example of how a particular site might set out and write its security plan to address the security risks it has identified. EIGA members should adapt the requirements to their own circumstances.

Transportation Security Plan

THIS PLAN IS SENSATIVE. ITS CONTENTS MUST ONLY BE DISCLOSED TO OTHERS ON A "NEED TO KNOW" BASIS AND THEN ONLY THAT PART OF THE PLAN THAT IS APPLICABLE TO THEM.

Company Name :

Site / Location :

Overall Accountability for Security (at site/location) Full Name ……..

The following functions apply to the location:

Function: Full Name

- Consignor or Freight Forwarder :
- Loader / Shipping Agent:
- Filler:
- Carrier:
- *Others: – name them here*

Based on their job description and/or their assignment, the above mentioned employees are responsible for security. *(Organisations may wish to document what aspects of security each has responsibility for)*

A. Personnel security

Verify the following information on employment applications:

- citizenship or immigration status (documentation required);
- references;
- recent employment history; and
- additional information as necessary, for example, background checks.

Employees should have valid government issued photo identification (examples include driver's license, transportation workers identification card, passport,)

Training of all staff with regards to security awareness – records kept with dates of training

B. Product security

Prevent unauthorised access to hazardous / dangerous materials or transport vehicles by non-employees or the general public by implementing on-site, vehicle, and en-route provisions. Include the control measures to reduce security risks

On-site provisions include the following:

- Put list here (include risk assessments and also security provisions whilst on customer sites).

Standard vehicle securement includes the following:

- Put list here.

En-route provisions - take the following into consideration: I.e. routes, stopping points, save havens, travelling in high risk areas or areas that are deemed vulnerable, communications, etc:

- Put list here

C. Remaining effective

The measures for dealing with and reporting security threats, concerns, incidents,

- Put list here

Response to increase risks and or threats levels

- Put list here

Measures to ensure transports loads security provisions are working and remains effective:

- Put list here

D. Review and audit

There should be an agreed timetable for review and audit

Date undertaken……

Who by:……

All issues identified have been action to named individuals against a timetable for completion – YES / NO

(Note - it is good practice to keep a copy of the action plan with this document)

Date of next Review and Audit……

THIS PLAN IS SENSATIVE. ITS CONTENTS MUST ONLY BE DISCLOSED TO OTHERS ON A "NEED TO KNOW" BASIS AND THEN ONLY THAT PART OF THE PLAN THAT IS APPLICABLE TO THEM.