SITE SECURITY GUIDELINES

AIGA 003/14

REVISION OF AIGA 003/07

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 003/14

SITE SECURITY GUIDELINES

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 Compressed Gases Association, document CGA-P-50-2014 (3rd edition) : Site Security Standard. Acknowledgement and thanks are hereby given to CGA for permission granted for the use of their document.

Table of Contents

1 Introduction 1

2 Scope 1

3 Resource information 1

4 Definitions 2

5 Facility security tier ranking 4

6 Security vulnerability assessment 5
- 6.1 Project planning 5
- 6.2 Facility characterization 6
- 6.3 Threat assessment 9
- 6.4 Vulnerability analysis 9
- 6.5 Countermeasure identification 10

7 Physical security 11
- 7.1 General information 11
- 7.2 Signage 12
- 7.3 Perimeter barrier 12
- 7.4 Perimeter clearance 14
- 7.5 Bollards 14
- 7.6 Access control 14
- 7.7 Lighting 16
- 7.8 COC Storage 16
- 7.9 Loss prevention and material control/accountability 16
- 7.10 Control room and systems security 16
- 7.11 Policies and procedures 17
- 7.12 Information (cyber) security 17
- 7.13 Intelligence 18
- 7.14 Incidents 18
- 7.15 Reporting 18
- 7.16 Investigation 19
- 7.17 Analysis 19

8 Crisis management plans and emergency response plans 19

9 Employee and contractor security issues 19

10 Periodic assessment and audit 19

11 References 19

12 Additional information 20

Tables

Table 1—Tier ranking 4
Table 2—Minimum physical security layers of protection 12

Figures

Figure 1—Security vulnerability assessment management process 5
Figure 2—Layers of protection 9

Amendments to AIGA 003/07

Section	Change
	Revised to CGA-P-50-2014 (3rd Edition) for the purpose of adoption
	Technical changes per successive CGA editions are underlined

1 Introduction

In the current atmosphere of terrorist threats and increased criminal activity, security has become an integral part of the industrial gas industry culture. Like safety measures, security measures protect facilities, employees, and the community by reducing the risk of a wide range of threats and mitigating the effects of incidents such as vandalism, sabotage, workplace violence, and terrorism. Security measures enhance process safety management (PSM), risk management programs (RMP), worker safety, and environmental protection.

A security program should include the following elements:

- site screening for risk prioritization;
- security vulnerability assessment (SVA);
- incident reporting and investigation;
- emergency response and crisis management;
- employee and contractor security issues; and
- periodic reassessment; and
- employee security awareness training

The Compressed Gas Association (CGA) thanks the Centre for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers for granting permission to reproduce and adapt large sections of its book *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* [1].[1]

2 Scope

This publication provides instruction to the industrial gas industry for assessing security risks and identifying and implementing preventive security measures at fixed sites. It is intended as a resource to help managers at individual facilities make security decisions based on risk.

The publication does not attempt to provide an all-inclusive list of security considerations for industrial gas companies nor does it address transportation security and security at customer sites. Additional security information is contained in AIGA 043/14 , *Transportation Security Standard for the Compressed Gas Industry*, and AIGA 091/14 *Security Standard for Qualifying Customers Purchasing Compressed Gases* [2, 3].

3 Resource information

This publication was developed using resource material from CCPS and the American Chemistry Council (ACC). The ACC *Site Security Guidelines for the U.S. Chemical Industry* is a helpful reference for companies seeking information in the following areas:

- risk assessment and prevention strategies;
- security policies;
- collaboration with other corporate departments and with local, state, and national law enforcement agencies, local emergency planning committees, etc.;
- incident reporting systems;
- employee training and security awareness;
- incident investigations;
- emergency response and crisis management;

[1] References are shown by bracketed numbers and are listed in order of appearance in the reference section.

- periodic reassessment of the security plan for physical security including access control, perimeter protection, intrusion detection, security officers, ongoing testing and maintenance, and backup systems;
- employee security measures including prudent hiring and termination practices;
- workplace violence prevention and response; and
- information, computer, and network security [4].

The ACC *Site Security Guidelines for the U.S. Chemical Industry* and other reference documents are available at the ACC public website.[2]

4 Definitions

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

4.1 Adversary

Individual, group, organization, or government that conducts activities or has the intention and capability to conduct activities detrimental to critical assets.

NOTE—Adversaries can include foreign intelligence services, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can also include site insiders, site outsiders, or the two acting in collusion.

4.2 Asset

Person, environment, facility, material, information, business reputation, or activity that has a positive 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.

4.3 Chemical of concern (COC)

Chemical that is a likely target for terrorist or criminal activity.

4.4 Consequence

Amount of loss or damage expected from a successful attack against an asset.

NOTE—Loss can be monetary but can also include political, morale, operational, or other impacts. Some examples of relevant consequences in a security vulnerability assessment include injury or death; significant disruption to public, private, or company operations; environmental damage; financial loss; loss of critical data; and loss of reputation.

4.5 Countermeasure

Action taken or physical capability provided to reduce or eliminate vulnerabilities.

4.6 Cyber security

Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

4.7 Delay

Countermeasure strategy that provides various barriers to slow the progress of an adversary's attempt to penetrate a site.

NOTE—A delay strategy is intended to prevent theft or attack.

4.8 Detect

Countermeasure strategy that identifies an adversary attempting to commit or in the process of committing a terrorist or criminal activity.

NOTE—Detection includes real-time observation, post-incident analysis, and identification of the adversary.

[2] www.responsiblecaretoolkit.com.

4.9 Deter
Countermeasure strategy that prevents or discourages a breach of security by causing fear or doubt.

NOTE—Physical security deterrence includes warning signs, lights, uniformed guards, cameras, and barriers.

4.10 Intelligence
Information that characterizes specific or general threats including the motivation, capabilities, and activities of adversaries.

4.11 Intent
Course of action that an adversary intends to follow.

4.12 Layers of protection
Multiple independent, overlapping layers of security.

NOTE—Layers of protection can include counter surveillance, counter intelligence, physical security, and cyber security (concentric rings of protection).

4.13 Mitigation
Action that causes a consequence to be less severe.

4.14 Physical security
Security systems and architectural features that increase protection.

NOTE—Examples include fencing, doors, gates, walls, turnstiles, locks, vehicle barriers, and hardened glass.

4.15 Risk
Potential for damage to or loss of an asset.

NOTE—Risk in the context of chemical process security is the potential for a catastrophic outcome. Examples include intentional release of hazardous materials to the atmosphere, theft of chemicals that can be used as weapons or for other criminal activities, contamination of chemicals that can later harm the public, or economic costs of the damage or disruption of a chemical process.

4.16 Risk assessment
Process of predicting the likelihood that an adversary will successfully exploit a company's vulnerability as well as predicting the resulting consequences.

NOTE—A risk assessment provides the basis for rank ordering risks to establish priorities for the application of countermeasures.

4.17 Security plan
Document describing a plan that addresses security issues and related events including security assessment and mitigation options.

NOTE— A security plan includes security alert levels and response measures.

4.18 Security vulnerability 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.

4.19 Target attractiveness
Estimate of the value of a target to an adversary.

4.20 Technical security
Electronic systems for increased protection (or for other security purposes).

NOTE—Technical security can include access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, motion detectors, annunciating and reporting systems, central stations

monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

4.21 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 promote political or social objectives.

4.22 Threat

Indication, circumstance, or event that can cause loss of or damage to an asset, or the intention and capability of an adversary to cause loss of or damage to an asset.

4.23 Vulnerabilities

Weakness that can be exploited by an adversary to gain access to an asset.

NOTE—Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel practices and behaviours, locations of people, equipment, and buildings, or operational and personnel practices.

5 Facility security tier ranking

Facility security ranking is divided into four levels (Tiers 1-4). Tier 1 is the highest level of concern.

Tier rankings are determined by the classification and quantity of chemicals of concern (COC) present at a site in addition to consideration of the following risk factors:

- intentional equipment damage or malicious release with loss of containment of hazardous chemicals resulting in multiple casualties, severe site damage, and significant public or environmental impact;
- chemical theft with the intent to cause severe harm at the facility or off site, or the intent to use the chemical for illegal activity; and
- contamination of product that causes harm to workers or to the public at the facility or off site.

Short term storage (less than 48 hours) for items in transport does not affect the overall tier ranking of a facility. See 7.8 for additional information.

Table 1 contains the COC and quantities that determine tier ranking. For detailed information on COC, see. Appendix A Table – Chemicals of concern, which is also shown in CGA P-53, Security Code Top Screen.

Table 1—Tier ranking

Rank	COC	Quantity
Tier 1	Chemical of Concern that could be used to create a weapon of mass destruction - see Appendix A[1] – Toxic, 2.3, hazard zone A with the exception of chlorine – Toxic, 2.3, hazard zone B with the exception of chlorine	Any quantity
Tier 2	Chemical of Concern that could be used to create a weapon of mass destruction - see Appendix A[1] – Toxic, 2.3, hazard zone C and chlorine – Toxic, 2.3, hazard zone D and chlorine DEA	Cylinders > 2000 lb (910 kg) Bulk > 15,000 lb (6820 kg)
	Flammable bulk	> 100,000 lb (45,460 kg)
Tier 3	Chemical of Concern – Toxic, 2.3, hazard zone C and chlorine – Toxic, 2.3, hazard zone D and chlorine DEA	Cylinders < 2,000 lb (910 kg) Bulk < 15,000 lb (6820 kg)

	Flammable bulk	10,000 lb(4,550 kg) to 100,000 lb(45,460 kg)
	Oxygen bulk	> 250,000 gal(946,250 litres)
Tier 4	Nitrous oxide (cylinders or bulk)	Any quantity
	Flammable bulk	< 10,000 lb(4,550 kg)
	Oxygen bulk	< 250,000 gal(946,250 litres)

6 Security vulnerability assessment

The SVA is used to determine which assets require protection, the threats that can be posed against those assets, and the likelihood and consequences of attacks against those assets. The SVA is intended to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, to protect the facility from malicious acts, and to evaluate the countermeasures to ensure the protection of the public, personnel, national interests, the environment, and the company. Figure 1 depicts a flow chart for the SVA management process.

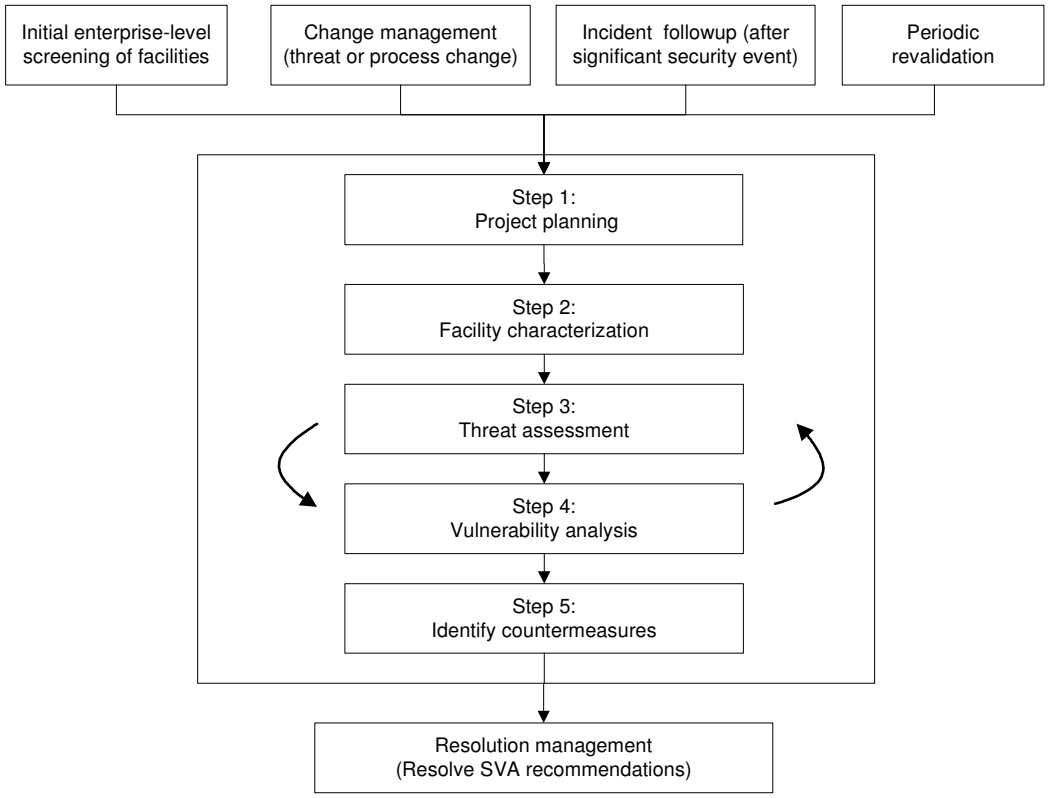

Figure 1—Security vulnerability assessment management process

There are a number of methodologies available for conducting an SVA. At the request of the ACC, CCPS developed an SVA methodology and established a set of criteria to define minimum acceptable standards for an SVA. See Section 12 for information on the websites where CCPS and other SVA methodologies are available.
Project planning

6.1 Project planning

SVA planning includes the selection of a multidisciplinary team skilled in security and process safety to conduct the analysis, determine the objectives and scope, and develop a plan to address the individual sites based on the initial screening that was performed.

6.1.1 Team selection

An SVA team typically consists of three to eight individuals. The size of the team is determined taking into consideration the facility complexity, hazards present, and expertise of the team members. One person should serve as the team leader. The team should have skills in security, process safety, and plant operations including SVA methodology, process safety analysis, and security procedures, methods, and systems.

6.1.2 Objectives

Defining objectives helps focus the SVA effort on issues that are of vital interest to the employees, the company, the industry, and the public. A key consideration should be the protection of the public from a terrorist or criminal event using chemicals obtained or released on site or off site.

6.1.3 Scope

The SVA team determines which facilities and threats (security event types) a company wants to address in the SVA process.

6.2 Facility characterization

Facility characterization includes identifying the potential target assets, locating information that describes the technical details of those assets to support the analysis, identifying the hazards and consequences of concern for the site and its surroundings, identifying existing layers of protection, and determining the target attractiveness.

6.2.1 Identifying critical assets

Examples of critical assets include but are not limited to:

- COC processed, stored, manufactured, or transported (see Appendix A);
- storage tanks;
- processing vessels;
- piping to interconnect systems;
- process control systems;
- operating personnel;
- utilities (power, water, natural gas, telecommunications systems);
- waste water treatment;
- business information;
- business management computer systems;
- company image;
- community relations; and
- customer relations.

6.2.2 Identifying hazards

The SVA team should identify and understand the hazards and the effect loss or damage would have on the assets. The team should review chemical process, storage, and hazard information as well as information about the facility to develop a list of assets that are potential targets requiring further analysis.

The SVA team should review the following information:

- lists of COC including raw materials, intermediates, and finished goods present at the facility that are likely to be potential targets of malicious acts, such as:
  - inhalation poisons
  - material destined for the food, nutrition, cosmetic, or pharmaceutical chains
  - chemicals that are susceptible to destabilization;
- chemical vessels and equipment, their location, volume, average contents, and construction;
- facility and process drawings including plot plans, piping and instrument drawings, and process flow diagrams;
- other relevant process safety information;
- PSM and RMP process hazard analysis studies and hazard assessments generated for the facility;
- information to support an estimate of the asset's criticality in terms of company, regional, industry, and national economic activity and in terms of the potential consequences;
- available security intelligence and information shared with national or local law enforcement officials;
- information on the plant and local area population and environment that can be impacted by a chemical security incident;
- reports on previous incidents of process safety and security events;
- security procedures;
- computer/control/communications (cyber attack issues); and
- utility issues, for example, critical cooling water supply.

The SVA team should determine whether the facility contains any chemicals or other assets that are harmful to or whose loss would be critical to the following:

- public surrounding the facility;
- company viability;
- regional or national chemical industry;
- regional or national economy; or
- national security, especially military applications.

6.2.3 Consequence analysis

The off site consequence analysis provides an understanding of the potential consequences of a successful adversary attack. It is up to the judgment of the SVA team to define the consequences of an attack. Examples include but are not limited to:

- potential consequences to the neighbouring population and the impact on assets;
- potential consequences associated with chemical thefts;
- for a cyber attack, the sudden shut down of a process resulting in an upset and loss of production;
- deliberate contamination of medical or food gas products potentially resulting in loss of life or
- shutdown the facility activities, which impacts your customer needs.

Consequences are generally described to help the team evaluate which substances and assets are of more concern and to determine the need for further analysis and countermeasures. In developing countermeasures, the SVA team should consider worst-case consequences first because doing so can eliminate the need to address lesser consequences.

6.2.4 Evaluation of target attractiveness

The attractiveness of the target to the adversary is a key factor in determining the likelihood of an attack. Examples of issues to consider are:

- proximity to a symbolic or iconic target such as a national landmark;
- potential to attract widespread negative media attention; or
- any other variable the SVA team determines has an impact on the site's value as a target.

Experience has shown, particularly for terrorist attacks, that some targets better accomplish the objectives of an adversary than others. Since the SVA is a risk-based, analytical approach, consideration shall be given to attractiveness factors when defining the threat and determining the need for any enhanced countermeasures.

Factors that determine target attractiveness are:

- potential for mass casualties or fatalities;
- potential for extensive property damage;
- proximity to national assets or landmarks;
- possible disruption or damage to critical infrastructure;
- disruption of the national, regional, or local economy;
- ease of access to target;
- media attention or possible interest of the media; and
- company reputation and brand exposure.

6.2.5 Layers of protection review

The SVA team identifies and documents the existing security and process safety layers of protection. This can include physical security, cyber security, administrative controls, and other safeguards. The security concept of layers of protection is based on the idea that for an undesired event to occur (accidental or malicious), a number of protective features and countermeasures must fail. Figure 2 shows an example of layers of protection.

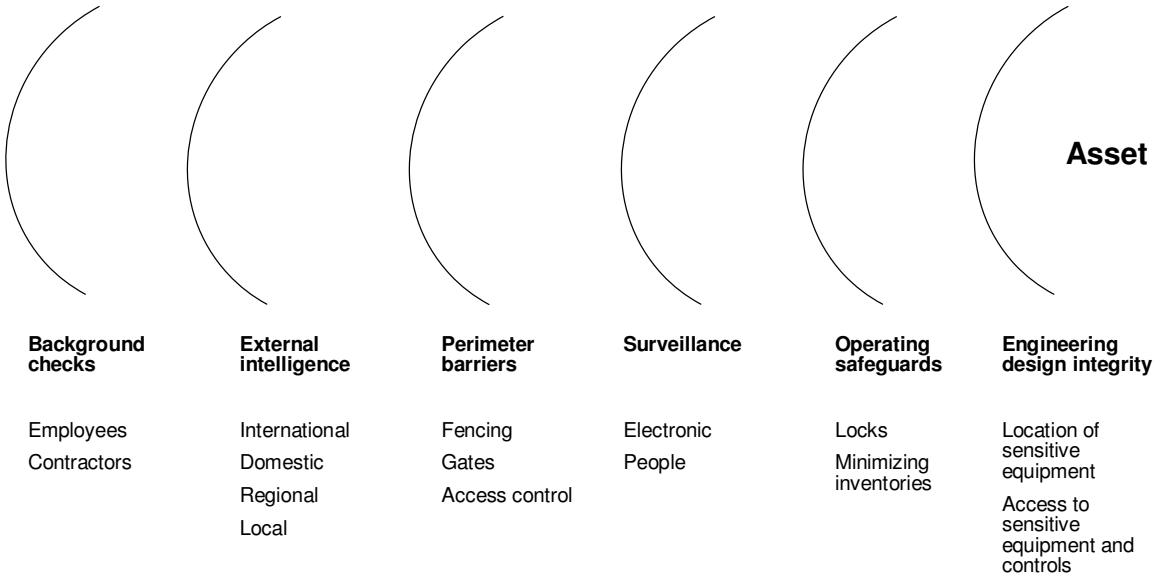

Figure 2—Layers of protection

6.2.6 Potential target list

3Appendix A identifies the COC that are potential targets. Each potential target should be evaluated for the following:

- level of hazard;
- specific value as a target;
- specific reason it has value as a target; and
- specific security needs associated with that target [5].

6.3 Threat assessment

Attacks can be committed by insiders, outsiders, or a combination of the two. Insiders are personnel that have routine, unescorted site access. Collusion between insiders and outsiders can be the result of monetary gain (criminal insider and terrorist outsider), ideological sympathy, or coercion. Once the facility is characterized and the assets and targets identified, the threats to identified targets should be evaluated. The threat assessment should include reasonable local, regional, or national intelligence information where available.

When assessing threats, security professionals should evaluate intent as well as capabilities. To determine intent, the motivation, goals, objectives, and specific events that might trigger the adversary to act shall be closely examined. The questions that should be asked about intent include:

- Does the adversary have a current or projected need for this asset?; and
- Does the adversary seek to deny or destroy the use of the asset?

6.4 Vulnerability analysis

The vulnerability analysis consists of pairing each asset and threat to identify potential vulnerabilities related to security events. This includes identifying existing countermeasures and their level of effectiveness in reducing those vulnerabilities.

6.4.1 Asset and threat pairing

Each asset that needs to be protected is paired with various threats. If a general terrorist threat is the only threat to be analyzed, this step is relatively simple.

6.4.2 Asset assessment

This asset-based approach is a top-down approach. For the asset-based approach, the details of numerous scenarios that can cause security events are not further documented. The asset-based approach is recommended because it is less complex and easier to accomplish than the scenario-based approach and is more applicable to the industrial gas industry. Each area of the plant that is considered an area of concern or potential target for the selected threat is identified and discussed. The key questions that should be answered are:

- What events for a particular target, for example, tank rupture, theft, process disruption, power loss, or cooling loss will cause the release of a chemical in a way that will result in the most serious consequences? For example, is this a chemical that:
  - If released to the atmosphere in a sufficient quantity, it can cause death or serious injury to a significant number of people?
  - If stolen, it can be used to produce chemical weapons or illegal drugs?
  - When in process or storage, it is vulnerable to sabotage, producing an uncontrollable reaction or a threat to human health and safety?; and
- If this asset is compromised, will the company will be unable to operate? For example, is this asset:
  - Key, irreplaceable process equipment?
  - Computer systems and process control?
  - Elements that will cause other catastrophic outcome?

This part of the analysis requires brainstorming by the SVA team. Given the security issue(s) relative to the potential target recorded in the previous step, the team shall estimate the specific consequences. For example, where the potential target is a storage tank or container of a toxic material that is an inhalation hazard, the security issue may be a deliberate release by an attack on the tank or container. Regardless of what causes a release, the consequence of such an attack remains the same. It is either extreme or very high. Therefore, the tank or container is determined to be a high value (to the attacker) target.

The team next considers the protective layers around the potential target including security, lighting, distance from public access areas, barriers, the construction of the tank/container, and other factors affecting the potential for and the potential results of an attack on that particular tank or container.

When the asset assessment is complete, the team will have identified key targets and have an understanding of the possible threat against each target.

6.4.3 Risk analysis/ranking

After identifying key assets and their worst-case threats and consequences, each asset should be ranked to prioritize the assets so appropriate countermeasures can be applied to each situation.

6.5 Countermeasure identification

Countermeasures include hardware, technical systems, software, interdictive response, procedures, and administrative controls. During the SVA process, an assessment is made of the effectiveness and reliability of the countermeasures against the threats and vulnerabilities of the assets. If deemed necessary based on the level of risk, enhanced countermeasures can be considered for ways of improving the existing security systems.

Examples of countermeasures include:

- physical security (see Section 7);

- loss prevention, material control, and inventory management;
- control room and systems security;
- crisis management and emergency response (see Section 8);
- policies and procedures;
- information technology (cyber) security; and
- intelligence.

The SVA team and management can use certain key concepts to evaluate whether existing countermeasures are adequate. Security risk reduction at a site can include the following strategies:

- deter, detect, and delay principles;
- physical or cyber layers of protection;
- procedures and administrative controls; and
- inherently safer systems to the extent that they can be designed and installed practically, particularly for existing processes.

Each site should have a plan to react to the discovery of a security breach or to the consequences of a security event. This can include the notification of law enforcement.

A countermeasure analysis is an exercise where the team identifies gaps between the existing security level and the desirable security based on risk and assesses the need for added countermeasures. Each potential target is protected against the highest level threat associated with it. At this point, the SVA team decides what level of risk reduction is achieved if the selected measures are implemented. These analyses should be documented.

Based on the consequences and likelihood that the layers of protection are breached, appropriate enhancements to the security countermeasures can be recommended. These include improved countermeasures that follow the principles of deter, detect, delay, diminish, mitigate, and possibly prevent. This step should also include the development of an appropriate SVA report or documentation, which can be used to communicate the results of the SVA to management for appropriate action.

The SVA team and management should determine whether existing countermeasures are adequate or whether additional countermeasures should be implemented to protect an asset.

Once the SVA is completed, it is necessary to follow up on the recommended enhancements to the security countermeasures so they are properly reviewed, tracked, and managed until they are resolved. Resolution can include adoption of the SVA team's recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Reasons for rejection of an SVA recommendation should be well documented.

7 Physical security

7.1 General information

The objective of physical and information security is to deter, detect, and delay a malicious act. Examples of physical security include:

- barriers that deter and delay movement along a pathway leading to an intended target, such as, perimeter protection, fencing, walls, landscaping;
- detection equipment that provides warning of unauthorized entry, for example, intrusion detection sensors and systems, video surveillance, alarm monitoring consoles; and
- communication equipment, for example, radio (fixed and portable), telephone, and intercom subsystems.

Table 2 contains the minimum physical security layers of protection requirements, which are based on a facility's security tier ranking.

NOTE—The requirements of the national authority having jurisdiction can supersede the security requirements in Table 2.

Communicate increased physical security at a facility (hardening target) with local first responders because these changes can have an impact on their response plans and procedures. For example, an access control gate may require a KNOX (high security)box

7.2 Signage

Signage provides clear communication of a facility's access policies.

General signs should describe company access restrictions and should be posted at main entry points and visitor areas.

PRIVATE PROPERTY and NO TRESPASSING signs should cover the full perimeter and should be posted at regular intervals based on the requirements of the authority having jurisdiction.

7.3 Perimeter barrier

A structural barrier (fence or wall) physically and psychologically deters or discourages the undetermined perpetrator, delays the determined perpetrator, and channels the flow of authorized traffic through entrances. A perimeter fence or wall is composed of two parts–structure and top guard.

Table 2— Recommended physical security layers of protection

Required layers of protection	Tier 1	Tier 2	Tier 3	Tier 4	Sections containing additional information
Perimeter					
Signage					7.2
– NO TRESPASSING posted at regular intervals	X	X	X	X	
– General security advisory posted at main entry points	X	X	X	X	
Barrier					7.3
– Structure	X	X	X	X	7.3.1
– Top guard	X	X	X	X	7.3.2
Clearance					7.4
– Interior	X	X	X	X	
– Exterior (applicable to company property)	X	X	X	X	
Bollards	O	O	O	O	7.5
Access control [1)]		[1)]	[1)]	[1)]	7.6
Access points					
– Building, exterior door	X	X	X	X	
– Main gate	X	X	X	X	
– Vehicle or construction gate	X	X	X	X	
– Personnel gate	X	X	X	X	
– Emergency exit	X	X	X	X	
Access control methods					
– Uniformed security guards	O	O	O	O	
– Controlled access system					
– Electronic (key pad, card, etc.)	X	O	O	O	7.6.1
– Manual (lock/key [key control process])	N	X	X	X	7.6.2
Facility security systems					

– Closed circuit TV (CCTV)/video motion detection (VMD) or infrared (IR)	X	O	O	O	
– Electronic alarm systems, external (external IR, contacts door and breakage windows)	O	O	O	O	
– Electronic alarm systems, internal (interior motion, door contact, heat detection, etc.	X	O	O	O	
Lighting					7.7
Perimeter	X	X	X	X	
Facility building (all sides)/parking lot	X	X	X	X	
Bulk storage	X	X	X	X	
Toxic storage	X	X	X	X	
Fill zones	X	X	X	X	
COC storage (and nitrous oxide) bulk and cylinders storage (full and empty)					7.8
Inventory control	X	X	X	X	
Access control	X	X	X	X	
– Secondary layer of security (security systems, storage building, cages, secondary fence/gate, bulk storage lockout controls [to reduce unauthorized release])	X	X	X	X	
– Security systems (can use any of the following 3 categories)	X	O	O	O	
– CCTV/VMD or IR					
– Electronic alarm system, external (exterior IR, contacts door and breakage windows)					
– Electronic alarm systems, internal (interior motion, door contact, heat detection, etc.)					

O = optional areas of security
X = required areas of security
N = not authorized
[1)] At a multi-business site, a facility's SVA and security plan may indicate the need for multiple tiers within the site. For example, an air separation unit (ASU) ranked Tier 3 can store Tier 1 product in a restricted area.

7.3.1 Structure

New construction should have a 7-ft (2.1 m) perimeter barrier. A 6-ft (1.8 m) perimeter barrier is permitted for existing or replacement construction if the structure is in good condition. Perimeter barriers can be constructed of a variety of materials including:

- chain-link fences
  - standard mesh (9 gauge mesh, 2-in [5.1 cm] diagonal opening)
  - high security mesh (less than 1-in [2.5 cm] opening)
  - bottom and top railing or tension wire;
- expanded metal and welded wire fabric fences
  - secure mesh (expanded metal)
  - architectural or decorative; and
- masonry fences
  - brick
  - reinforced or hollow block
  - poured form concrete or prefabricated.

7.3.2 Top guard

A top guard is placed above the barrier structure to deter unauthorized entry by climbing or scaling the barrier. Material commonly used for top guards include barbed wire, barbed tape, and spikes. A top guard can be included in the architectural or decorative design. Examples of top guards include:

- angle guard consisting of 3-strand wire;

  NOTE—A 3-strand, 45-degree arm should be angled away from the secured area.

- V-shaped guard consisting of 3-strand barbed wire (increased deterrent); and
- coil consisting of tape or ribbon.

  NOTE—single or multiple coils placed around/through 3-strand wire provides maximum protection.

Facilities should check local codes and ordinances regarding top guard material, application, and minimizing the negative visual impact of physical security on public or open property.

7.4 Perimeter clearance

Adequate clearance ensures clear visibility and allows inspection and integrity verification of a fence line. Wherever possible the clear zone should be equal to the height of the structure of the barrier. The clear zone shall be kept free of objects that can damage the perimeter or facilitate unauthorized entry, such as, saplings, weeds, overhanging tree branches, stored materials, etc.

7.5 Bollards

Permanent or temporary bollards are used at access points and full plate windows to deter and delay unauthorized entry. Bollard design can be ornamental to reduce negative visual impact on customers.

7.6 Access control

Control over personnel, property, and vehicles that pass through a site's perimeter is an essential feature of physical security. Effective access control deters unauthorized personnel or vehicles from entering a facility. The following are typical access control measures:

- requiring government issued photo identification, such as, driver's license or transportation worker's identification credential for visitors and contractors;
- issuing and controlling visitor and contractor identification badges;
- escorting visitors as required;
- maintaining a visitor log that includes the date, visitor's name (name printed and signed), citizenship, local contact, and visitor badge information;

  NOTE—A log is not required in public domain areas, such as, retail store operations.

- signing visitors and contractors in and out;
- numbering badge(s) to ensure that missing badges are identified; and
- using property passes to control the flow of material into and out of the site.

NOTE—At a multi-business site, a facility's SVA and security plan may indicate the need for multiple tiers within the site. For example, an ASU ranked Tier 3 can store Tier 1 product in a restricted area.

7.61 Electronic security systems

Because of the variety of industrial gas facilities, electronic security system design should be based on the facility's design. The following elements should be considered:

- external electronic security
  - CCTV/VMD
    - motion detection
    - activated alarm system
  - yard beam
    - electronic IR beams
    - multiple beams
  - fence
    - motion/noise detection
    - variety of designs and applications;
- internal electronic security
  - standard—contact alarm
    - door contacts and motion detectors
    - back up power, minimum 120 minutes
    - loss of power/signal alarm—security vendor control centre
    - internal reporting—system, activation/deactivation—for internal review purposes
  - additional internal coverage
    - detection of window breakage
    - infrared beams
    - noise sensors; and
- CCTV coverage
  - main entry
  - emergency exits
  - retail store counter and register area.

7.6.2 Physical security systems

7.1.1.1 Windows/doors

Bars or wire mesh can be used for temporary and permanent windows and doors. Window and door design can be ornamental to reduce negative visual effect.

7.6.2.1 Security lock and key systems

Security lock and key systems can include:

- common locks (unrestricted application);
- high-security locks (restricted application)
  - all-weather design with shackle shroud
  - key control policy; and

- chains
  - at a minimum, 3/8-in (9.5 mm) hardened carbon, boron manganese alloy steels with surface hardness sufficient to resist cuts from hacksaws or 1 yard bolt cutters.

7.7 Lighting

Lighting is used to reduce dark zones. Foot-candles/lumens usage is based on the facility security design and local codes. Primary lighting coverage areas include:

- entry points, for example gates and buildings;
- driveways and internal roads;
- perimeter (coverage is based on the site security rating);
- loading zones;
- bulk storage area; and
- COC storage area.

7.8 COC Storage

COC storage should have secondary containment for all full and empty containers of products classified as a chemical that could be used to create a weapon of mass destruction (see APPENDIX A[1]) and for all full and empty containers of nitrous oxide. COC storage includes:

- inventory control (full and empty); and
- access control
  - lock and key or key card (key card is recommended)
  - cage, pen, secured pallet, secured room, or bunker based on facility and facility security plan.

    NOTE—Based on COC product(s) and volume(s), a security system or CCTV can be used.

As part of a cross-dock function, facilities can store products that have a tier ranking that is higher than the facility's overall tier ranking for up to 48 hours. Security requirements for these products include the use of secondary layers of protection, applicable security systems, and inventory control.

7.9 Loss prevention and material control/accountability

The current security environment requires a new emphasis on material control and accountability. There are many chemicals that can be used directly or indirectly for terrorist or criminal activity. It is therefore critical that every site impose the controls necessary to reduce the likelihood of theft. Examples include:

- Securing buildings and areas that contain materials or information that requires safeguarding. Consideration should be given to establishing restricted areas within the site with additional barriers;
- Maintaining proper inventory controls (full and empty) COC, an internal document retention program, and internal review process for discrepancies; and
- Securing areas such as research and development areas and buildings, maintenance areas (shops); shipping and receiving areas (particularly where hazardous materials are handled), pipelines and their valving, storage tanks, vessels, and tank farms.

7.10 Control room and systems security

Control room and systems security establishes physical security and procedural control measures that provide for the integrity of control rooms, distributed control systems (DCS), and process logic controllers (PLC). System integrity is a critical factor in the security of facilities. A key feature in the overall system security program is

restricting access to the system itself. To accomplish this, management must rely heavily on control of physical space and physical connection by implementing the following or similar measures:

- providing additional barriers for the control rooms;
- not allowing uncontrolled items and materials into the control room;
- providing DCS and PLC that limit access to process control equipment to authorized personnel only; and
- having control systems with appropriate password protection and other protective features.

7.11 Policies and procedures

Company and site policies and procedures should be generated or revised to include security and its related functions and how security functions will be organized, executed, and managed. Typical polices and procedures may include:

- security awareness training;
- employee termination procedures;
- mail handling and suspicious parcel and package procedures;
- inspection of incoming vehicles and rail cars for contraband, explosives, or unauthorized personnel;
- handling of bomb threats;
- incident reporting;
- background screening of employees and contractors;
- positive identification of all personnel requesting access to the facility;
- information protection and security; and
- cyber security.

7.12 Information (cyber) security

The objective of cyber security is to protect critical information and systems including hardware, software, infrastructure, and data from loss, theft, or damage. Cyber security is a highly complex and evolving subject that requires specialized training and knowledge.

Protecting information and computer networks in a chemical facility means more than safeguarding a company's proprietary information. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases. To an adversary, information and network access can provide the power to harm the company, its employees, and the community at large.

Examples of cyber security procedures can include the following:

- Physically secure computer rooms, motor control centres, rack rooms, server rooms, telecommunications rooms, and control rooms;
- Provide firewalls, periodically changed passwords, virus protection, encryption, user identification, and message and user authentication to protect both the main computer network and any subsidiary networks such as access control systems that are connected to it or to the outside;
- Control access to the process control system from remote computers;
- Limit information from leaking from the site by limiting, to the extent possible, radio transmissions that contain operational or process information;
- Require the systems administrator to disable all internet connection software that can be prepackaged in operating systems;

- Allow the principles of least access, need to know, and separation of functions to guide the determination of user authorizations rather than position or precedent;
- Locate the computer room above the first floor of the building to reduce the likelihood of theft and water damage (from broken water lines, floods, or firefighting). The computer room should not be adjacent to an exterior building wall;
- Do not post signs indicating the location of the computer facility;
- Equip the computer room with adequate communications capabilities to facilitate prompt reporting of emergencies;
- Allow only authorized personnel physical access to central computer rooms, and supervise any visitors;
- Do not give keys or lock combinations to visitors;
- Require employees to notify management in advance if they wish to gain entry to the computer facility during hours when they are not scheduled to be working; and
- Maintain an audit trail of access to system resources.

Guidance on cyber security is contained in the American Chemistry Council (ACC) Chemical Information Technology Council (ChemITC).[3]

7.13 Intelligence

Sites should monitor intelligence sources to identify threat exposures and should liaise with local and

national law enforcement groups

7.14 Incidents

Improving security depends on reporting, investigating, and analyzing all security-related incidents, including suspicious activities.

7.15 Reporting

All security incidents that involve suspicious activity should be reported to the designated level of management in an organization. Keeping detailed records of security incidents allows companies to spot trends and piece together information that leads to successful investigations and corrective actions. In addition, any suspicious activity should be reported to the appropriate level of law enforcement. Examples of security incidents that should be reported include:

- doors not secured, holes in fence lines, and indication of illegal entry;
- unauthorized entry or exit by personnel in restricted areas of the facility;
- signs of vehicles in restricted areas along pipelines, fence lines, electrical substations, or remote plant security gates;
- individuals asking for technical information about the facility that could be used by an adversary to cause harm;
- unexplained process upsets;
- unexplained loss of containment of hazardous material;
- unexplained loss of raw material or product; and
- cyber attack against internal process control systems.

[3] American Chemistry Council (ACC) Chemical Information Technology Council (ChemITC) www.chemicalcybersecurity.com

7.16 Investigation

All suspicious activities and security incidents should be investigated. The critical findings of the investigation should be documented and any resulting corrective action(s) implemented.

7.17 Analysis

Each company should establish a single collection point for all security incident information, which will allow companywide sharing of information and analyses of all available data. Periodically, all security incidents and suspicious activity reports should be reviewed and analyzed to identify any common trends. This information can then be used to develop and implement companywide corrective actions with the goal of improved security. Some security managers use incident management software, which has graphing, charting, and search functions that can help bring an offense or loss pattern to light and identify issues of security concern.

8 Crisis management plans and emergency response plans

Crisis management plans (CMP) and emergency response plans (ERP) are integral parts of a company's overall security management program and may prevent an intrusion or attack from becoming a major incident. This section does not attempt to specify how a company should respond to emergencies and manage crises. Measures that managers may consider include:

- developing and implementing a CMP and an ERP that fit the specific facility's needs and resources and establishing communications with local, and national responders as necessary (law enforcement, fire, health [emergency medical technicians], etc.);
- developing a system that accounts for employees and visitors during emergencies;
- developing procedures to control the incident so evidence will be preserved for later investigations;
- developing a crisis communication system for key personnel and security staff; and
- conducting regular drills and exercises to test the effectiveness and increase awareness of CMP and ERP.

9 Employee and contractor security issues

It is possible for threats to come from within as well as from the outside. Disgruntled employees and former employees sometimes pose a risk. Background screening can help companies identify job candidates, employees, and contractors with criminal histories. Workplace violence policies, awareness, and response plans can help forestall other threats. Companies should address these issues in their overall corporate security program.

10 Periodic assessment and audit

Managers should review their security measures periodically. When a facility's assets, products, layout, or personnel change or various threats increase or diminish, it may be necessary to review the SVA. It may also be necessary to do the following:

- update risk assessments and site surveys;
- review the level of employees' and contractors' compliance with security procedures;
- consider whether security procedures need modification; and
- establish ongoing testing and maintenance of security systems (such as access control, intrusion detection, and video surveillance).

In addition, companies should expand their auditing procedures to address site security equipment, training, policies, and procedures.

11 References

Unless otherwise specified, the latest edition shall apply.

[1] *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, Centre for Chemical Process Safety, American Institute of Chemical Engineers, Three Park Ave., New York, NY 10016. www.aiche.org/ccps

[2] AIGA 043/14, *Transportation Security Standard for the Compressed Gas Industry*, Asia Industrial Gases Association, 3 HarourFront Place, HarbourFront Tower 2, Singapore 099254, www.asiaiga.org

[3] AIGA 091/14 *Security Standard for Qualifying Customers Purchasing Compressed Gases*, Asia Industrial Gases Association,3 HarourFront Place, HarbourFront Tower 2, Singapore 099254, www.asiaiga.org

[4] *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, 1300 Wilson Blvd., Arlington, VA 22209. www.americanchemistry.com

[5] CGA P-53, *Security Code Top Screen*, Compressed Gas Association, 4221 Walney Rd., 5th Floor Chantilly, VA 20151. www.cganet.com

12 Additional information

CCPS and other SVA methodologies including forms are available from the following websites:

- www.responsiblecaretoolkit.com;
- www.aiche.org/ccpssecurity; and
- www.dot.gov.

CCPS also offers a wide range of references that support vulnerability analysis and risk analysis. These are available at www.aiche.org/ccps

Physical Security Measures Guideline, American Society of Industrial Security. www.asisonline.org

Business Continuity Guideline, American Society of Industrial Security. www.asisonline.org

Appendix A - Chemicals of concern

The products listed in Appendix A are classified by a number of government and global organizations as weapons of mass destruction (WMD) or products that can be used to produce WMD or illegal drugs.

Chemical name	C.A.S No.	Comments
Acetylene	74-86-2	Greater than 4,540 Kg 10 000 lbs
Ammonia[1]	231-635-3	Any quantity
Ammonium nitrate	6484-52-2	Any quantity
Arsenic[1]	7440-38-2	Any quantity
Arsine (arsenic hydride)[1]	7784-42-1	Any quantity
Boron tribromide	10294-33-4	Any quantity
Boron trichloride	10294-34-5	Any quantity
Boron trifluoride [1]	7637-07-2	Any quantity
Bromine trifluoride	7787-71-5	Any quantity
Carbon monoxide	630-08-0	Greater than 4,540Kg 10,000lbs
Chlorine [1]	7782-50-5	Any quantity
Chlorine pentafluoride	13637-63-3	Any quantity
Chlorine trifluoride	7790-91-2	Any quantity
Cyanides[1]		Any quantity
Cyanogen	460-19-5	Any quantity
Cyanogen chloride	506-77-4	Any quantity
Diborane[1]	19287-45-7	Any quantity
Dichlorosilane	4109-96-0	Any quantity
Disilane	1590-87-0	Any quantity
Ethylamine	75-04-7	Any quantity
Ethyl chloride	75-00-3	Any quantity
Ethylene	74-85-1	Any quantity
Ethylene oxide	75-21-8	Any quantity
Formaldehyde	50-00-0	Any quantity
Fluorine[1]	7782-41-4	Any quantity
Germane	7782-65-2	Any quantity
Germanium tetrafluoride	10038-98-9	Any quantity
Hexafluoro-1, 3-butadiene	685-63-2	Any quantity
Hydrogen, gaseous (cylinder/tube trailer)	1333-74-0	Any quantity
Hydrogen, liquid	1333-74-0	Greater than 4,5400Kg

Chemical name	C.A.S No.	Comments
		10 000 lbs
Hydrogen bromide[1]	10035-10-6	Any quantity
Hydrogen chloride [1]	7647-01-0	Any quantity
Hydrogen cyanide	74-90-8	Any quantity
Hydrogen fluoride [1]	7664-39-3	Any quantity
Hydrogen selenide	7783-07-5	Any quantity
Hydrogen sulfide [1]	7783-06-4	Any quantity
Methane	74-82-8	Any quantity
Methylamine	74-89-5	Any quantity
Methyl chloride	74-87-3	Any quantity
Methylsilane	992-94-9	Any quantity
Methyltrichlorosilane	75-79-6	Any quantity
Nickle carbonyl	13463-39-3	Any quantity
Nitrogen oxides (NO; NO_2; N_2O_4; N_2O_3)	10102-43-9,10102-44-0,10544-72-6,	Any quantity
Nitrogen trifluoride (NF_3)	7783-54-2	Any quantity
Nitrous oxide	10024-97-2	Any quantity
Octafluorocyclopentene	559-40-0	Any quantity
Phosgene[1]	75-44-5	Any quantity
Phosphine[1]	7803-51-2	Any quantity
Phosphorus oxychloride (POCl)	10025-87-3	Any quantity
Phosphorus trichloride[1]	7719-12-2	Any quantity
Propane	74-98-6	Greater than 4,540 Kg 10 000 lbs
Propylene	115-07-1	Greater than 4,540Kg 10 000 lbs
Red phosphorus	7723-14-0	Any quantity
Silane	7803-62-5	Any quantity
Silicon tetrachloride	10026-04-7	Any quantity
Silicon tetrafluoride	7783-61-1	Any quantity
Sulfur dioxide[1]	7446-09-5	Any quantity
Sulfuric acid	7664-93-9	Any quantity
Sulfur tetrafluoride	7783-60-0	Any quantity
TBA (Tertiary butyl arsine)	4262-43-5	Any quantity
TBP (Tertiary butyl phosphine)	2501-94-2	Any quantity
TDEAT (Tetra kis (diethylamino) Titanium)	4419-47-0	Any quantity
TDMIAT (Tetra kis (dimethylamino) Titanium)	3275-24-9	Any quantity
Tetramethylsilane	993-07-7	Any quantity
Titanium tetrachloride	7550-45-0	Any quantity
Trichlorosilane	10025-78-2	Any quantity
Triethyl phosphite	122-52-1	Any quantity

Chemical name	C.A.S No.	Comments
Trimethyl phosphate (TMPI)	121-45-7	Any quantity
Trimethylsilane	993-07-7	Any quantity
Tungsten hexafluoride [1]	7783-82-6	Any quantity
Zinc arsenide	56450-43-2	Any quantity
Toxic Mixtures; For toxic mixtures the supplier shall determine whether the toxicity and risk the mixture are similar to the products listed above		Any quantity

The list of chemicals of concern is based upon the AIGA 091/14, EIGA 920/13 Security Guidelines for Qualifying Customers Purchasing Compressed Gases and CGA P-53 Security Code Top Screen

[1]These are chemicals that are capable of causing mass casualties when abused or released. Sometimes refrred to as chemicals that could be used as a weapon of mass destruction (WMD)