

NACD
SECURITY VULNERABILITY
ASSESSMENT METHODOLOGY
for
CHEMICAL DISTRIBUTION
FACILITIES



- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

Copyright © 2008

LEGAL DISCLAIMER

This vulnerability assessment methodology was prepared by the National Association of Chemical Distributors (NACD). Neither the NACD, nor any of its employees, contractors, subcontractors, or their employees makes any warranty, expressed or implied, or assumes any legal liability for the contents of this document, nor assumes any liability for the use of this methodology by any party, nor assumes any liability for the results conveyed by the use of this methodology by any party to a third party.

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	6
A. Overview	6
A.1 Prologue.....	6
A.2 Purpose.....	7
A.3 Methodology.....	8
B. Screening	10
B.1 Overview	10
B.2 Applicability	10
B.3 Prioritization	11
SECTION I: PLANNING THE ASSESSMENT	13
SECTION 2: CHARACTERIZING THE FACILITY.....	16
SECTION 3: ASSESSING THREATS.....	23
SECTION 4: ANALYZING VULNERABILITY	26
SECTION 5: IDENTIFYING POTENTIAL COUNTERMEASURES	29

- FINAL -

EXHIBITS

Exhibit 1: Facility Prioritization for Conducting a SVA	12
Exhibit 2: Consequence Values	20
Exhibit 3: Target Attractiveness Values.....	21
Exhibit 4: Risk Matrix.....	22

APPENDICES (Separate attachments)

A	Chemical Facility Anti-Terrorism Final Rule, 6 CFR Part 27, Appendix A, DHS Chemicals of Interest
B	List of Risk Management Program Chemicals
C	Process Safety Management Summary
D	List of Chemicals Used for WMDs
E	Planning Forms
F	Screening & Facility Characterization Forms
G	Asset Characterization Forms
H	Threat Assessment Form
I	Scenario Worksheet & What If Questions

- FINAL -

ABBREVIATIONS / ACRONYMS USED

CCPS	Center for Chemical Process Safety
CFATS	Chemical Facility Anti-Terrorism Standards Department of Homeland Security 6CFR Part 27
CSAT	Chemical Security Assessment Tool
CSI	Chemical Security Incident
DHS	Department of Homeland Security
DOT HM 232	Department of Transportation Hazardous Material Rule 49 CFR Part 172
EPA RMP	Environmental Protection Agency Risk Management Plan
OCA	Off-Site Consequence Analysis
OSHA PSM	Occupational Safety and Health Administration Process Safety Management
RDP	Responsible Distribution Process
SVA	Security Vulnerability Assessment
STQ	Screening Threshold Quantity
WMD	Weapons of Mass Destruction

- FINAL -

Introduction

A. Overview of Full-Line and Factory Packed Chemical Distributors Security Vulnerability Assessment Methodology

A.1 Prologue

The National Association of Chemical Distributors' (NACD) Responsible Distribution ProcessSM (RDP) requires that each of its member companies address site and transportation security, including the conducting of a vulnerability assessment.

This Security Vulnerability Assessment was developed to assist NACD members in complying with their RDP security requirements. Member adherence and implementation of this requirement is independently verified by an Association-designated third-party verification firm once every three years. Successful completion of the verification is a condition of membership in NACD.

This security vulnerability assessment methodology for NACD members that store, warehouse, repackage, and blend chemicals will assist them in identifying potential security vulnerabilities and to determine measures to address these issues.

NACD's assessment focuses on a fixed facility, including:

- Chemical Bulk Storage
- Chemical Distribution General Facility
- Personnel
- Production
- Rail Car
- Branch locations that store CFATS Appendix A Chemicals
- Chemical Warehouse
- Chemical Product Mix

- FINAL -

This methodology is designed to only address site security. Transportation security is addressed through compliance with DOT HM 232.

NACD's Chemical Distribution Security Vulnerability Assessment Methodology was developed by NACD's Security Vulnerability Assessment Model Task Group and NACD staff. Various industry models were reviewed during the development of this methodology, notably The Chlorine Institute's *Chlorine Packaging and Sodium Hypochlorite Plant Security Vulnerability Assessment Methodology*, the Synthetic Organic Chemical Manufacturer Association's *Manual on Chemical Site Security Vulnerability Analysis Methodology and Model*, and the Center for Chemical Process Safety's *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*.

Many of these models contain scenarios and steps appropriate to chemical distribution and are consistent with the methodology of other recognized models. NACD's intention in developing this SVA was not to duplicate previous models but to provide a simpler, more applicable alternative for chemical distribution facilities not requiring the level of complexity found in some of the previously-mentioned models.



In places within the SVA where RDP is mentioned as a reference, the RDP logo appears to identify how members may use or revise their RDP policies and procedures, if necessary, while conducting the assessment.

A.2 Purpose

This document describes a security assessment methodology that can be used to identify security hazards, threats, and vulnerabilities facing a chemical distribution facility resulting in a Chemical Security Incident (CSI) and to evaluate

- FINAL -

the security options and their effectiveness in reducing the consequences or likelihood of such an incident. The purpose of NACD's security vulnerability assessment methodology is to ensure the protection of the public, workers, national interests, the environment and the company.

A.3 Methodology

The NACD Chemical Distribution Security Vulnerability Assessment Methodology is designed to provide recommendations to reduce security risk. Before starting an assessment, a company could conduct a screening to determine if a SVA is necessary or to prioritize the assessment if the company has multiple sites (see Section B). The NACD SVA consists of the following steps:

1. Define and Plan the SVA: Facility management determines the scope of the SVA, forms the multi-disciplinary SVA team, and assures that appropriate resources and information are available.
2. Characterize the Facility (identify potential targets and determine current risk): The team evaluates the facility assets (i.e. chemicals, equipment, processes, and other resources) to identify and prioritize potential targets based on their ability to cause significant consequences and their attractiveness as a target. This includes identifying the critical chemical distribution assets, the hazards of the assets, the effect of the loss of or damage to the assets, the operations of the facility, the layers of protection already in place, and characteristics of areas surrounding the facility.
3. Threat Assessment (identify applicable threats): The team identifies the types of threats (e.g., type of adversary (aggressor), chemical release, fire, sabotage/damage, theft) applicable to each potential target. Consideration of possible adversaries should include insiders, outsiders and insiders working in collusion with outsiders. The selection of the threats should consider reasonable local, regional or national intelligence information.

- FINAL -

4. Vulnerability Analysis: For each threat event, the team develops general types of attack scenarios (e.g., ram with vehicle or plant a bomb) for each asset and identifies existing countermeasures to decrease the likelihood of successful attack or mitigate the consequences. The team may use a “What If” list to brainstorm potential scenarios.

5. Identify Potential Countermeasures: Based on the existing countermeasures, the team assesses the existing risk for each scenario. If the risk is not considered acceptable, the team will then brainstorm additional countermeasures, reevaluate the risk, and develop recommendations where appropriate. Reasonable actions (cost vs. benefit vs. impact) that should be taken to reduce the consequence and/or likelihood of attack to acceptable levels are determined. Site management and the SVA team address recommendations from the SVA and develop an action plan.

B. Screening for the Need to Conduct a Vulnerability Assessment

B.1 Overview

Each individual facility where chemicals are stored or handled should first undergo a screening process. Screening individual facilities has two purposes:

- Screening determines whether or not a vulnerability assessment should be conducted at that facility (unless already required by CFATS).
- For companies with multiple locations, the screening determines which facilities should conduct a SVA and prioritizes them.

Determining whether a facility should undergo a SVA, via screening, is based on the possible consequences of potential terrorist incidents at the facility. The NACD SVA includes a five-question Applicability Screening list to help distribution facilities determine whether a SVA should be conducted at a facility.

B.2 Applicability

The first question: **Is the facility subject to the Chemical Facility Anti-Terrorism (CFATS) Regulations?** (See *Appendix A* for a list of chemicals and the screening threshold quantity (STQ) that qualifies a site under the regulations.)

The second question: **Does the facility's inventory include a threshold quantity or greater of chemicals covered by EPA's RMP rule?** (See *Appendix B* for a list of substances and thresholds.) Facilities that are subject to RMP are a focus of Department of Homeland Security officials, particularly those with potential large off-site consequences from accidents, which are a part of the Risk Management Plans (RMP) mandated by the rule. An event potentially desired by terrorists is an off-site release of a chemical that could impact the local community or beyond. A facility that is subject to EPA's RMP rule is required to complete an Off-site Consequence Analysis (OCA).

The third question: **Is the facility subject to the Occupational Safety and Health Administration's Process Safety Management (PSM) rule?** (See *Appendix C* for a description of the regulation.)

The fourth question: **Does the facility's inventory include chemicals considered to be weapons of mass destruction (WMDs)?** (See *Appendix D* for a list.)

The fifth and last question: **Was the facility required to register under the Bio Terrorism Act of 2002?** Many distribution facilities handle food-grade chemicals or chemicals used in food ingredients for human or animal consumption and must be registered under this Act.

Other factors to consider in screening facilities for conducting a SVA include:

- Accessibility of the facility to the general public
- Recognizability of the facility to the general public
- Importance to the company, region, and the Nation

B.3 Prioritization

To prioritize facilities according to those at which a SVA should be conducted, consider the following model:

**Exhibit 1: Facility Prioritization for Conducting a SVA
(Also appears in Appendix F)**

On a scale of 1 (lowest priority) to 5 (highest priority)

Question	If 'YES'	If 'NO'	Score
Does the facility's inventory include a threshold quantity or greater of chemicals covered by CFATS Regulation? (Refer to Appendix A for list of chemicals)	5	0	
Does the facility's inventory include a threshold quantity or greater of chemicals covered by EPA RMP Rule?	4	0	
Is the facility subject to the Occupational Safety and Health Administration's Process Safety Management (PSM) rule?	3	0	
Does the facility's inventory include chemicals considered to be weapons of mass destruction?	2	0	
Was the facility required to register under the Bio Terrorism Act of 2002?	1	0	
TOTAL			
Score			

If the answer is NO to all of the above and the facility is not particularly accessible or recognizable to the general public nor distributes products that are essential to the community, region, and Nation, then there is no significant security risk and a SVA is not appropriate. Continue to take the normal and customary measures to protect employees, the public and the environment.

SECTION 1: PLANNING THE ASSESSMENT

Establish Basis for the Analysis

A prerequisite in conducting an assessment is the establishment of a group of knowledgeable and capable personnel that comprises a SVA Team, defining a scope and list of objectives, and understanding the site's assets. See Appendix E – Planning Forms Attachment 1 for applicable documentation and Appendix E Attachment 2 for a suggested planning form.

1.1 Typical Planning Process

- a. Form SVA team
- b. Set scope and objectives
- c. Gather pre-SVA data to evaluate baseline security
- d. Analyze previous security incidents data
- e. Conduct interviews with site and security personnel
- f. Conduct a site inspection (including an inspection after dark)
- g. Gather threat information

1.2 Forming a Security Vulnerability Assessment Team



A team is typically comprised of no less than three people, with one serving as the team leader. A site security team needs to be formed consisting of persons that have knowledge of:

- a. The facility including
 - Site hazards
 - Operations of the facility
 - Raw materials and finished goods (particularly chemicals)
 - Process safety and equipment design
 - Transportation equipment and systems
- b. Adversary characteristics and capabilities */ Facility Security

- FINAL -

- Present level of security
 - Security procedures, methods and systems;
- c. The surrounding community;
 - d. Responsible Distribution ProcessSM security requirements and procedures that impact the site;
 - e. For the team leader, knowledge of and/or prior experience in conducting a security vulnerability assessment and the development of a site security plan, and if possible impartiality;
 - f. Applicable regulations (i.e., Chemical Facility Anti-Terrorism Standards, DOT's HM-232 security plan rules, Coast Guard's Maritime Transportation Security Act, & Food & Drug Administration's Bio-Terrorism Act).
 - g. Other resources as needed
 - Environmental
 - Safety & Industrial Hygiene
 - Process Safety

*Represented either by a security professional to make this judgment or an individual who knows how to defeat the existing security measures

1.3 Define SVA Scope and Objectives

It is important to develop a mission statement, SVA scope, and a list of objectives for the SVA. The scope should specify the critical assets to be evaluated and relevant security events such as:

- a. Theft/diversion of material for subsequent use as a weapon or component of a weapon
- b. Deliberate loss of containment
- c. Contamination of a chemical, tampering with a product or sabotage of a system
- d. Any act (including fire or explosion) causing harm including degradation of assets, infrastructure, business and/or value of a company or industry

- FINAL -

Remember, the focus of this NACD Security Vulnerability Assessment Methodology is any quantity of chemical or chemicals located on-site at a distribution facility or warehouse that may be:

- Loaded onto a company vehicle, common carrier, or customer pick-up vehicle;
- Unloaded to storage at a distribution facility or public warehouse*;
- Unloaded directly to a process at a distribution facility or public warehouse*; and
- Stored at a distribution facility or public warehouse*, including factory-packed materials

Stated objectives of an SVA may include:

- a. To conduct an analysis to identify security hazards, threats and vulnerabilities facing the chemical distribution facility as it relates to the handling and storage of chemicals in bulk and non-bulk quantities.
- b. To evaluate the appropriate countermeasures necessary to provide for the protection of the company's or facility's assets as well as protection to the public, workers, national interests, the environment, and the company.

*The NACD Security Vulnerability Assessment Methodology is designed for facilities owned or controlled by NACD members. As Responsible Distributors, NACD members should require proof or certification from the public warehouses they use that these facilities have exercised due diligence and conducted their own SVAs, particularly if they can answer "yes" to any of the questions in Section B.2.

SECTION 2: CHARACTERIZING THE FACILITY

Determine Existing Risk

In Section 2, The SVA team identifies potential targets. The team evaluates the facility assets (i.e. chemicals, equipment, people, processes, and other resources) to identify and prioritize targets based on their potential to cause significant consequences or their attractiveness as a target. The team should initiate this process with a tour of the facility, including security systems and process safeguards. The team should interview appropriate management, security, and operations personnel to develop an understanding of the facility. Prior to proceeding with Section 2, the team should review related materials gathered in Section 1 (Attachment 1, Appendix E Planning Forms).

2.1 Existing Countermeasures

The SVA team identifies and documents the existing security measures which may include physical security, cyber security, administrative controls, and personnel training. The SVA team should identify methods used in employee background checks and other types of screening used for individuals authorized to be on site. This SVA model includes an Appendix F – Screening & Facility Characterization Form, to assist in gathering existing countermeasures. Use the documentation from Section 1, interviews with plant and security personnel (to determine how well the procedures match actual practice), and the tour to complete Appendix F. Random interviews with employees will help to determine where vulnerabilities may exist.

Identify layers of protection, including any processes or impediments to attacks such as warning signs, physical barriers, cameras, and security guards that could (1) Deter an event from happening; (2) Detect an adversary during the planning or committing of an act; and/or (3) Delay an event from taking place.

- FINAL -



In addition to the information on the various facility characteristics listed in this section, it will be important to gather operational procedures implemented at the facility that address security, such as those under the company's Responsible Distribution ProcessSM.

2.2 Asset Identification

Record assets in Appendix G – Asset Characterization Forms in the Asset-Consequence Worksheet. When recording information on the operation of the facility, include the maximum number and location of chemical containers, storage tanks, and tank cars that could be on the site and how long they could be at the site.

2.2.1 Asset Groups

The SVA team uses the reference materials and information gathered on the tour to develop a list of critical assets and identify potential consequences to guide the subsequent SVA steps. Specific areas within a generic distribution facility that should be considered when characterizing a facility are:

- Bulk chemical storage
- General distribution facility
- Information and Cyber Systems
- Facility personnel
- Facility production
- On-site rail tank cars
- Branch locations that store CFATS Appendix A Chemicals
- Chemical transportation equipment and processes, including contracted carriers
- Chemical warehouse
- Chemical product mix

2.2.2 Examples of Assets

Assets at a chemical distribution facility can vary, but the general areas of chemicals, people, facilities and equipment, operations and information / cyber systems, should be the focus of the SVA. Below are a few suggestions of assets to consider:

Chemicals listed in Appendices A, B, C and D

- Used or produced

People

- Employees, visitors, outside contractors, common carrier drivers, local community citizens.

Facilities and Equipment

- Outdoor structures, such as buildings, tank farms, vehicles, rail cars, storage areas.
- Indoor assets, such as, tanks, offices, computers, supplies, other necessary equipment.

Operations

- Company image, utilities, and telecommunication systems.

Information / Cyber Systems

- Computer LANS, trade secrets, customer data, employee data, sensitive passwords, compliance records, product data.
- Outside access of computer LANS via the Internet

2.3 Consequence Characterization

Possible consequence categories include, but are not limited to, employee and facility impacts, offsite population and structural impact, environmental impact, economic impact, and public image impacts (See below for details). The effectiveness of safeguards and feasibility of adversaries (aggressors) achieving these consequences will be evaluated during subsequent SVA steps. The team conducts this consequence evaluation step by completing the Asset – Consequence Worksheet in Appendix G. This information is used to determine the consequence value by applying the five factors in the Consequence Value Worksheet in Appendix G to each asset. The total consequence score for each asset is automatically translated to the Consequence Value (see Exhibit 2 for score conversion) and automatically transferred to the Risk Ranking Worksheet in Appendix G. This is the first step in identifying the level of risks.

SVA assessment of consequences should possibly go beyond the worst-case scenarios as required in the EPA RMP. For example, if the worst case involves complete loss of containment from the largest tank on the site and a second tank nearby, it should be assumed that an adversary will attack both tanks, resulting in a consequence greater than determined in the RMP. Engineering judgment should be used to consider if it is credible to assume multiple items of equipment could be included in the scenario. For theft, this might mean a sufficient amount of hazardous materials is stolen that would pose a significant risk to the public. Do not limit analysis to RMP chemicals. Consider any asset that could cause a significant impact on the public (neighbors and other businesses).

The following are some impact factors that should be analyzed and recorded in Appendix G:

- FINAL -

Death and injuries of employees - Many chemical facilities, if successfully attacked, will likely have an off-site consequence as a result. But the most immediate consequence may be the impact on facility employees and structures.

The surrounding community - Consideration must also be given to the off-site consequence beyond the fence line. Worst-case conditions including temperature and wind direction should be considerations.

Environmental or infrastructure impact - Some adversaries may seek to inflict environmental or infrastructure damage. Consider how the facility's surrounding environment may be impacted. For example, is the facility near a waterway or critical infrastructure?

Financial impact on the company/local economy - Consider items such as the risk of bankruptcy, the ability of the company to continue doing business at that location, and the loss of customers to competitors and the impact this will have on the local economy.

Proximity to a national landmark/sensitive facility or major city - Some distribution facilities are in urban settings or within sight of major U.S. cities. What impact would an attack have on the economy or normal environment within the city? Are any important landmarks, such as museums, statues, parks, memorials, places of national significance or sensitive facilities such as hospital, schools and local government located near the facility?

Exhibit 2a: Target Consequence Values

Total Consequence Score	Consequence	Consequence Value (1)
0	None	0
1 to 5	Low	1
6 to 10	Medium	2
11 to 15	High	3
16 to 20	Very High	4

(1) This value is transferred to the Risk Ranking Worksheet in Appendix G

- FINAL -

2.4 Target Attractiveness Characterization

After addressing the potential consequence factors, the SVA team then evaluates the target attractiveness factors using Attractiveness Value Worksheet in Appendix G. Target attractiveness is used to describe the likelihood of an event. Similar to the consequence factor sheets, for each target attractiveness category (e.g., public knowledge, emergency response, etc.), rate each asset. In conducting this assessment, the team should look at the facility from the perspective of a potential aggressor. The team continues this process until all target attractiveness factor categories have been evaluated for each asset. The total target attractiveness score for each asset is automatically translated to the Attractiveness Value (see Exhibit 3 for score conversion) and automatically transferred to the Risk Ranking Worksheet in Appendix G.

Exhibit 3: Target Attractiveness Values

Total Attractiveness Score	Attractiveness	Attractiveness Value (1)
<10	Very Low	1
11 to 20	Low	2
21 to 30	Medium	3
31 to 40	High	4
41 to 50	Very High	5

(1) This value is transferred to the Risk Ranking Worksheet in Appendix G

2.5 Risk Ranking

The Risk Ranking worksheet in Appendix G now provides a summary of the potential targets and their associated consequence and attractiveness (likelihood of an attack). Key targets typically are those assets associated with significant consequences or high target attractiveness.

This consolidation provides two key outputs:

- Identification of the potential targets at each site based on potential consequences
- Identification of the potential target attractiveness features of the site and potential targets.

The high risk targets in Exhibit 4: Risk Matrix, become the focus of the SVA scenario analysis. Target attractiveness is used to help assess likelihood of attack scenarios that may be successfully accomplished by given aggressors.

Exhibit 4: Risk Matrix

		Severity (Consequence)			
Likelihood (Attractiveness)		4	3	2	1
	5	20	15	10	5
	4	16	12	8	4
	3	12	9	6	3
	2	8	6	4	2
	1	4	3	2	1

Red - High Risk / High Priority to reduce

Yellow – Moderate Risk / Consideration to reduce

Green – Low risk / Risk tolerable

SECTION 3: ASSESSING THREATS

Identify How Critical Assets Could Be Threatened



- 3.1** The purpose of this step is to identify and document ways that the identified critical assets could be threatened or perhaps attacked. NACD members most likely have completed this step as part of their RDP policies and procedures development process to address site security, specifically under RDP Section IV, Handling and Storage. Threats could involve internal attacks, external attacks, or a combination. Potential threats to chemicals in storage at a distribution facility, in the process of loading for delivery, or unloading at the facility are identified in this step.

3.2 Evaluation of Possible Threats

Below are examples of possible threats that a chemical distribution facility may wish to address:

- Loss of product containment
- Sabotage of a blend tank, storage vessel, transfer valve/hose/other equipment
- Hijacking of a company vehicle from the site
- Public warning, such as a bomb threat
- Protestors disrupting operations
- Intentional product contamination

3.3 Defining Adversaries (aggressors)

There may be numerous different types of adversaries, domestic and international, known and unknown, criminal and first-time offender. Below are a few possible examples to consider:

Possible Types of Adversary (in no particular order)

- Criminals
- Violent activists
- Deranged persons
- Disgruntled employees
- Thieves/Vandals
- Terrorists, foreign or domestic

Possible Adversary Goals (in no particular order)

- Inflict maximum physical damage and loss of lives (including widespread contamination via food-grade product consumption)
- Inflict psychological terror
- Demonstrate government's inability to protect its citizens
- Disrupt the economy
- Disrupt the site's normal operations to negatively impact beneficiaries of its products or services

Possible Adversary Skills (in no particular order)

- Highly trained in military tactics
- Capable of using sophisticated weapons, explosives, or incendiaries
- Capable of using improvised explosives/incendiaries
- Capable of deception through the use of fake IDs
- Knowledgeable of the inner-workings of a chemical manufacturing or distribution facility and chemical processing

3.4 Identifying Threats

The team completes the Appendix H - Threat Assessment Form. This will be used in the vulnerability assessment in Section 4 to pair appropriate threats to assets to develop attack scenarios. Local and state law enforcement may be the best source of information of potential threats in the community. The FBI Joint Terrorism Task Force, U.S. Coast Guard and other federal agencies may provide input.

Appendix H contains general categories and sub-categories of types of threats that could exist for any facility or operation and will assist in identifying them for purposes of the SVA. Consider the potential for each threat at this facility, then rate and indicate the threat level probability (Low, Medium or High). Also, indicate if there is any known history of the threat at this facility. The type of threat could be either Outside (O), Inside (I) or collusion between inside and outside (C). Use the comment column to record rationale for selection and the level of threat.

Terrorists are the most difficult adversaries based on training and their willingness to die to achieve their objective. For distribution sites, theft of materials may be a high management priority requiring focus on motivation and capability of criminals and modeled the same way as a terrorist threat.

SECTION 4: ANALYZING VULNERABILITY

Determine Existing Weaknesses

Once the SVA team has determined the consequence and likelihood of a Chemical Security Incident (CSI), it should determine how an adversary could perpetrate the incident by developing scenarios for asset and threat combinations.

The NACD SVA Methodology uses scenarios to identify security weaknesses that could be exploited to attack or destroy an asset. A scenario is defined based on the SVA Team's perspective of the consequences that may result from undesired security events given an assumed threat for a given asset. This is described as an event sequence including the specific malicious act or cause and the potential consequences, while considering the challenge to the existing countermeasures. It is conservatively assumed that the existing countermeasures are exceeded or fail, resulting in the most serious consequences. When considering the risk, the existing countermeasures (layers of protections) need to be assessed as to their integrity, reliability and ability to deter, detect and delay. Improved countermeasures to reduce either the severity of the consequence or the likelihood of the event will reduce the risk. The degree of risk reduction for each combination of improved countermeasures can be assessed by using the Consequence and Attractiveness forms for establishing the original risk in Appendix G.

4.1 Development of the Attack Scenarios

Reasonable attack scenarios should be considered for each critical asset.

In this step the SVA team will analyze how vulnerable a chemical distribution asset is to the threats described in Section 3. Each attack scenario should be analyzed for the particular location of chemical assets in the plant and an appropriate threat. The various vulnerabilities to the

attack should be documented. The countermeasures already in place that make up the layers of protection and would hinder the attack are recorded.

Examples of On-Site Attacks

Explosives

- Strategically placing explosives or incendiary devices within the facility, near tanks, storage areas, or on transportation equipment containing flammable or toxic chemicals
- Placing explosives on the vehicle that transports chemicals in bulk or non-bulk quantities
- Shooting (Fire arm, RPG, etc.) bulk or non-bulk containers, tanks, or transportation equipment

Vandalism

- Tampering with storage or transportation equipment
- Tampering with transfer equipment
- Adding a foreign substance to an empty container before it is filled or loaded for transportation
- Setting a fire in the area of the containers
- Product contamination (i.e., food-grade products)

Theft

- Stealing container(s) or transportation equipment and removing from the site
- High-jacking the truck or cargo tank in order to cause a crash or detonation or toxic release in a highly populated area or over a major thoroughfare, on a bridge, or through a tunnel.

Several factors can impact an asset's vulnerability to attack. Some of these include:

- FINAL -

- Visibility – How easily can the site or assets be observed (recognized as a hazardous or dangerous material) by outsiders?
- Consistency – How frequently is the asset present on-site?
- Response & Detection Capability – How quickly could the facility detect outside surveillance or an intrusion? (Consider its use of security patrols, camera surveillance and automatic alarms).
- Accessibility – How easy is it to breach the facility's or asset's security?
- Assets – Recognizable hazardous assets

4.2 Evaluation of the Attack Scenarios

The use of a “What-if/Checklist” may aid the team in developing scenarios. The SVA Team would ask questions such as shown in Appendix I, Attachment 1. The scenarios (undesired Event) can be developed by group brainstorming sessions and recorded on the Scenario Worksheet in Appendix I.

Completing the Scenario worksheet (Appendix I, Attachment 2) will provide the foundation for recommendations to reduce the security risk at a facility. Information collected in the facility asset characterization for the site's key target assets, the attractiveness of these targets, the existing layers of protection, and identified threats will be used to complete the Scenario Worksheet. Attachment 3 in Appendix I provides examples for completing the Scenario Worksheet.

SECTION 5: IDENTIFYING POTENTIAL COUNTERMEASURES

Developing Recommendations, Reports & Implementation

The outcome of the SVA is identification of the security vulnerabilities of the facility and a set of recommendations (as appropriate) to reduce risk. The team identifies potential enhanced countermeasures that in the professional judgment of the SVA Team reduce risk to an acceptable level for the given scenario. Each potential target is protected against the highest level threat associated with that specific target. The recommendations contained in the SVA should be based on a security principles of deter, detect, delay. These principles should be employed in the design and operation of security systems at the site to consider the spectrum of risk reduction options from a recognized list of potential security countermeasures. Recognize that there may be multiple scenarios that result in unacceptable outcomes. Evaluate all scenarios that result in significant impact, not just the highest level threat.

The objective of this SVA model is to emphasize the need for identifying and implementing meaningful countermeasures that appropriately address the vulnerabilities identified and recorded. Because of the diversity of the types of distribution facilities within the NACD membership, and the unique characteristics of each facility, this model does not prescribe specific measures. It does, however, outline general suggestions that, at a minimum, should be considered during the process of developing site-specific countermeasures.

5.1 Using Countermeasures from Chemical Distribution Security Plans - A



reduction in the likelihood or risk of attack is accomplished through the use of enhanced countermeasures. Much of the work of developing vulnerability-reducing countermeasures required by this section has already been done in the implementation of the Responsible Distribution ProcessSM security measures and through compliance with existing regulations such as DOT's HM-232 security plan rules.

- FINAL -

As with any portion of RDP, each member's policies and procedures addressing security will differ from one another. The rule of thumb is to ensure that the security practices are appropriate for the level of risk identified at the site, are regularly audited internally, and corrected if found deficient, with proper documentation of any policy or procedure changes. New or revised countermeasures, if in the form of a new operating procedure or RDP policy, need to be immediately communicated to all employees and readily available to employees. Ensure that security plan documentation is properly protected (access restricted on a need to know basis), however, to prevent against tampering or theft.

Common countermeasures that chemical distribution facilities should consider are listed in Appendix F. Several key examples of countermeasures are highlighted below:

- *Background checks* – on existing employees and those applying for company positions.
- *Installation of physical security barriers* – to protect against attacks on outdoor and indoor assets.
- *Installation of computer security barriers (firewalls)* – prevent access via internet to the LAN or process control systems.
- *Limited access onto the property* – both to office and storage areas.
- *Mandatory employment of photo identification* – for all employees accessing the facility.
- *Regular emergency response drills with company employees as well as the local fire department or first responders* – which is already a membership requirement under NACD's Responsible Distribution ProcessSM.



- 5.2 Use of Existing Government and Industry Guidance on Site and Transportation Security** – Excellent guidance exists that should be considered when implementing countermeasures that address a site or transportation-related vulnerability. The U.S. Department of Homeland Security Guidelines will provide examples of countermeasures for each of the 19 Risk Based Performance Standards under CFATS. The Federal Motor Carrier Safety Administration’s *Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials* is a good resource for transportation – related issues. In addition, following the attacks of September 11, 2001, NACD, along with the American Chemistry Council and the Chlorine Institute, developed *Transportation Security Guidelines for the U.S. Chemical Industry*, which recommends many relevant countermeasures. This document, can be obtained on the NACD Web site at <http://www.nacd.com/advocacy/guidanceDocs.aspx>, or by contacting NACD by phone at 703/527-6223.
- 5.3 Justifications in Selecting or Rejecting Countermeasures** – One final important step is to use the vulnerability and consequence information obtained in Section 4 to determine the necessary specific vulnerability-reduction actions that need to be taken and to be able to justify why some actions were taken and why others were not. It is important to record the justification for the actions taken as well as the actions not taken. Some actions will reduce the impact of an attack. Most actions, however, will be ones that reduce the asset’s likelihood of attack. An appropriate SVA report or documentation (see Section 5.4) should be developed that can be used to communicate the results of the SVA to management for appropriate action. Again, all actions taken and/or enhancements put into place should be documented. Countermeasure recommendations can be prioritized by applying the level of risk identified in Section 2.5 for each asset.



Someone should be assigned to follow-up to ensure that the countermeasures have been implemented. Regular internal compliance audits are required by the Responsible Distribution ProcessSM. Corrective and preventive actions are also required under RDP, with actions documented following an internal audit and any corrective action taken.

5.4 SVA Report – The SVA report should provide adequate documentation of results and technical basis so that “outside-the-team” review is possible and to facilitate future revalidation. The outcome of the SVA is recognition of the security vulnerabilities of the facility and a set of recommendations (as appropriate) to reduce risk.

The SVA results should include a written report that documents:

- The security vulnerabilities of the facility;
- A set of recommendations (as appropriate) to reduce risk;
- A description of or reference to the methodology used for the SVA.
- Results of the SVA should be on a “need to know” basis. This document could provide a roadmap for adversaries.

5.5 Alert Level Actions - Alert levels called for by the U.S. government reflect the premise that there are occasions when the threat to an asset is increased from that of a normal post 9/11 period. The Threat Rating Systems used by the Department of Homeland Security or any of the other governmental or industry alert level system are dynamic systems. The SVA is a point in time (static) assessment and does not provide guidance to changes in the alert level. Response to changes in alert levels (security actions) should be included in *security response plans*.

5.6 Management of Change – As part of the Management of Change (MOC) at the site, the SVA should be revisited based on changes to the site or surrounding community.

NACD Staff acknowledges the many contributions made by numerous NACD member company volunteers in the development of this methodology as well as guidance from other industry trade associations, such as The Chlorine Institute, the Synthetic Organic Chemical Manufacturers Association, and other entities, such as Sandia National Laboratories and the Center for Chemical Process Safety via their methodologies. Without the input and support from NACD members, products such as this one would not be possible.

- FINAL -

APPENDIX A

Chemical Facility Anti-Terrorism Final Rule, 6 CFR Part
27, Appendix A, DHS Chemicals of Interest

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

Copyright © 2008

APPENDIX B

List of Risk Management Program Chemicals

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

B

Copyright © 2008

APPENDIX C

Process Safety Management Summary

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

C

Copyright © 2008

APPENDIX D

List of Chemicals Used for WMDs

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

D

Copyright © 2008

APPENDIX E

Planning Forms

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

E

Copyright © 2008

APPENDIX F

Screening & Facility Characterization Forms

- *FINAL* -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

F

Copyright © 2008

APPENDIX G

Asset Characterization Forms

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

G

Copyright © 2008

APPENDIX H

Threat Assessment Form

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

H

Copyright © 2008

APPENDIX I

Scenario Worksheet & What If Questions

- FINAL -

NACD Chemical Distribution
National Association of Chemical Distributors
Security Vulnerability Assessment Methodology

I

Copyright © 2008