

# **Site Security Guidance for Chlorine Facilities**

**A Chlorine Institute Guidance Document**

**November 15, 2002**

**The Chlorine Institute, Inc.  
1300 Wilson Boulevard  
Arlington, VA 22209**

# TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION</b> .....	<b>1</b>
1.1	Background.....	1
1.2	Scope.....	1
1.3	Responsible Care.....	1
1.4	Disclaimer.....	2
1.5	Approval.....	2
1.6	Revisions.....	2
<b>2.</b>	<b>GENERAL CONSIDERATIONS</b> .....	<b>2</b>
<b>3.</b>	<b>PREVENTION AND MITIGATION ENHANCEMENTS</b> .....	<b>3</b>
3.1	Components of a Security Survey.....	3
3.2	Process and Handling Areas.....	3
3.3	Pipelines.....	3
3.4	Storage Tanks.....	3
3.5	Physical Facilities.....	4
3.6	Facility Access Control.....	4
3.7	Emergency numbers.....	5
3.8	Formal (Written) Procedures.....	5
<b>4.</b>	<b>REFERENCES</b> .....	<b>6</b>

## 1. INTRODUCTION

### 1.1 Background

The events of September 11 have shown that terrorists can inflict damage to people, physical assets, and infrastructures in a way previously unimaginable in the United States and most everywhere else in the world. As a result, chlorine production, use and repackaging facilities have already undertaken numerous steps and continue to undertake additional steps to enhance their security measures. The goals of these enhanced security measures are to (1) reduce the likelihood of a terrorist attack; and (2) mitigate the consequences of any successful attack.

### 1.2 Scope

This document is intended to provide guidance to assist facilities whether they produce, use, or repackage chlorine, or some combination thereof, in implementing site security measures to reduce the facility's vulnerability to terrorist threats. Readers of this document should note that simply because a measure is presented does not necessarily mean that it needs to be implemented by the facility. It simply means that the facility should evaluate the item. A decision on whether to implement the measure should be based on site-specific factors. Site-specific factors may include such matters as the relative difficulty to attack the facility, the relative severity of a successful attack, and the attractiveness of the target to terrorists.

This guidance document is intended to serve as an interim guidance. Both as a nation and as an industry, we are undergoing a learning curve in addressing threats from terrorists. It is expected that, as we acquire a better understanding of terrorists threats and the benefits of specific countermeasures, we will need to reconsider which recommendations are best suited to reduce these threats.

This document is intended to supplement, not replace, other publications addressing security and related subjects. Such publications include *Site Security Guidelines for the U.S. Chemical Industry* (Reference 4.1.1) and *Emergency Response Plans for Chlorine Facilities* (Reference 4.2.1). The reference section of this document is a compendium of resources providing information on security issues.

### 1.3 Responsible Care

The Institute is a partner in the American Chemistry Council's Responsible Care® initiative. In this capacity, the Institute is committed to fostering the adoption by its members of the Codes of Management Practices; facilitating the implementation of the Codes; and encouraging members to join the Responsible Care initiative directly.

Institute members who produce, distribute, or use chlorine are required to follow the elements of a Responsible Care® program such as those sponsored by the American Chemistry Council, the Canadian Chemical Producers Association, the Asociación Nacional de la Industria Química, A.C. (ANIQ) in Mexico, or other associations worldwide, and the National Association of Chemical Distributors' Responsible Distribution Program® as applicable.

The American Chemistry Council requires its members to implement the Responsible Care Security Code per a defined timetable. Information about the Security Code can be found on the website: [www.responsiblecaretoolkit.com/workshops.asp](http://www.responsiblecaretoolkit.com/workshops.asp) . Most chlorine facilities that handle chlorine are likely to be in either Tier 1 or Tier 2 in the ranking system. Tier 1 facilities are required to have their security vulnerability assessment complete by December 31, 2002. Tier 2 facilities are required to have their security vulnerability assessment complete by June 30, 2003. Implementation is due twelve months later.

#### 1.4 Disclaimer

The information in this guidance document is drawn from sources believed to be reliable. The Institute and its members, jointly and severally, make no guarantee, and assume no liability, in connection with any of this information. Moreover, it should not be assumed that every acceptable procedure is included, or that special circumstances may not warrant modified or additional procedures. The user should be aware that changing technology or regulations may require changes in the recommendations contained herein. Appropriate steps should be taken to ensure that the information is current when used. These recommendations should not be confused with federal, state, provincial, municipal, or insurance requirements, or with national safety codes.

#### 1.5 Approval

The Plant Operations and Safety Committee approved interim guidance document on September 24, 2002 and directed that it be posted in the Members Only section of the Institute's website.

#### 1.6 Revisions

Suggestions for revisions should be directed to the Secretary of the Institute.

## 2. **GENERAL CONSIDERATIONS**

The following are general items that should be considered as the facility addresses security issues.

1. Does the facility have a written security plan for the site?
2. Has the facility fully implemented its security plan?
3. Does the facility maintain on-going two-way communications among employees to increase awareness and follow-up on any unusual developments?
4. Does the facility utilize the expertise of security consultants or local law enforcement agencies to strengthen site security?

### **3. PREVENTION AND MITIGATION ENHANCEMENTS**

The following items are enhancements that should be considered as the facility addresses security issues.

#### **3.1 Components of a Security Survey**

- Has the security of the site as it currently exists been determined?
- Has the survey identified security deficiencies?
- Has the needed level of protection been established?
- Have the recommended measures to enhance overall security been thoroughly reviewed and implemented?
- Have appropriate quality control procedures been utilized in conducting security surveys and in implementing and maintaining enhancement measures?
- Have the implementation measures been audited by qualified third parties?

#### **3.2 Process and Handling Areas**

- Is access restricted to authorized personnel?
- Are traffic barricades, where appropriate, in place?
- Are remote process areas being monitored?

#### **3.3 Pipelines**

- Does the facility conduct periodic, frequent inspections of pipelines at staggered times?
- Do pipelines and pipeline lift stations; when accessible to vehicles, have suitable protection in place to prevent collision by vehicles (e.g., traffic barricades, fences, ditches)?
- Do pipelines have monitoring devices with 24 hour live monitoring to ensure no unauthorized access?
- Are frequent checks of locking devices for serviceability and or sabotage being undertaken?

#### **3.4 Storage Tanks**

- Are tank areas being monitored with cameras to ensure no unauthorized access?
- When accessible to vehicles, do storage tanks have suitable protection in place to prevent collision by vehicles (e.g., traffic barricades, fences, ditches)?

- Is access to storage areas restricted to only authorized personnel?
- Have remote shutoff devices for liquid transfer lines been considered?
- Are chlorine inventories kept at the minimum levels consistent with production and sales needs?

### 3.5 Physical Facilities

- Are guardhouses adequately protected and equipped with a means of instant communication (e.g., two-way radio, telephone, or cell phone)?
- Have straight roadways approaching facilities been evaluated for the need to protect internal plant areas from unauthorized fast moving vehicles (e.g. traffic barricades forcing vehicles to weave slowly as they approach access gates)?
- Is the fencing around the perimeter a clear indication of the plant boundaries or does the fencing need to be marked with “No Trespassing” signs?
- Are the perimeter fences maintained in sound condition with gates closed and locked at all times except during authorized use?
- Are infrequently used gates checked frequently or blocked with additional barriers to further deter unauthorized access?
- Are remote access areas monitored either through physical inspections or through the use of surveillance cameras?
- Has the need for video recording devices to have the capability for storing surveillance videos for a finite period of time (e.g., 24 hours) been evaluated?
- Are procedures in place to test security guards for compliance with “Security Expectations” (See Section 3.8)?
- Is the lighting adequate to illuminate all areas of the process or facility perimeters?
- Does the facility conduct frequent, periodic training for security personnel?
- Does the facility engage employees to serve as members of the security team?

### 3.6 Facility Access Control

The facility should take appropriate steps to limit access to authorized personnel and necessary vehicles. In addition to the use of fencing, lighting, and guard service, the facility should consider the following items to better insure access is limited to authorized personnel and to facilitate compliance.

- Except for small facilities where authorized personnel are readily identifiable, are employees and contractors provided with a badge that is to be worn and visible? When practicable photo badges should be utilized.

- Are all visitors provided with a badge that is to be worn and visible and has a termination date on it?
- Are all visitors verified by their contact and escorted when appropriate?
- Are deliveries verified and inspected utilizing at least a random procedure before granting access?
- Does everyone sign in/sign out or register (electronically) before entering and leaving?
- Are vehicles inspected before entering a plant utilizing at least a random procedure?
- Are passengers in vehicles who accompany the driver denied access unless there is a bonafide need for that person to assist in the task at hand?

### 3.7 Emergency numbers

It is recommended that the facility have an emergency contact list to allow for quick access to officials pertaining to security issues. This list should supplement (and sometimes duplicates) the contacts listed in Reference 4.2.1. The contact list should include the following:

- FAA
- FBI
- Local Law Enforcement
- Local Fire Departments and EMS
- Postal Master
- Hazardous Material Handling companies
- Coast Guard
- Office of Homeland Security

### 3.8 Formal (Written) Procedures

Does the facility have a written policy for the following? Procedures should discuss what to do in the event of a suspected security breach (e.g., suspicious package or item found)

- “How to” inspect vehicles and what to look for.
- “What to do” in the event “something” is discovered within the facility.
- Handling “Armed intruder” and hostage situations.
- Handling of mail.
- Handling of bomb threats.
- “Special Situations Plan” to put in effect in case of a catastrophic situation.

- Conducting tank car (rail car) and tank truck inspections with a focus on security issues. Such inspections should include the verification of drivers for sensitive shipments and receipts.
- Addressing cyber attacks.
- Background checks for new employees including contractors with access to sensitive areas of the facility. Consideration should be given to incorporating background checks by contractors for their employees as a part of standard purchasing contracts.
- “Security Expectations”, for all employees and contract security personnel. The policy should define what is expected of employees, contractors, visitors and delivery drivers requesting admittance to a facility.

## 4. REFERENCES

### 4.1 General

- 4.1.1 *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Chlorine Institute, Inc., Synthetic Organic Chemical Manufacturers Association. This document can be downloaded from the Chlorine institute website at [www.CL2.com](http://www.CL2.com) .
- 4.1.2 American Chemistry Council security website. This website has a lot of information on security issues including the new Responsible Care® security code. It can be downloaded at [www.americanchemistry.com/cmaweb site.nsf/s?readform&nnar-5a6k kh](http://www.americanchemistry.com/cmaweb site.nsf/s?readform&nnar-5a6k kh) .
- 4.1.3 Center for Chemical Process Safety (CCPS) website. The CCPS® Security Vulnerability Analysis can be obtained from the website at [www.aiche.org/ccpssecurity/](http://www.aiche.org/ccpssecurity/) .
- 4.1.4 United States Department of Justice website. The document, A Method to Assess the Vulnerability of U.S. Chemical Facilities, November 2002, can be downloaded from the website at <http://www.ojp.gov/nij/pubs-sum/195171.htm> .
- 4.1.5 Sandia National Laboratories website. Information on security can be obtained from the website at [www.sandia.gov/capabilities/homeland-security/index.html](http://www.sandia.gov/capabilities/homeland-security/index.html) and [www.sandia.gov/capabilities/homeland-security/links.html](http://www.sandia.gov/capabilities/homeland-security/links.html)

### 4.2 Institute Publications

- 4.2.1 *Emergency Response Plans for Chlorine Facilities*, ed. 5; Pamphlet 64; The Chlorine Institute: Washington, DC, **2000**.