Second Edition

Petroleum Refineries

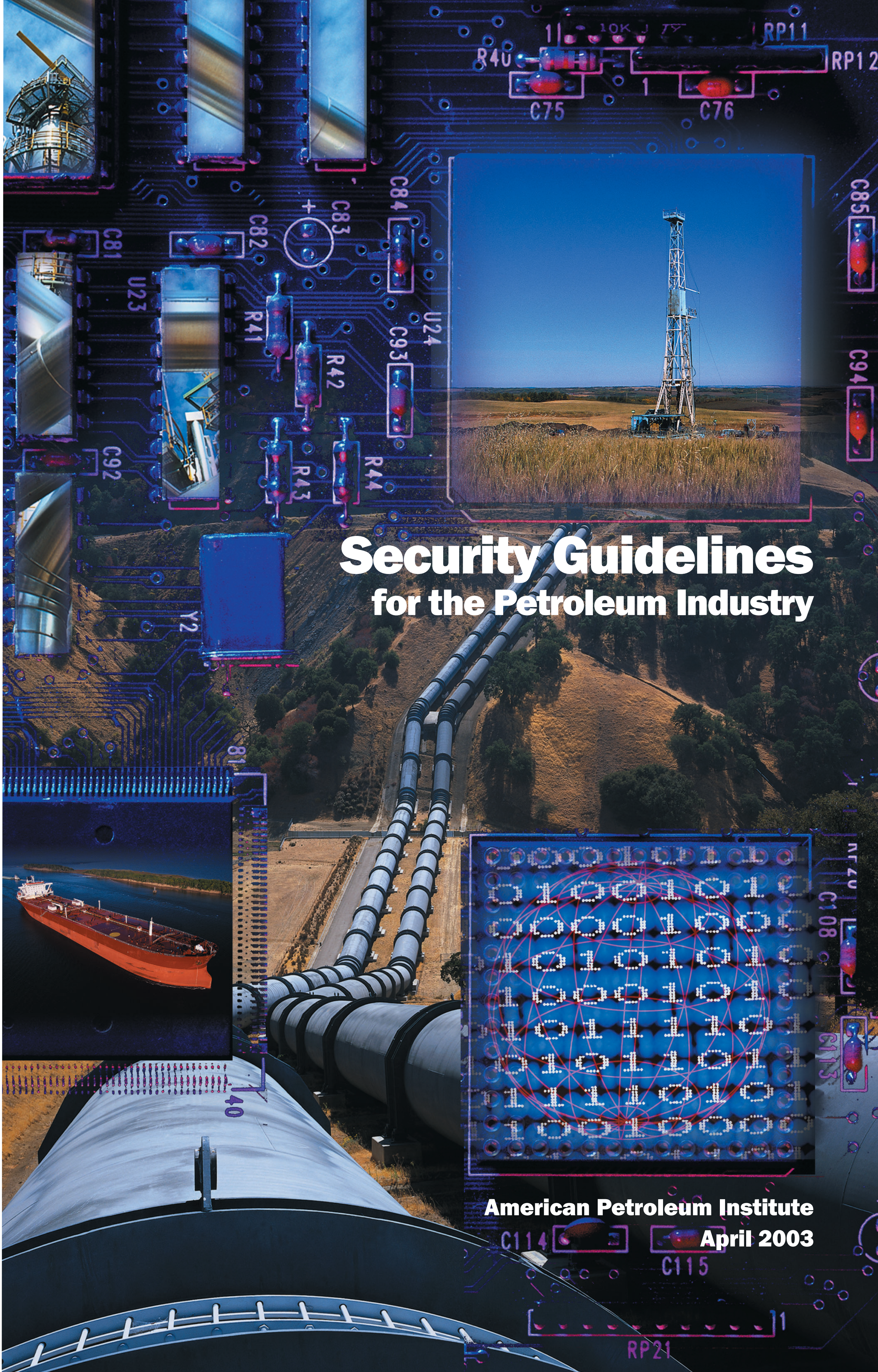
Liquid Petroleum Pipelines

Petroleum Products Distribution and Marketing

Oil and Natural Gas Production Operations

Marine Transportation

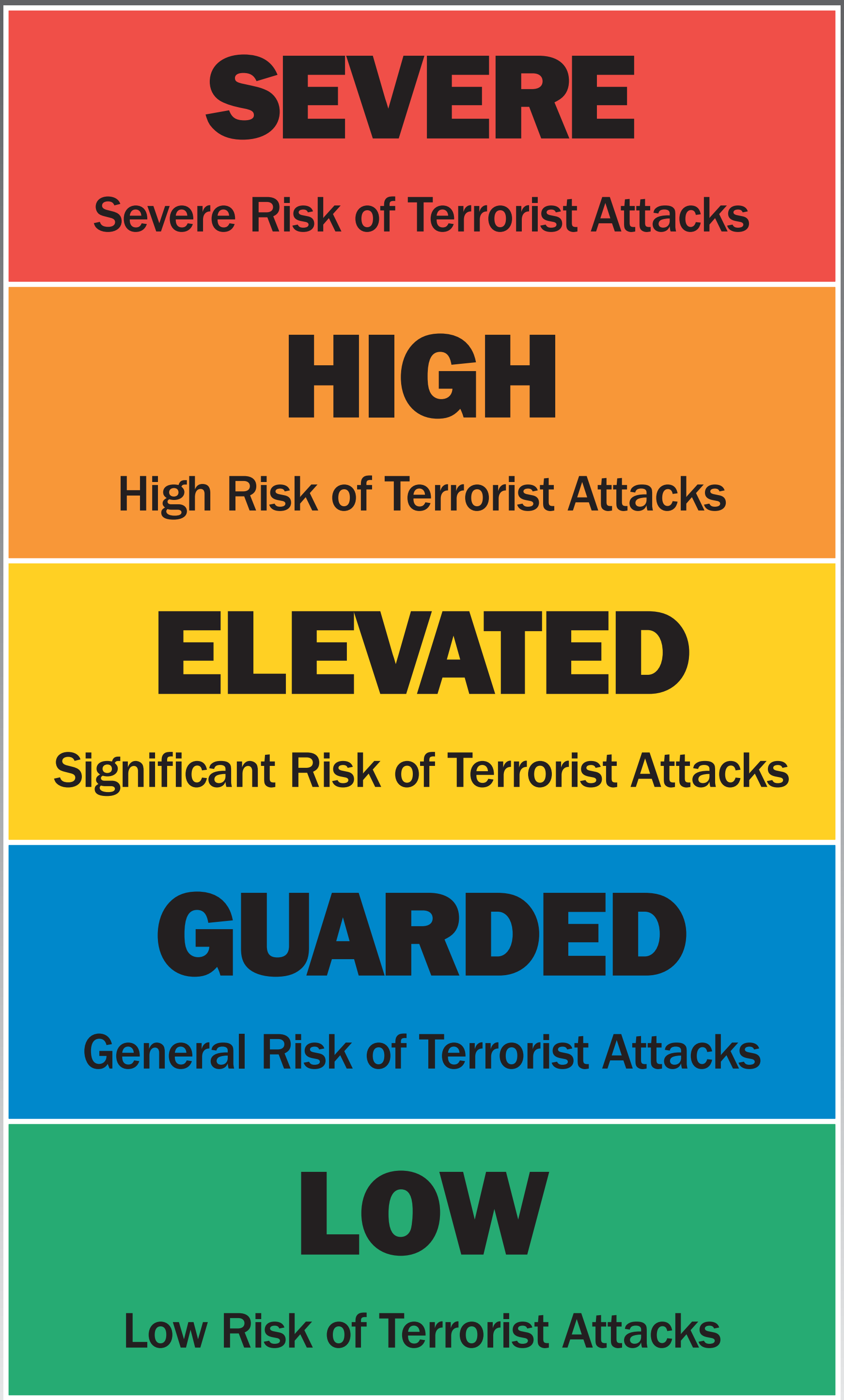
Cyber/ Information Technology for the Petroleum Industry



Security Guidelines
for the Petroleum Industry

American Petroleum Institute
April 2003

Homeland Security Advisory System



SEVERE

Severe Risk of Terrorist Attacks

HIGH

High Risk of Terrorist Attacks

ELEVATED

Significant Risk of Terrorist Attacks

GUARDED

General Risk of Terrorist Attacks

LOW

Low Risk of Terrorist Attacks

www.dhs.gov

American Petroleum Institute
Security Guidelines
For the Petroleum Industry

Table of Contents

Executive Summary iv

Part I—Overview of a Management Systems Approach

1.0 Introduction 1
1.1 Possible Need for Enhanced Security Measures 1
1.2 API Activities to Develop Industry Guidance on Security 1
1.3 Objectives, Intended Audience, and Scope of the Guidance 1
1.4 Underlying Basis of the Guidance 2
1.5 Ongoing Initiatives/Additional Measures Taken Since September 11, 2001 3
2.0 Overview of Terrorism and the Petroleum Industry 5
2.1 Background on Terrorism and Security 5
2.2 Threat to the Petroleum Industry 5
3.0 Threat Assessment 7
3.1 Value of Threat Assessment 7
3.2 Threat Assessment Process 7
3.3 Communication of Security Intelligence 9
3.4 Alert Levels 9
3.4.1 Introduction 9
3.4.2 Department of Homeland Security Alert System (HSAS) 10
3.4.3 Maritime Security Conditions 11
4.0 Elements of a Security Plan 13
5.0 Security Vulnerability Assessment Concepts 15
5.1 Security Vulnerability Assessment Overview 15
5.2 Steps in the SVA Process 16
5.3 Estimating Risk Using SVA Methods 18
5.4 Definition of SVA Terms 18
5.4.1 Risk Definition for SVA 18
5.4.2 Consequences (C) 20
5.4.3 Threat (T) 21
5.4.4 Vulnerability (V) 22
5.4.5 Target Attractiveness (A_T) 22
5.5 SVA Approach 23
5.6 Characteristics of a Sound SVA Approach 23
5.7 First Step in the SVA Process 24
5.8 Data Gathering, Review, and Integration 25
5.8.1 Data Sources 25
5.8.2 Identifying Data Needs 26
5.8.3 Locating Required Data 26

5.8.4 Data Collection and Review 27
5.9 SVA Strength and Limitations..27
5.10 Recommended Times for Conducting and Reviewing the SVA 28
5.11 Core SVA Methodology Components 28
5.12 Validation and Prioritization of Risks..29
5.13 Risk Control and Mitigation 31

Part II—Security Guidelines for Petroleum Refineries 33

Part III—Security Guidelines for Liquid Petroleum Pipelines 49

Part IV—Security Guidelines for Petroleum Products Distribution and Marketing 89

Part V—Security Guidelines for Oil and Natural Gas Production Operations 105

Part VI—Security Guidelines for Marine Transportation 115

Part VII—Security Guidelines for Cyber/Information Technology for the Petroleum Industry..123

Figures

Figure 4.1 Framework for a Security Plan 13
Figure 5.1 Security Events Evaluated during the API SVA Process.. 16
Figure 5.2 API Security Vulnerability Assessment Methodology.. 17
Figure 5.3 Schematic Illustration of Risk.. 19
Figure 5.4 SVA Risk Definition.. 19
Figure 5.5 SVA Risk Variables.. 20
Figure 5.6 Target Attractiveness Features.. 22
Figure 5.7 Recommended Times for Conducting and Reviewing the SVA 28
Figure 4.1 Simplified Risk Assessment Matrix 59

Appendices

Glossary and Terms 137
Appendix A—Framework for a Computer Security Incident Response Plan................................ 143
References……………. 169

FOREWORD

This document is intended to offer security guidance to the petroleum industry and the petroleum service sector. Individual companies have assessed their own security needs and have implemented security measures they consider appropriate. This document is not intended to supplant the measures adopted by individual companies or to offer commentary regarding the effectiveness of individual operator efforts. With respect to particular circumstances, local, state and federal laws and regulations should be reviewed.

Information concerning security risks and proper precautions with respect to particular materials and conditions should be obtained from individual companies or the manufacturer or supplier of a particular material.

API is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning security risks and precautions, nor undertaking their obligation under local, state or federal laws.

To the extent this document contains company specific information such information is to be considered confidential.

Executive Summary

Recognizing the vital importance of safe, reliable energy supplies to our nation's health, security has always been a top priority at petroleum facilities. From designing safe and secure facilities to protecting plants and infrastructure to training with local emergency response teams, companies have long recognized and responded to the need to protect their workers, communities, and energy supplies through a variety of standards and procedures. Since September 11th, the petroleum industry has been broadly evaluating security at its facilities and voluntarily taking actions to improve security as deemed appropriate based on the size, geographic location, potential risk to workers and the surrounding communities, and potential risk of attacks.

In order to help petroleum companies evaluate and respond appropriately to their potential and real security threats, the American Petroleum Institute has worked with other industry associations and companies to prepare security guidance. The risks from terrorist attacks to the U.S. energy supply vary by segment of the petroleum industry, which is broadly defined as petroleum exploration and production, refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution, marketing and the petroleum service sector. Security guidance is therefore provided that is tailored to the differing security needs of these varied segments.

This guidance builds on the existing solid foundation of design and operational regulations, standards and recommended practices, which relate to facility design and safety, environmental protection, emergency response, and protection from theft and vandalism. These existing guidelines are broadly applicable to facility security in light of September 11th, and provided the starting point for developing security guidance at petroleum facilities and operations.

This security guidance is by necessity general in nature. Individual companies, working cooperatively with local officials, are best suited for conducting more detailed assessments of their own facilities and determining how best to protect their assets. This is because both potential threats and appropriate security measures vary dramatically based on size, location, facility type and existing security measures already in place. For obvious security reasons, the individual companies wish to keep the details of their individual plans and countermeasures confidential.

Part I—Overview of a Management Systems Approach

1.0 Introduction

1.1 Possible Need for Enhanced Security Measures

The demands for security at facilities operated by the petroleum industry have dramatically changed since the September 11th terrorist attacks. It is clear that Owner/Operators now face new threats from intentional acts posed by changing world political and social conditions, including an increase in domestic and international terrorism. These previously obscure threats, to U.S. domestic operations in particular, are now considered credible. As such, every facility is challenged with addressing general or specific security threats as appropriate.

1.2 API Activities to Develop Industry Guidance on Security

In order to develop guidance to further help petroleum companies evaluate and respond to their potential and real threats, the American Petroleum Institute has:

- Assessed the general types of risks to the public, workers, the environment, and to petroleum supplies that each sector may face due to terrorism;
- Developed guidance on how to conduct a Security Vulnerability Assessment (SVA) that petroleum companies may use to evaluate terrorism risk;
- Identified existing standards, recommended practices, guidance and other operational practices, as well as ongoing initiatives that may mitigate those risks or vulnerabilities;
- Worked with other industry associations and companies to prepare appropriate guidance.

1.3 Objectives

The objective of this document is to provide general security guidance to owners and operators of petroleum facilities and to the petroleum service sector for managing security risks including the guidance on the principles of security vulnerability analysis.

This document is presented in seven parts. Part I describes a management system to ensure proper planning, organization, and oversight of security. A model is presented that describes the overall concept and the key components of this management system.

Also included in Part I is an example of a generic approach for assessing security vulnerabilities. Referred to as a Security Vulnerability Assessment (SVA), it is a fundamental step in the process of managing security risks. The purpose of the SVA is to understand the threats, security consequences, and the vulnerabilities facing a facility, and then to evaluate specific countermeasures to address those vulnerabilities. This guideline document focuses on the recommended steps of a SVA as it applies to all sectors of the petroleum industry.

In Parts II – VII of this document more specific security guidance is provided for each industry segment including:

- Part II—Petroleum Refineries
- Part III—Liquid Pipelines
- Part IV—Petroleum Products Distribution and Marketing
- Part V—Oil and Natural Gas Production Operations
- Part VI—Marine Transportation
- Part VII—Cyber/Information Technology

API developed this guidance for the industry as another tool that can be used with other available references. Additional guidance on security and security vulnerability assessment includes:

- American Petroleum Institute/National Petrochemical and Refiner's Association Guidance *Security Vulnerability Assessment Methodology*, May 2003
- API RP 70, *Security for Offshore Oil and Natural Gas Operations*, First Edition, April, 2003
- The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) *Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites*, August 2002[1],
- Sandia National Laboratories *Vulnerability Assessment Methodology for Chemical Facilities* (VAM-CF).

The API security guidelines should also be considered in light of any applicable governmental security regulations and guidance.

1.4 Underlying Basis of the Guidance

Owner/Operators should ensure the security of facilities and the protection of the public, the environment, workers, and the continuity of the business through the management of security risks. The premise of the guidelines is that security risks should be managed in a risk-based, performance-oriented management process.

The foundation of the security management approach is the need to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of the countermeasures provided to mitigate the threats. Security Vulnerability Assessment (SVA) is a management tool that can be used to assist in accomplishing this task, and to help the owner/operator in making decisions on the need for and value of enhancements.

The need for security enhancements will be determined partly by factors such as the degree of the threat, the degree of vulnerability, the possible consequences of an incident, and the attractiveness of the asset to adversaries. In the case of terrorist threats, higher risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of consequences, and where the level of vulnerability and threat is high.

Appropriate strategies for managing security can vary widely depending on the circumstances including the type of facility and the threats facing the facility. As a result, this guideline does not prescribe security measures but instead suggests means of identifying, analyzing, and reducing vulnerabilities. The specific situations must be evaluated individually by local management using best judgment of applicable practices. Appropriate security risk management decisions must be made commensurate with the risks. This flexible approach recognizes that there isn't a uniform approach to security in the petroleum industry, and that resources are best applied to mitigate high risk situations primarily.

A basic premise is that security risks cannot be completely prevented. The security objectives are to employ four basic strategies to manage the risk including Deter, Detect, Delay, and Respond.

All Owner/Operators are encouraged to seek out assistance and coordinate efforts with federal, state, and local law enforcement agencies, and with the local emergency services and Local Emergency Planning Committee. Owner/Operators can also obtain and share intelligence, coordinate training, and tap other resources to help deter attacks and to manage emergencies.

1.5 Ongoing Initiatives/Additional Measures Taken Since September 11, 2001

Since September 11, 2001, the petroleum industry has been actively working to reassess potential threats to its facilities and its vulnerability to terrorism. API and its companies have been working closely with the Department of Energy (DOE) and the Department of Homeland Security (DHS) under an industry/government partnership to ensure that safe and reliable energy supplies are secure and that workers and surrounding communities are safe. To do this, there is recognition that each petroleum facility has its own set of unique circumstances and its own unique security needs based on a variety of geographical and operational characteristics. These needs can vary widely for individual facilities depending on such factors as size, complexity, location, products, consequences if attacked, importance to the energy supply chain and the safeguards and mitigation controls that are in place. A risk-based approach that considers both the consequences and likelihood of a potential terrorist attack considers these factors during the assessment process and can provide a balanced approach with a focus toward that of greatest impact.

Following are examples of enhanced security measures that have been implemented at petroleum facilities across the country:

- API established a DOE/Industry Security Partnership, including vulnerability assessment, threat information sharing and technology transfer
- API is conducting industry security conferences and workshops, emphasizing best practice sharing and benchmarking
- Industry has set up an Energy Industry Information Sharing and Analysis Center (ISAC) to help better share intelligence and industry practices
- API has developed Industry Security Guidelines and a Petroleum Industry Security Vulnerability Assessment Methodology
- Individual companies have improved security measures by:

    - Conducting security vulnerability assessments
    - Establishing access control procedures for persons and vehicles entering and leaving the facility
    - Establishing heightened security procedures for handling packages

- Enhancing perimeter protection against vehicular intrusion
- Bolstering security procedures for ship personnel disembarking the ship onto facility docks
- Applying technical security sensors and intrusion detection to facility perimeters and waterside access
- Liaison and coordination with industry leaders to exchange security best practices and countermeasures
- Establishing or enhancing corporate in-house intelligence gathering and analysis capabilities
- Increasing security guards and surveillance equipment
- Conducting background checks of employees and contractors
- Tracking security information and alert levels and have appropriate security procedures in place to respond to the alert levels.
- Modifying assessments relating to physical security, product theft and hostile threat
- Providing 24/7 lock-in with card-in procedures at marketing terminals
- Instructing drivers not to leave running trucks or keys unattended (trucks are kept locked while driving and unloading)
- Enhancing communications with local police and emergency response personnel to discuss emergency procedures and security issues
- Locking pumps at loading facilities to prevent theft
- Assessing the need for 24/7 attendants at retail facilities
- Considering biomarker identification technology for marketing terminal access
- Requiring heightened awareness by facility personnel for suspicious behavior
- Use of video/CCTV to monitor remote areas such as docks and gates.

2.0 Overview of Terrorism and the Petroleum Industry

2.1 Background on Terrorism and Security

The FBI defines terrorism as, "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives." It has become abundantly clear that various organizations and individuals are determined to use previously unseen means and forces to cause maximum damage and harm to governments, businesses, the environment, and members of the public. All sectors of the U.S. economy are potentially subject to these illicit activities. The number of international terrorist incidents has increased recently and the potential threat posed by terrorists has increased[2].

2.2 Threat to the Petroleum Industry

The petroleum industry is in all probability generally subject to these threats due to several factors:

- the physical and chemical properties of the materials processed, stored and handled at these facilities may create attractive targets for an adversary to cause malicious release with the intent to harm a neighboring population,
- the critical importance of the products produced by companies to the domestic and international infrastructure and to other businesses and individuals may make disruption of operations of the petroleum industry an attractive option.

Reports from organizations such as the U.S. State Department[3], Federal Bureau of Investigation and others have concluded that the petroleum industry is targeted by various terrorist groups. These new threats must be jointly addressed by government and industry due to the potential harm that intentional releases may cause.

The challenge facing the industry is to work with the appropriate law enforcement agencies to address this concern in an expeditious manner while the threat remains generalized however there is little to no experience with terrorism causing such events in the petroleum industry in the United States at the present time. This poses a particularly difficult management problem, but more informed risk management decisions can be made if a complete Security Vulnerability Analysis is used as a basis of the threat assessment and security plan provided.

The risks from terrorist attacks to U.S. energy supplies vary by segment of the oil industry. The industry’s facilities and assets are widely distributed, consisting of over 300,000 producing sites, 4,000 offshore platforms, more than 600 natural gas processing plants, over 160,000 miles of pipelines (petroleum liquids), multiple oil offloading ports and facilities, 144 refineries, and more than 1,400 product terminals, 7,500 bulk stations and 170,000 gasoline retail stations. This wide distribution of domestic assets suggests that it is very difficult to interrupt, in any material way, the distribution of petroleum and petroleum products in the U.S. by targeting a single, or even a few facilities. Also, a large majority of these facilities are small, geographically remote, or difficult to use as an instrument for terrorist purposes. Nonetheless, the industry supports the need to evaluate risks to determine the individual and collective risk of major security events caused by terrorism.

The general risks to energy supply and vulnerability varies by segment of the petroleum industry, which we define broadly for these purposes as petroleum exploration and production, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing. Electronic data, computer hardware and software, prevalent throughout the high tech petroleum industry, are logically treated separately with respect to security.

3.0 Threat Assessment

3.1 The Value of Threat Assessment

Threat assessment is an important part of a security management system, especially in light of the emergence of international terrorism in the United States. There is a need for understanding the threats facing the industry and any given facility or operation to properly respond to those threats. This section describes a threat assessment approach as part of a security management process. Later in Section 5.0 the use of the threat assessment in the SVA process will be explained.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets.[4] It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of an attack.

Threat assessment is a process that must be systematically done and kept current to be useful. The foundation of the determination of acceptable security risk is the concept of design basis threats. The determination of these threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of required countermeasures to manage the threats. Without a specific threat in mind, a company cannot effectively develop a cost-effective security management system.

3.2 Threat Assessment Process

In characterizing the threat to a facility or a particular asset for a facility, a company examines the historical record of security events and adversaries and obtains available general and location-specific threat information from government organizations and other sources. It then evaluates these threats in terms of company assets that represent more likely, higher payout targets to those adversaries.

Some threats are assumed continuous, whereas others are assumed to be variable. As such, this guidance follows the Department of Homeland Security’s Homeland Security Advisory System (HSAS) for management of varying threat levels to the industry, which is further explained in section 3.4. The threat assessment determines the estimated general threat level, which forms a baseline for which security measures can be defined. Then intelligence and threat assessment works to help evaluate situations as they develop. Depending on the increased threat level, different security measures over baseline measures may be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated as on a regular basis, threat assessments might not adequately capture emerging threats posed by some terrorist groups. Consequently, a threat assessment must be accompanied by a vulnerability assessment to provide better assurance of preparedness for a terrorist attack.

Intelligence and law enforcement agencies assess the foreign and domestic terrorist threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The Terrorist Threat Integration Center was established to gather and coordinate information and assess the threat posed by domestic sources of terrorism. [5]

Threat information gathered by both the intelligence and law enforcement communities can be used to develop a company-specific threat assessment. A company attempts to identify threats in order to decide how to manage risk in a cost-effective manner. All companies are exposed to a multitude of threats, including terrorism or other forms of threat.

A threat assessment can take different forms, but the key components include:

1. The identification of known and potential adversaries;
2. The recognition and analysis of their intentions, motivation, operating history, methods, weapons, strengths, weaknesses, and intelligence capabilities;
3. The assessment of the threat posed by the adversary factors mentioned above against each asset, and the assignment of an overall criticality ranking for each adversary.

Threats need to be considered from both insiders and outsiders, or a combination of those adversaries working in collusion. An external adversary uses unauthorized access to the facility and systems to destroy or steal a target asset. Insiders are defined as those individuals who normally have authorized access to the asset. Insiders pose a particularly difficult threat, due to the possibility for deceit, deception, training, knowledge of the facilities, and unsupervised access to critical information and assets.

The threat categories that should be considered are those that could, at the least, be intent and capable of causing major catastrophic harm to the facilities and to the public or environment. Four typical threats that may be included in a SVA are the threat posed by international terrorists, domestic terrorists including disgruntled individuals/’lone wolf’ sympathizers, disgruntled employees, or extreme activists. Other adversaries may need to be evaluated as appropriate.

All companies are encouraged to discuss threats with local and Federal law enforcement officials, and to maintain networking with fellow industrial groups including national, regional, and local, to improve the quality of information relied upon. In particular, owner/operators should coordinate with the Joint Terrorism Task Force offices.

The threat assessment is not necessarily based on precise information. In fact, for most facilities, the best available information is vague or nonspecific to the facility. A particularly challenging part of the analysis can be the absence of site specific information on threats, particularly the recent concern for international terrorism. A suggested approach is to make a design basis threat assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat. Site specific threat information adjusts the generic average rankings accordingly. Until better information is available, this assumption is crucial to the analysis.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats facing the assets. At that time the company's threat assessment should be referred to and possibly updated as required given additional information and assessment of vulnerabilities.

3.3 Communication of Security Intelligence

One important key to mitigate acts of terror and to protect facilities lies in good intelligence, and the quick dissemination of information to the large number of Owner/Operators that may need the information.

The Energy Information Sharing and Analysis Center (ISAC was created to serve as an information dissemination organization to provide government intelligence to industry concerning potential acts of terrorism).

An ISAC consists of a secure database, analytic tools, and information gathering and distribution facilities that allow authorized individuals to submit either anonymous or attributed reports about information and physical security threats, vulnerabilities, incidents, and solutions. ISAC members also have access to information and analysis relating to information provided by other members and obtained from other sources, such as the US government and law enforcement agencies, technology providers, and security associations such as CERT. The ENERGY-ISAC is exclusively for, and designed by, professionals in the energy industries. No US government agency, regulator, or law enforcement agency can access the ENERGY-ISAC. Other critical industries, such as finance and telecommunications, have ISACs in place.

Organizations wishing to apply for membership in the ISAC may obtain membership information at (http://www.energyisac.com/) or by calling API at 202-682-8590. Membership requests should be mailed to the ISAC administrator at:

Energy ISAC, C/o American Petroleum Institute
1220 L. Street N.W.
Washington, D.C. 20005
USA
Attn: Energy ISAC Program Coordinator

3.4 Alert Levels

3.4.1 Introduction

The basis of operational security is that as threat climates change, variable security measures are provided accordingly. Alert levels describe a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent risk of attack or action, based on government or company intelligence information. Refer to Parts II through VII of the guidelines for possible sector-specific actions the petroleum industry may take based on these threat levels.

There are two relevant alert level systems that have been developed by the government or government/industry partnerships to warn of the potential for acts of terrorism:

- Homeland Security Advisory System (HSAS): A 5-level alert system based on the National Threat Advisory System developed by the Department of Homeland Security.
- Marine Security Levels (MARSEC): A 3 level alert system developed by the U.S. Coast Guard for use by marine vessels and ports.

The purpose of these systems is to provide clear information to industry on the potential for terrorist action. This is to help facilities implement appropriate response measures, if needed, during a threat crisis. The petroleum industry would prefer a single alert system, and is actively encouraging government agencies to adopt the Homeland Security Advisory System which could then be used by all of the petroleum industry segments.

3.4.2 Department of Homeland Security Alert System (HSAS)

The Homeland Security Advisory System (HSAS) was established on July 27, 2002. This five level color-coded threat advisory system was designed to improve coordination and communication at all levels of Government and with the American public in the fight against terrorism. HSAS provides a framework to assign threat conditions, which can apply nationally, regionally, by sector or to a specific target. The following factors that may be used to assess the threat are:

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- What are the potential consequences of the threat?

Threat conditions characterize the risk of a terrorist attack. Protective measures are the steps to be taken by a potential target to reduce their vulnerabilities. The HSAS establishes five threat conditions with associated general protective measures. It must be emphasized that specific protective measures should be developed by the facility based on the unique characteristics of that particular facility and from the findings from a site-specific SVA.

- **Low Condition—Green:** Low risk of terrorist attacks. The following general protective measures may apply:
    - Refine and exercise preplanned protective measures;
    - Ensure personnel receive training on HSAS, corporate and facility specific protective measures;
    - Regularly assess facility vulnerability and take measures to reduce them.

- **Guarded Condition—Blue:** General risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
    - Check communications with designated emergency response locations;
    - Review and update emergency response procedures;

    - Provide the surrounding community with necessary information.

- **Elevated Condition—Yellow:** Significant risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
    - Increase surveillance of critical locations;
    - Coordinate emergency plans with local jurisdictions;
    - Assess further refinement of protective measures within the context of the current threat information;
    - Implement, as appropriate, contingency and emergency response plans.

- **High Condition—Orange:** High risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
    - Coordinate necessary security efforts with armed forces or local law enforcement
    - Take additional precautions at public events;
    - Prepare to work at an alternate site or with a dispersed workforce;
    - Restrict access to essential personnel only.

- **Severe Condition—Red:** Severe risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
    - Assign emergency response personnel and pre-position specially trained teams;
    - Monitor, redirect or constrain transportation systems;
    - Close facilities;
    - Increase or redirect personnel to address critical emergency needs.

The National Infrastructure Protection Center publishes guidance on protective measures that are recommended for the different threat levels[6]'.

3.4.3. Maritime Security Conditions

The U.S. Coast Guard has developed a three level Maritime Security Conditions (MARSEC) alert system for use by marine vessels and ports. The MARSEC alert levels are:

- **MARSEC I:** Low or Moderate Threat—this alert is defined as the "new normalcy".
- **MARSEC II:** Heightened Alert—this alert is issued when there is credible intelligence suggesting a high threat, but no specific target or delivery method is known.
- **MARSEC III:** Maximum Alert—this alert is issued when there is credible intelligence coupled with a specific threat.

The U.S. Coast Guard will communicate heightened levels of alert using Maritime Security levels (MARSEC) 1, 2, and 3 that align with the graduated color-coded Threat condition levels defined by the Homeland Security Advisory System (HSAS). MARSEC is the maritime sector's tool for communicating risk and in most cases will be linked to the HSAS. MARSEC Level I generally correspond to the lowest three levels of HSAS: Green (Low), Blue (Guarded), and Yellow (Elevated). MARSEC Level 2 corresponds to HSAS Orange (High); and MARSEC Level 3 corresponds to HSAS Red (Incident Imminent).

Facilities should develop and implement protective measures, to be reflected in their security plans, which increase as the MARSEC level increases to reduce the risk of a transportation security incident. MARSEC levels may be assigned for the entire nation, or they may be set for a particular geographic area, industrial sector, or operational activity. It should be noted that it is possible to shift from MARSEC 1 directly to MARSEC 3 without an intermediate shift to MARSEC 2. [7]

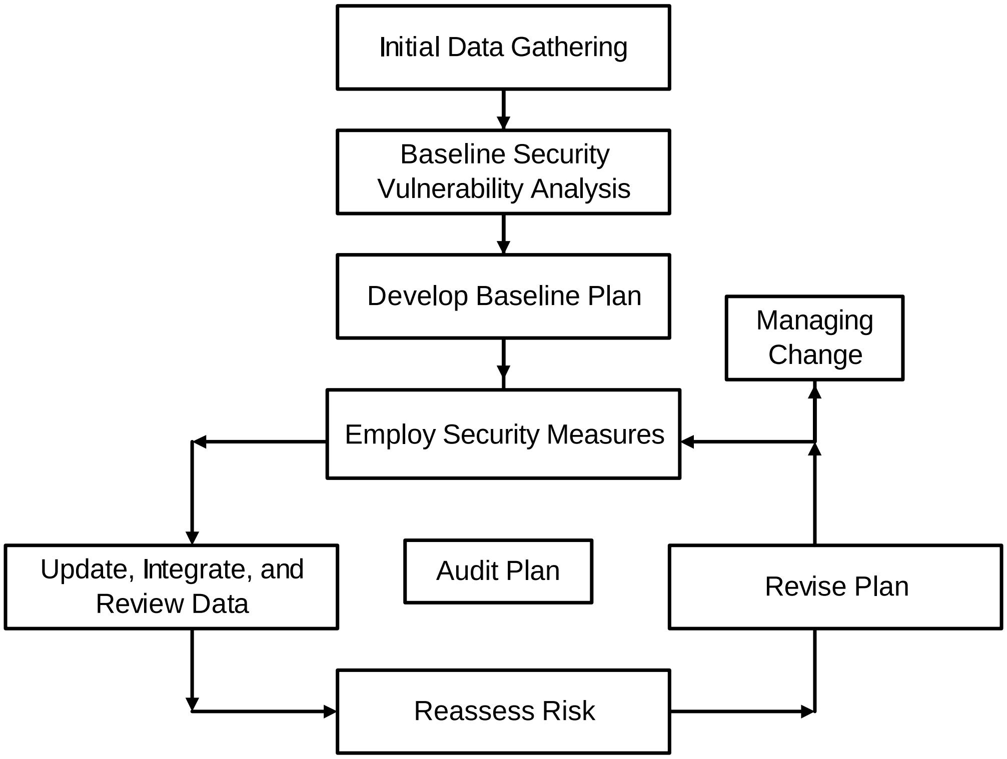
4.0 Elements of a Security Plan

A security plan to manage security risks should be developed for all facilities subject to these guidelines. All petroleum facilities have unique design features and operating characteristics, necessitating individualized facility security plans. An effective security plan should have a solid base of several essential elements. Figure 4.1 illustrates a typical security plan framework.

The framework shown in Figure 4.1 provides a common structure upon which to develop a site-specific security plan. In developing a security plan, Owner/Operators should consider their unique security risks, and then assess the risks to assure the plan addresses key risks. There are many different approaches to implementing the different elements identified in Figure 4.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all petroleum facilities for all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

The details of what should be included in each of the steps of Figure 4.1 are included in Parts II – VII.

Figure 4.1 – Framework for a Security Plan



It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 4.1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, the selection of a SVA approach depends in part on what risk related data and information are available. Conversely and while performing a SVA, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and SVA elements could be highly integrated and iterative.

Section 5.0 describes a key element in this plan—the analysis of risks to the public, employees, facility, and operations through a risk-based security vulnerability assessment process.

5.0 Security Vulnerability Assessment Concepts

5.1 Security Vulnerability Assessment Overview

Security Vulnerability Assessment (SVA) is a systematic, analytical process to evaluate the likelihood that a threat will harm an asset or individuals and considers the probable severity of consequence resulting from the malevolent act. One purpose of this is to systematically identify actions that may reduce the risk of an attack or event as required. It is a team-based approach whereby the combined expertise of employees knowledgeable of the facility and its operation work with those knowledgeable of security, process safety, and other disciplines necessary to conduct the assessment.

There are several SVA techniques and methods available and they all share common elements. Ultimately, it is the responsibility of the operator to choose the SVA method and depth of analysis that best meets the requirements of the SVA task.

Independent of the SVA method used, all techniques include the same basic components:

1. Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure, and the consequences if they are damaged or stolen;
2. Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary;
3. Identify potential security related events or conditions that threaten the system's service or integrity;
4. Determine risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
5. Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk;
6. Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk.

The objective of conducting an SVA at a facility should be:

"To conduct an assessment to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company."

Owner/Operators can use any appropriate security vulnerability assessment methodology including:

- the American Petroleum Institute/National Petrochemical and Refiner's Association guidance "Security Vulnerability Assessment Methodology";
- the American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites";

- the Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF);
- another appropriate methodology suitable for this purpose.

This guidance should also be considered in light of any applicable governmental security regulations and guidance.

While the SVA process can be used to assess a wide variety of security issues, the SVA should address at a minimum the security events listed in Figure 5.1 since these represent key consequences of concern. These are the same four security issues identified in the CCPS® SVA guidelines.

Figure 5.1
Security Events Evaluated During the SVA Process

1. Loss of containment of toxic substances or flammable hydrocarbons at the facility from intentional damage of equipment or the malicious release of these materials, which may cause multiple casualties, severe damage, and public or environmental impact;
2. Toxic substance or flammable hydrocarbons theft or misuse with the intent to cause severe harm at the facility or offsite;
3. Contamination or spoilage of plant products to cause worker or public harm on or offsite;
4. Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive malevolent acts.

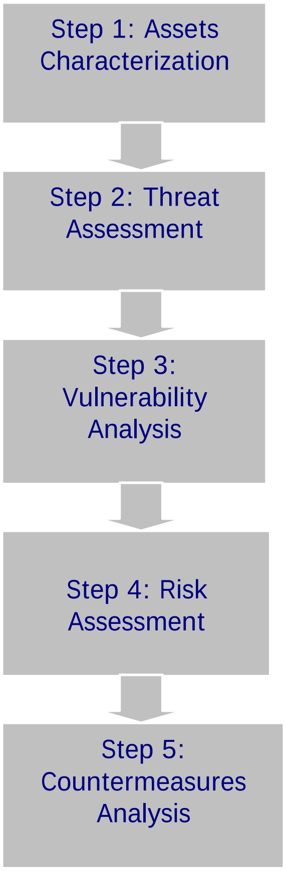
5.2. Steps In the SVA Process

Figure 5.2 presents the SVA process flow diagram from the API/NPRA Security Vulnerability Assessment Methodology. It should be noted that this approach to conducting security vulnerability assessments has been developed specifically for the petroleum industry. Other valid approaches to conducting vulnerability assessments have been developed and are being used successfully within the petroleum industry as mentioned in Section 5.1 above.

To obtain a copy of the “API/NPRA SVA Methodology” contact:

American Petroleum Institute 1220 L. Street, N.W. Washington, DC 20005 (202) 682-8439	National Petrochemical and Refiners Association 1899 L. Street, N.W. Washington, D.C. 20036 (202) 457-0480

Figure 5.2
API/NPRA Security Vulnerability Assessment Methodology


Step 1: Assets Characterization
Step 2: Threat Assessment
Step 3: Vulnerability Analysis
Step 4: Risk Assessment
Step 5: Countermeasures Analysis

1.1 Identify critical assets
1.2 Identify critical functions
1.3 Identify critical infrastructures and interdependencies
1.4 Evaluate existing countermeasures
1.5 Evaluate impacts
1.6 Select targets for further analysis

2.1 Adversary identification
2.2 Adversary characterization
2.3 Target attractiveness

3.1 Define scenarios and evaluate specific consequences
3.2 Evaluate effectiveness of existing security measures
3.3 Identify vulnerabilities and estimate degree of vulnerability

4.1 Estimate risk of successful attack
4.2 Prioritize risks

5.1 Identify and evaluate countermeasures options
5.2 Prioritize potential enhancements

5.3 Estimating Risk Using SVA Methods

Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it. This is particularly true for the threat of terrorism. While this is the case, it is important to make risk decisions about these threats using a systematic method. SVA methods are tools that provide management with risk information based on a thorough, more defensible process. However, the quality of the study is dependent on the quality of the inputs and the soundness of the logical relationships inherent in the SVA method used to evaluate the input and output conditions.

5.4 Definition of SVA Terms

5.4.1 Risk Definition for SVA

Security risks are different from safety risks. The concept of threat needs to be understood as a combination of an adversary's capability plus their intent. One without the other, and there is no threat.

The petroleum industry has a great deal of experience in managing risks in the safety arena. In that context, risk is usually expressed as a product of probability and consequences. Traditional risk management has focused on the likelihood of an accidental event taking place.

In the security realm, this traditional model begins to break down. In the absence of specific intelligence information, it is impossible to be specific about the likelihood of an attack. One conclusion of this reasoning is that there is no risk—a misleading and incorrect conclusion.

For this reason, surrogates to likelihood of attack are necessary. Due to the uncertainty of estimating the likelihood of an attack on any particular location, it is recommended to use several variables to compose an estimate. These are a function of an assumed threat, i.e., for example a terrorist. For the purposes of a SVA, the definition of risk is:

"Risk is an expression of the likelihood that a defined threat will target and successfully exploit a specific vulnerability of an asset and cause a given set of consequences."[8]

Figure 5.3 provides a simple depiction of risk, and Figure 5.4 defines risk for the SVA process.

Figure 5.3 – Schematic Illustration of Risk

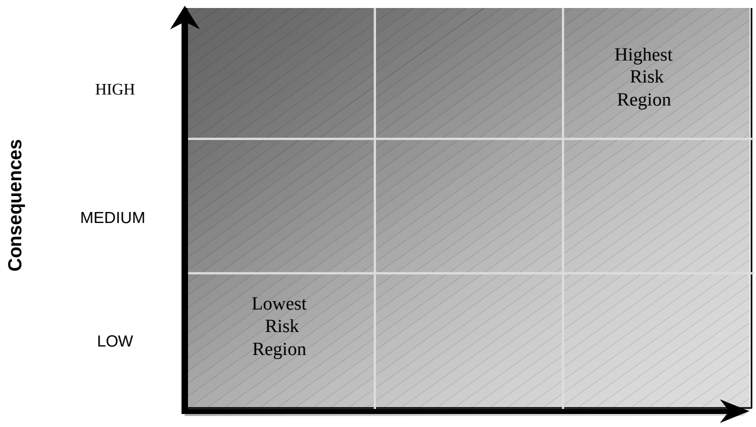


Figure 5.4 **SVA Risk Definition**
Security risk is a function of the consequences of an attack and the likelihood of the attack
The likelihood of damage or loss of an asset is a function of the target's attractiveness, the degree of threat, and the degree of vulnerability to the attack.

The risk variables are defined as shown in Figure 5.5.

Figure 5.5
SVA Risk Variables[9]

Consequences	The potential impacts of the event.
Likelihood	Likelihood which is a function of the chance of being targeted for attack, and the conditional chance of mounting a successful attack (both planning and executing) given the threat and existing security measures. This is a function of three variables below.
Threat	Threat, which is a function of the adversary intent, motivation, capabilities, and known patterns of potential adversaries. Different adversaries may pose different threats to various assets within a given facility.
Vulnerability	Any weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt a critical function. This is a variable that indicates the likelihood of a successful attack given the intent to attack an asset.
Target Attractiveness	Target Attractiveness, which is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to the adversary and their degree of interest in attacking the target.

A high risk event, for example, is one which is represented by a high likelihood of a successful attack against a given critical target asset. Likelihood is determined by its attractiveness to the adversary, the degree of threat, and the degree of vulnerability. Criticality is determined by the asset's importance or value, and the potential consequences if attacked. If the likelihood of a successful attack against this type of asset is high, then the risk is considered high and appropriate countermeasures would be required for a high-risk asset.

For the SVA, the risk of the security event is estimated qualitatively. It is based on the consensus judgment of a team of knowledgeable people as to how the likelihood and consequences of an undesired event scenario compares to other scenarios. The assessment is based on best available information, using experience and expertise of the team to make sound risk management decisions. The team may use a risk matrix, which is a graphical representation of the risk factors, as a tool for risk assessment decisions.

5.4.2 Consequences

The severity of the consequences of a security event at a facility is generally expressed in terms of the degree of injury or damage that would result if there was a successful attack. They may involve effects that are more severe than expected with accidental risk. Some examples of relevant consequences in a SVA include:

- Injuries to the public or to workers
- Environmental damage
- Direct and indirect financial losses to the company and to suppliers and associated businesses
- Disruption to the national economy, regional, or local operations and economy
- Loss of reputation or business viability

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to maximize damage, so a worse credible security event has to be defined. Critical infrastructure especially may have dependencies and interdependencies that need careful consideration.

In addition, theft of hazardous materials should be included in SVAs as applicable. Terrorists may be interested in theft of hazardous materials to either cause direct harm at a later date or possibly to make chemical weapons using the stolen materials as constituents.

Consequences are used as one of the key factors in determining the criticality of the asset and the degree of security countermeasures required. During the facility characterization step, consequences and attractiveness are used to screen low value assets from further consideration. For example, terrorists are assumed to be uninterested in unattractive

5.4.3 Threat

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset.[10] It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- Terrorists (international or domestic)
- Activists, pressure groups, single-issue zealots
- Disgruntled employees
- Criminals (e.g., white collar, cyber hacker, organized, opportunists)

Adversaries may be categorized as occurring from three general groups:

- Insider threats
- External threats
- Insiders working as colluders with external threats

The threat information is gathered and is used during the SVA process as an important reference point. To assess an adversary's capability and intent, you need to understand what may motivate them. An operator should consider a range of threats and then look at his system's vulnerabilities to each type of threat. That assessment will determine the areas where an operator will need additional help from federal, state, and local governments.

5.4.4 Vulnerability

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset.[11] Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. In a SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect, or analyzed by considering multiple potential specific sequences of events (a scenario-based approach).

5.4.5 Target Attractiveness

Not all targets are equally of value to adversaries. A basic assumption of the SVA process is that this factor is one factor that influences the likelihood of a security event. ***Target attractiveness*** is an estimate of the real or perceived value of a target to an adversary based on such factors as shown in Figure 5.6.

During the SVA, the attractiveness of each asset should be evaluated based on the adversary's intents or anticipated level of interest in the target. Security strategies can be developed around the estimated targets and potential threats.

Figure 5.6
Target Attractiveness Factors

Type of effect:
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
Type of target:
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognizability of the target

5.5 SVA Approach

Each facility should have an approach for addressing the process of conducting SVAs. This includes a management system for the SVA program for purposes of defining roles and relationships, for obtaining necessary resources, for ensuring the effort is done when required, for ensuring quality of effort, and for following up on implementation of enhanced countermeasures, as examples.

5.6 Characteristics of a Sound SVA Approach

It is important to distinguish between a risk management process and a SVA method, which is what a SVA represents. Risk management is the overall process that includes the SVA, development and implementation of a security plan, and reintegration of data into subsequent SVAs. SVA is the estimation of risk for the purposes of decision-making. SVA methods can be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks of a system. However, SVA methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. SVA methods should be used as part of a process that involves knowledgeable and experienced personnel that critically review the input, assumptions, and results. This review should integrate the SVA output with other factors, the impact of key assumptions, and the impact of uncertainties created by the absence of data or the variability in assessment inputs before arriving at decisions about risk and actions to reduce risk.

A variety of different approaches to SVA have been employed in the petroleum as well as other industries. The major differences among approaches are associated with:

- The relative "mix" of knowledge, data, or logic SVA methods;
- The complexity and detail of the SVA method; and
- The nature of the output (probabilistic versus relative measures of risk).

Ultimately, it is the responsibility of the operator to choose the SVA method that best meets the requirements of the SVA task. Therefore, it is in the best interest of the operator to develop a thorough understanding of the various SVA methods in use and available, as well as the respective strengths and limitations of the different types of methods, before selecting a long-term strategy. A SVA should be:

Structured. The underlying methodology is structured to provide a thorough assessment. Some methodologies employ a more rigid structure than others do. More flexible structures may be easier to use; however, they generally require more input from subject matter experts. However, all SVA methods identify and use logic to determine how the data considered contributes to risk in terms of affecting the likelihood and/or consequences of potential incidents.

Given adequate resources. Appropriate personnel, time, and financial resources must be allocated to fit the detail level of the assessment.

Experience-based. The frequency and severity of past security related events and the potential for future events should be considered. Understand and account for any actions that have been made to prevent security related events. The SVA should consider the system-specific data and other knowledge about the system that has been acquired by field, operations, and engineering personnel as well as external expertise.

Predictive. A SVA should be investigative in nature, seeking to identify recognized as well as previously unrecognized threats to the facility service and integrity. It should make use of previous security related events, but focus on the potential for future events, including scenarios that may never have happened before.

Based on the use of appropriate data. Some SVA decisions are judgment calls. However, relevant data and particularly data about the system under review should affect the confidence level placed in the decisions.

Able to provide for and identify means of feedback. SVA is an iterative process. Actual field drills, audits, and data collection efforts from both internal and external sources should be used to validate (or invalidate) assumptions made.

5.7 First Step in the SVA Process

After obtaining management approval and authorization to proceed, a typical first step in all SVA approaches is to collect a representative group of company experts plus outside experts if needed to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the operator’s system. These experts draw on the years of experience, practical knowledge, and observations from experienced field operations and maintenance personnel in understanding where the security risks may reside and what can be done about them. Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts will focus on the potential problems and risk control activities that would be effective in a facility security plan. The primary goal of this group is to capture and build into the SVA method the experience of this diverse group of individual experts so that the SVA process will capture and incorporate information that may not be available in typical operator databases.

There are a number of techniques employed by these expert teams that have proven useful in assuring a systematic and thorough review. These include:

- Free-form brainstorming of issues and potential risks;
- Conducting an asset-by-asset review;
- Using checklists or structured question sets designed to solicit information on a comprehensive list of potential risks and integrity issues; and
- Using simple risk matrices to qualitatively portray and communicate the likelihood and consequences of different security related events.

For each potential security threat or risk factor, the characteristics or variables that potentially could impact risk (both beneficially and adversely) are identified. During the SVA process, specific risk increasing characteristics of the system are generally either external variables, e.g., outside influences acting on the system, or operation variables, e.g., characteristics associated with the physical properties. In either case, these variables are features of the in-service system and are not easily altered. Variables should be considered individually based on how they impact a specific risk factor. This means that variables could be used in different ways, and with potentially contradictory influences within the SVA.

5.8 Data Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for Owner/Operators to obtain the data needed to manage the security of their facility system. Most Owner/Operators will find that many of the data elements suggested here are already being collected. This section provides a systematic review of potentially useful data to support a security plan. However, it should be recognized that all of the data elements in this section are not necessarily for all systems.

The types of data required depend on the types of risks and failure modes that are anticipated. The operator should consider not only the risks and failure modes currently suspected in the system, but also consider whether the potential exists for other risks and failure modes not previously experienced in the system, e.g., bomb blast damage. This section includes lists of many types of data elements. The following discussion is separated into four subsections that address sources of data, identification of data, location of data, and data collection and review.

5.8.1 Data Sources

The first step in gathering data is to identify the sources of data needed for facility security management. These sources can be divided into four different classes.

Facility and Right of Way Records. Facility and right of way records or experienced personnel are used to identify the location of the facilities. This information is essential for determining areas and other facilities that either may impact the facility or may be affected by the system and for developing the plans for protecting the facility from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various potentially exposed areas surrounding the facility i.e., HCA’s, population centers, and industrial and government facilities.

System Information. This information identifies the specific function of the various parts of the process and their importance from a perspective of identifying the security risks and mitigations as well as understanding the alternatives to maintaining the ability of the system to continue operations when a security threat is identified. This information is also important from a perspective of determining those assets and resources available in-house in developing a security plan and those assets and resources which are needed to complete the plan. Information is also needed on those systems in place, which could support a security plan such as an integrity management program and IT security functions.

Operation Records. Operating data are used to identify the products transported and the operations as they may pertain to security issues to facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, e.g., type of product, facility type and location, and volumes transported. Included in operation records data gathering is the need to obtain incident data to capture historical security events.

Outside Support and Regulatory Issues. This information is needed for each facility or pipeline segment to determine the level of outside support that may be needed and can be expected for the security measures to be employed at each facility or pipeline segment. Data are also needed to understand the expectation for security preparedness and coordination from the regulatory bodies at the government, state, and local levels. Data should also be developed on communication and other infrastructure issues as well as sources of information regarding security threats, e.g., ISAC's (Information Sharing and Analysis Center's).

5.8.2 Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the SVA methodology selected, and the decisions that are to be made. The data collection approach will follow the SVA path determined by the initial expert team assembled to identify the data needed for the first pass at SVA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the SVA team to begin their work with an overview or screening assessment of the most critical issues that impact the facility or pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this SVA. As the SVA process evolves, the scope of the data collection will be expanded to support a more detailed assessment and improved results.

5.8.3 Locating Required Data

Operator data and information are available in different forms and format. They may not all be physically stored and updated at one location based on the current use or need for the information. The first step is to make a list of all data required for security assessment and locate the data. The data and information sources may include:

- P&ID's (Process and Instrument Drawing's)
- Pipeline alignment drawings
- Facility plot plans, equipment layouts and area maps
- Existing company standards
- Product throughput and product parameters
- Emergency response procedures
- Company personnel interviews
- LEPC (Local Emergency Planning Commission) response plans
- Police agency response plans
- Historical security incident reviews
- Support infrastructure reviews

5.8.4 Data Collection and Review

As the collection effort begins, every effort should be made to collect good quality data. When data of suspect quality or consistency are encountered, such data should be flagged so that during the assessment process, appropriate confidence interval weightings can be developed to account for these concerns.

In the event that the SVA approach needs input data that are not readily available, the operator should flag the absence of information. The SVA team can then discuss the necessity and urgency of collecting the missing information.

5.9 SVA Strengths and Limitations

Each of the SVA methods commonly used has its strengths and limitations. Some approaches are well suited to particular applications and decisions, but may not be as helpful in other situations. In selecting or applying SVA methods, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

- Does the scope of the SVA method encompass and identify significant security related events and risks of the facility or along the system? If not, how can the risks that are not included in the SVA method be assessed and integrated in the future?
- Will all data be assessed as it really exists along the system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, e.g. station-by-station or mile-by-mile, dependent on the evaluation needs?
- What is the logical structure of variables that are evaluated to provide the qualitative and quantitative results of the SVA? Does this provide for straightforward data assimilation and assessment?
- Does the SVA method use numerical weights and other empirical factors to derive the risk measures and priorities? Are these weights based on the experience of the system, operator, industry, or external sources?
- Do the basic input variables of the SVA method require data that are available to the operator? Do operator data systems and industry data updating procedures provide sufficient support to apply the SVA method effectively? What is the process for updating the SVA data to reflect changes in the system, the infrastructure, and new security related data? How is the input data validated to ensure that the most accurate, up-to-date depiction of the system is reflected in the SVA?
- Does the SVA output provide adequate support for the justification of risk-based decisions? Are the SVA results and output documented adequately to support justification of the decisions made using this output?
- Does the SVA method allow for analysis of the effects of uncertainties in the data, structure, and parameter values on the method output and decisions being supported? What sensitivity or uncertainty analysis is supported by the SVA method?

5.10 Recommended Times for Conducting and Reviewing the SVA

There are six occasions when the SVA may be required, as illustrated in Figure 5.7:

Figure 5.7
Recommended Times for Conducting and Reviewing the SVA

1	An initial review of all relevant facilities and assets per a schedule set by the an initial planning process
2	When an existing process or operation is proposed to be substantially changed and prior to implementation (revision or rework)
3	When a new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the manager of the facility (revision or rework)
5	After a significant security incident, at the discretion of the manager of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

5.11 Validation and Prioritization of Risks

Independent of the process used to perform a SVA, the owner/operator must perform a quality control review of the output to ensure that the methodology has produced results consistent with the objectives of the assessment. This can be achieved through a review of the SVA data and results by a knowledgeable and experienced individual or, preferably, by a cross-functional team consisting of a mixture of personnel with skill sets and experience-based knowledge of the systems or segments being reviewed. This validation of the SVA method should be performed to ensure that the method has produced results that make sense to the operator. If the results are not consistent with the operator's understanding and expectations of system operation and risks, the operator should explore the reasons why and make appropriate adjustments to the method, assumptions, or data. Some additional criteria to evaluate the quality of a SVA are:

- Are the data and analyses handled competently and consistently throughout the system? (Can the logic be readily followed?)
- Is the assessment presented in an organized and useful manner?
- Are all assumptions identified and explained?
- Are major uncertainties identified, e.g., due to missing data?

- Do evidence, analysis, and argument adequately support conclusions and recommendations?

Once the SVA method and process has been validated, the operator has the necessary information to prioritize risks. To determine what risk mitigation actions to take, the operator considers which systems (or segments of systems) have the highest risks and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

The SVA process or SVA methods can be applied at different stages of the overall security assessment and evaluation process. For example, it can be applied to help select, prioritize, and schedule the locations for security assessments. It can also be performed after the security assessment is completed to conduct a more comprehensive SVA that incorporates more accurate information about the facility or pipeline segment.

5.12 Risk Control and Mitigation

SVA methods are also important tools to help Owner/Operators make cost effective and sound decisions to control security risks on their systems. Once a potential risk has been identified, SVA methods can be used to estimate the expected risk reduction or benefits that will be achieved. The process typically mimics an operator’s current workflow when proposing capital or maintenance projects. When combined with project cost estimates, the SVA methods can compare the cost/benefit results of several proposed projects to help a company determine if the project will be the best solution for the time period under consideration. Potential capital and maintenance improvement activities can be prioritized to support management decision-making. This section provides an overview of this process.

After the results of the SVA are available, the next step is to examine the most significant risks on the system, as well as other opportunities to more efficiently control risks and determine what mitigation actions might be desirable. The risk control and mitigation process involves:

- Identification of risk control options that lower the likelihood of a security related event, reduce the consequences, or both, i.e., mitigation activities;
- A systematic evaluation and comparison of those options to quantify the risk reduction impact of the proposed project; and
- Selection and implementation of the optimum strategy for risk control.

Typically there are many ways to address a particular risk. For example, improvements or modifications can be made to the system hardware or equipment configuration, operation and maintenance practices, assessment practices, personnel training, control and monitoring methods, emergency response, and interface with the public and other external organizations. This guideline provides a discussion of risk control options that are frequently used to reduce different petroleum sector security risks. In order to find the optimum approach to risk control, it is important that a variety of options, and perhaps combinations of activities, be considered, rather than just taking the first idea that is proposed or doing what has always been standard practice. This allows management to consider innovative solutions and perhaps new technologies that may be more effective in addressing risk. Many Owner/Operators have found that a structured process for identifying risk control options and encouraging innovative solutions has produced unique insights and contributed to more effective risk management.

After identifying the risk control options available, the next step is to evaluate and compare the effectiveness of the different alternatives. This evaluation and comparison is often performed at more than one level. For example, a company may desire to select the best approach among several options to address a specific risk. However, on a broader scale, the company may need to evaluate the relative benefits of a number of risk-reduction projects and activities as part of its budget process. In each case, the basis for comparison and ranking should consider both the magnitude of risk reduction benefits expected as well as the resources expended. Many Owner/Operators use a benefit-to-cost ratio where the benefit is the expected risk reduction to evaluate and rank potential risk control projects. This can provide a simple, easy-to-understand metric that allows projects with diverse benefits to be compared.

When conducting a ranking of projects based on a benefit-to-cost approach, a comprehensive evaluation and comparison process should also include a review of the system risks to be sure that relatively high risks are not overlooked simply because the risk control projects proposed don't have a high benefit-to-cost ratio. This may signal the need to consider other risk control options.[1] The process should also consider the amount of risk reduction being achieved to be sure the most effective projects are being proposed. There are many other practical factors that are typically considered when evaluating and prioritizing activities. These can include:

- Uncertainties in both the risk reduction and cost estimates.
- Technological value of a particular option, e.g., employing a new security camera.
- Human resource and equipment constraints.
- Logistical and implementation issues, e.g., delay in ability of vendor to supply necessary equipment.
- Concerns of government organizations and other external constituencies.

Owner/Operators have found that a structured and consistent methodology for evaluating the relative benefits of different options or activities has led to more effective use of resources in their organizations. There are a number of ranking and prioritization tools and approaches that are employed to provide structure and consistency to this evaluation process. These include expert panel reviews, SVA methods, priority matrices, and multi-attribute utility models. Whatever approach is used, it is important that the process consistently uses defined inputs, specific analytical steps, established and clear decision criteria, and documented output.

The security assessment and risk mitigation decisions that are produced by this process are used to develop the security plan, or modify the existing plan, as described in Section 4.0.

When establishing a SVA program, an operator should consider the many features that are unique to its systems and operations to determine which approach is most appropriate. SVA is a

[1] Although summarized in a linear fashion for this guideline, the risk control and mitigation process, like the risk assessment process, can be highly iterative in nature.

"fact finding", not a "fault finding" system analysis. The ultimate goal of SVA is to identify and prioritize significant security risks in the system so the operator can determine how, where, and when to allocate risk mitigation resources to improve system security. The operator must decide what information could be useful in performing the assessment and how that information can be used to maximize the accuracy and effectiveness of the SVA.

SVA is a very important analytical process in a security plan. Although there are a number of different methods for performing SVAs, all approaches should answer the following basic questions:

- What kind of security related events and/or conditions might lead to a loss of system integrity or other serious consequences?
- How likely are these events and/or conditions to occur?
- What is the nature and severity of the consequences if these events and/or conditions occur?
- What overall risks do these events and/or conditions present?

In selecting an appropriate SVA method, an operator must answer a few key questions:

- What management decisions will be made based on the results of the SVA?
- What specific results are required from the SVA to support the decision making process?
- What level of commitment and resources (both internal and external) are required for successful implementation?

5.13 Risk Screening

Security issues exist at every facility managed by the petroleum industry, but the threat of malevolent acts is likely to be differentiated across the industry. This is captured by the factor known as 'target attractiveness', whereby certain assets are considered to be more likely to be of interest to terrorists than others. Based on many reported threat assessments, intelligence reports, and actual events around the world, these factors can be used to evaluate target attractiveness.[12]

It is likely that most facilities have no specific threat history, so the assumption must be made that potential malevolent acts are generally credible at each facility and this is then tempered by the other factors involved. A screening process may contain the following factors:

1. Target attractiveness or target value;
2. Degree of Threat;
3. Difficulty of attack (function of the adversary and the current security measures and vulnerabilities);
4. Potential consequences (casualties, environmental, infrastructure and economic).

These are the same factors as are used for evaluating an individual asset risk, but the difference is that this is done at a generalized facility level for the risk screening.

Note that target attractiveness itself includes the other factors of consequences and difficulty of attack/vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting and anti-terrorism.

Arguably target attractiveness is the dominant factor in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk dilemma. Priority should be given to the Attractiveness Ranking when making assessments. In this way resources can be appropriately applied to assets where they are most likely to be important.

Part II—Security Guidelines for Petroleum Refining

Part II—Security Guidelines for Petroleum Refineries

1.0 Purpose & Objective

The goal of refinery Owner/Operators is to operate and maintain the refineries such that there are no adverse effects on employees, the environment, the public, or the customers as a result of the refiner's actions.

A refinery security program provides a means to improve the security of refineries and to allocate resources to effectively:

- Identify and analyze actual and potential precursor events that can result in refinery security-related incidents.
- Identify the likelihood and consequence of potential refinery security-related events.
- Provide a comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities available.
- Provide a structured, easily communicated means for selecting and implementing risk reduction activities.
- Establish and track program performance with the goal of improving that performance.
- Establish alert and response measures for a broad range of security threats.
- Establish a communications program to share threat information between federal agencies and industry.

This guideline outlines a Security Vulnerability Assessment (SVA) process that a refinery security manager or team can use to assess risks and make decisions about risks in operating a refinery, and to make progress towards the goal of reducing the risks associated with refinery operations. Part I, Section 4.0 describes the framework for creating a refinery security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 4.1. Part I, Section 5 describes the basic features of a SVA.

This guidance does not attempt to provide an all-inclusive list of refinery security considerations, but does provide a basis for measures that could be implemented when evaluating and implementing refinery security measures.

It must be recognized that some of the information that would be part of a refinery security program needs to remain confidential. Facilities may want to develop a confidentiality program to ensure it is understood what information can be shared and what should remain confidential.

2.0 Overview of Segment Operations

There are 144 refineries in the U.S., which have a combined operating capacity of about 16.5 million barrels per day. The average refining capacity of these refineries is about 125,000 barrels per day. Many of these refineries are located on the West and Gulf coasts, primarily because of access to major sea shipping routes. These refineries process crude oil into a variety of petroleum products such as gasoline, heating oil, jet fuel and asphalt.

3.0 Ongoing Initiatives/Additional Measures Taken Since September 11, 2001

Since every refinery is different, individual refineries have been evaluating their own security preparedness and the relative vulnerability of operating units and associated systems. A risk-based approach would take into account both the likelihood and possible consequences of potential terrorist acts. These will vary widely for individual plants depending on the size, complexity, location, products, and associated facilities for particular assets.

4.0 Security Guidelines

The following elements provide general security guidance for petroleum refinery operations relative to potential malevolent acts:

- Each operator should assess the risk and impact of a terrorist attack. The assessment may include a determination of the likelihood of an act or attack, the type of terrorist action and the size and location of the refinery. The assessment may include: 1) the potential risk to workers, 2) the potential risk to the environment and surrounding community; 3) the potential impact to the local, regional and national energy supply; and 4) the potential risk to adjacent and/or interdependent facilities and infrastructure.

- After conducting the assessment, the operator should develop a facility security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, or event, and; 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets and terrorist tactics, actual or attempted incidents, major changes to the facility or new facilities, and periodically audited or tested, as appropriate.

- Owner/Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout its organization. Owner/Operators should respond appropriately to this information to safeguard potential targets. Owner/Operators should also, as appropriate, report suspicious persons, suspicious activities and behaviors, attempted or suspected incursions, terrorists' threats, or actual events (that may suggest a terrorist link) to the appropriate agencies. The Energy Information Sharing and Analysis Center (Energy ISAC) is an avenue to stay informed of intelligence and threat information.

- Each operator should establish clear communication channels and responsibilities for receiving, assessing, preparing for, responding to and recovering from potential or actual threats.

- Owner/Operators should be aware of existing regulations, standards and operating practices as they relate to refinery security.

5.0 Elements of a Refinery Security Management Plan

In developing a refinery security management plan, several basic elements should be considered. The security management plan framework shown in Figure 4.1 provides a general structure upon which a security management plan can be developed. When developing a refinery security management plan, one should consider, to the extent possible, the refinery's unique security risks, and then, if possible, assess the risks to ensure the plan addresses them. There are many different approaches to implementing the different elements identified in Figure 4.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all facilities. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a refinery security management plan could be a highly integrated and iterative process. Although the elements depicted in Figure 4.1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, the details of the SVA approach depends in part on what risk related data and information are available. Also, additional data needs are usually identified during a SVA that better address potential vulnerability issues. Thus the data gathering and SVA elements could be highly integrated and iterative.

A refinery security management plan could include elements such as:

- SVA and prevention strategies
- Incident reporting mechanism
- Communications plan within the facility and with appropriate local, state and federal agencies
- Incident investigation procedures
- Emergency response and crisis management programs
- Reassessment of SVAs
- Reassessment of security management plan
- Cyber security program

6.0 Security Management Plan Framework

An overview of the individual framework elements, with several examples, is provided in this section.

Initial Data Gathering. The first step in understanding the potential risks that may occur at a refinery is to assemble information about such risks. In this element, one performs the initial collection, review, and integration of data that is needed to understand location-specific risks to security. The types of data to support a SVA may include information on the operation, surveillance practices, security measures, and the specific security issues and concerns that are unique. For those that are just formalizing an approach to a security plan, the initial data gathering may be focused on a limited number of facilities or assets so that a screening for the most significant security risks can be readily identified.

Examples of refinery facilities or assets that may be subject to potential risk include:

- Process units
- Control rooms and associated control systems
- Administration offices
- Electrical power grid and facilities (including back-up power systems)
- Utilities such as natural gas lines
- Storage tanks
- Boilers, turbines and process heaters
- Water supply
- Sewer systems
- Wastewater treatment units
- Railroad lines and railcards
- Product loading racks and vehicles
- Pipelines entering and leaving plants
- Ships, dock area and associated equipment

Initial SVA. In this element, the data assembled from the previous step is used to conduct a SVA. The SVA begins with a systematic and comprehensive search to identify possible security risks to the facility. Through the integrated evaluation of the information and data collected in the previous step, the SVA process identifies the location-specific security-related events or conditions, or combinations of events and conditions that could lead to loss of security, and provides an understanding of the likelihood and consequences of these events.

There is a significant variation in the detail and complexity associated with different SVA methods. Some refiners without formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Other refiners may find a screening approach as the most practical means to prioritize facilities for SVA.

Examples of security risks or threats for refineries can include:

- Loss of containment from a process unit
- Loss of containment from a storage tank
- Loss of refinery management team
- Interruption, disruption, or attack of:
  - Electrical power
  - Water supply
  - Communications systems
  - Computer systems
  - Sewer systems
  - Raw material (crude oil) supply
  - Finished product distribution
- Raw material (crude oil) contamination
- Finished product contamination
- Infiltration by outsiders
- Bomb threats
- Bioterrorism
- Cyber attack
- Vandalism

After identifying the most significant risks, the next step is to determine what mitigation actions or security measures might be desirable to reduce risk, and where assessment techniques such as facility security inspections would be of the most value in identifying potential risk-threatening issues. The risk control and mitigation process involves:

- identification of risk control options that lower the likelihood of an incident, reduce the consequences, or both;
- a systematic evaluation and comparison of those options; and
- selection and implementation of a strategy for risk control.

SVA also helps to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote or where the consequence is less than other targets. A tiered, risk-based approach can be the most effective way to evaluate, identify, and prioritize potential targets. There are, however, a number of methods that can be employed to conduct a SVA and identify risk control activities.

Develop Baseline Security Plan. Using the output of the SVA, a plan is developed to address the most significant risks and assess the security of the facility. This plan should include the mitigation risk control actions, as well as security assessment activities, e.g., inspections and traffic and personnel control.

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that

might lead to system failures are controlled. As noted previously, a SVA may identify other risks that should be addressed.

Examples of physical security elements include, but are not limited to:

- Controlling access into, within and out of a refinery
- Perimeter protection
- Security personnel
- Redundant systems (electrical, water, communications, sewer, gas)
- Mail and package screening system

Update, Integrate, and Review Data. After the initial security assessments have been performed, the refiner has available improved and updated information about the security of the facility. This information should be retained and added to the database of information used to support future SVAs and security evaluations. Furthermore, as operations continue additional surveillance and other data are collected, thus expanding and improving the historical database and experience levels.

Reassess Risk. SVAs should be performed periodically to factor in recent operating data, consider changes to the facility design, and to analyze the impact of any external changes that may have occurred since the last SVA, e.g., adjacent facilities and changes in traffic flow. The results of security assessments, such as inspections and drills, should also be factored into future SVAs to ensure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The baseline security management plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated SVA results should also be used to support scheduling of future security assessments.

Audit Plan. Refiners should collect information and periodically evaluate the success of their security assessment techniques and other mitigation risk control activities. The refiner should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions.

Managing Change. A systematic process should be used to ensure that changes to a facility or its operations are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future SVAs to be sure the SVA process addresses the facility as it is currently configured. As this final element indicates, managing security is not a one-time process. As implied by the loop in the lower portion of Figure 4.1, a security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs must be periodically updated and revised to reflect current conditions.

7.0 Security Conditions and Potential Response Measures

This section describes a progressive level of protective measures that may be implemented in response to the possibility of a terrorist threat or to a terrorist threat directed at a refinery, refinery assets, and refinery personnel (including contractors) consistent with the Homeland Security Advisory System (HSAS) developed by the Department of Homeland Security. The purpose of the HSAS is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and operator personnel prior to and during a threat crisis. The associated response measures may be implemented for each security alert level at a refinery.

Each operator should develop a means to advise and communicate to operator personnel and others as warranted the security condition at the refinery and otherwise as applicable. The potential measures associated with each alert level are not prioritized but those implemented should be initiated concurrently where practical and as applicable. Refinery management should maintain a record of specific actions taken for each alert level. Following is a detailed explanation for each alert level and the potential response measures associated with each level:

Low Condition—Green: this condition exists when there is a low risk of possible terrorist activity or civil unrest. **Green** condition is for normal operating conditions. All measures under **Green** should be maintained indefinitely. Potential measures to consider implementing include:

<u>Access Control/Perimeter Protection</u>

- Having all contractors and visitors check or sign in and out of the refinery at designated location(s).

- Ensuring existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting. Identifying those additional security measures and resources that could enhance the security at the higher alert levels, e.g. increased surveillance or lighting.

<u>Communications</u>

- Establishing emergency communications and contact information with appropriate agencies. Considering redundant emergency communications in both the hardware and the means for contacting agencies.

<u>Training/Policies/Procedures/Plans</u>

- Developing terrorist and security awareness information and providing education to employees on security standards and procedures. Cautioning employees not to talk with outsiders concerning their facility or related issues.

- Advising all refinery personnel to report the presence of unknown personnel, unidentified vehicles, aircraft or watercraft, vehicles, watercraft or aircraft operated out of the ordinary, abandoned parcels or packages, and other suspicious activities.

- Incorporating security awareness and information into public education programs and notifications to emergency response organizations as appropriate.

- Surveying surrounding areas to determine those activities that might increase the security risks that could affect the refinery, e.g., airports, government buildings, industrial facilities, and other facilities.

- Ensuring contingency and business continuity plans are current and include a response to terrorist threats.

- Reviewing existing emergency response plans and modifying them, if required, in light of potential threats.

<u>Cyber Security</u>

- Develop and implement hardware, software, and communications security for computer-based operating systems.

Guarded Condition—Blue: This condition exists when there is an increased general threat of possible terrorist activity against the refinery or refinery personnel, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher alert measures. It may be necessary to implement certain selected measures from higher alert levels to address information received or to act as a deterrent. All measures under **Blue** should be maintained as long as the **Blue** threat exists. In addition to the measures suggested by **Green**, the following measures could be considered:

<u>Perimeter Protection/Access Control</u>

- Securing all facilities, buildings and storage areas not in regular use, if possible. Increasing frequency of inspections and patrols within the refinery, including the interior of buildings and along the refinery perimeter.

- Inspecting perimeter fencing and repairing all fence breakdowns. In addition, reviewing all outstanding maintenance and capital project work that could affect the security of the refinery.

- Reducing the number of access points, if possible, for vehicles, aircraft, watercraft and personnel to minimum levels and periodically spot checking the contents of vehicles, watercraft, or aircraft at the access points. Being alert to vehicles or watercraft parked or moored for an unusual length of time in or near a refinery.

- Checking designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increasing surveillance in designated areas.

- Requiring visitors to check in at a refinery office and verifying their identification—being especially alert to repeat visitors or outsiders who have no apparent business at the refinery and are asking questions about the refinery or related issues including the refinery's personnel. Familiarizing refinery personnel with vendors who service the refinery and investigating unusual changes in vendor personnel.

- Inspecting all packages/equipment coming into the refinery. Not opening suspicious packages. Reviewing the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving packages.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.

- Testing security and emergency communications procedures and protocols.

Training/Policies/Procedures/Plans

- Reviewing all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.

- Ensuring that an operator response can be mobilized appropriate for the increased security level. Reviewing communications procedures and back-up plans with all concerned.

Elevated Condition—Yellow: This condition exists when there is an elevated risk of terrorist activity against the refinery or refinery personnel. All measures under **Yellow** should be maintained as long as the **Yellow** threat exists. In addition to the measures suggested by **Blue**, the following measures could be considered:

Perimeter Protection/Access Control

- Closing and locking gates and barriers except those needed for immediate entry and egress. Inspecting perimeter and perimeter fences on a regular basis. Ensuring that other security systems are functioning and are available.

- Inspecting on a more frequent basis the interior and exterior of all buildings and around all storage tanks and other designated critical areas.

- Dedicating personnel to assist with security duties with duties to monitor personnel entering the refinery and to inspecting the area on a regular basis, reporting to refinery management as issues surface.

- Limiting visitors and confirming that the visitor has a need to be and is expected at the refinery. Escorting visitors while at the refinery.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.

- Advising appropriate agencies that the refinery is at a **Yellow** level and advising the measures being employed—requesting agencies to increase the frequency of their routine patrol of the refinery if possible.

- Checking to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirming availability of security resources that can assist with extended coverage, if needed.

- Identifying areas where explosive devices could potentially be hidden.

- Instructing employees working alone to check-in on a periodic basis.

- Directing that all personal, operator, and contractor vehicles at the refinery are secured.

High Condition—Orange: This condition applies when there is a high risk of terrorist attacks or an incident occurs or information is received indicating that some form of terrorist action against the refinery or refinery personnel is imminent. Implementation of measures in this alert for more than a short period will probably create hardship and affect the routine activities of the refinery and its personnel. In addition to the measures suggested for **Yellow**, the following measures could be considered:

Perimeter Protection/Access Control

- Reducing refinery access points to the absolute minimum necessary for continued operation.

- Securing a trained and knowledgeable security workforce at the refinery - ensuring that all security personnel have been briefed concerning policies governing the use of force and pursuit.

- Increasing security patrol activity to the maximum level sustainable. Increasing perimeter patrols and inspections.

- Checking all security systems such as lighting and intruder alarms to ensure they are functioning. Installing additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.

- Prohibiting unauthorized or unidentified vehicles/personnel entrance to the refinery.

- Inspecting all vehicles entering the refinery, if possible, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed. Inspecting all packages and cargo being delivered by aircraft or watercraft.

- Limiting access to the refinery to those personnel who have a legitimate and verifiable need to enter. Implementing positive identification of all personnel. Evacuating all non-essential personnel.

- Implementing frequent inspection of the refinery including the exterior and roof of all buildings and parking areas. Increasing patrolling or inspections at night and ensuring all vulnerable critical points are fully illuminated and secure.

- Protecting the refinery from an attack by a parked or moving vehicle - operator vehicles may be used for this purpose. Implementing centralized parking and shuttle service where feasible.

- Canceling or delaying all non-vital refinery work conducted by contractors, or continuously monitor their work with operator personnel.

Communications

- Advising appropriate agencies that the refinery is at an **Orange** alert level and advise of the measures being employed—requesting an increase in the frequency of their patrol of the refinery.

- Consulting with local authorities about control of public roads and accesses by waterway that might make the refinery more vulnerable to terrorist attack if they were to remain open.

Training/Policies/Procedures/Plans

- Continuing **Green**, **Blue** and **Yellow** measures or introducing those that have not already been implemented.

- Developing procedures for shutting down and evacuation of the refinery, if considered necessary, in case of imminent attack.

- Activating emergency response plans for the refinery.

- Scheduling more frequent visits to designated unmanned locations that are potentially impacted.

- Ensuring that employees not work alone in remote areas or increasing the frequency of call-ins from remote locations.

Severe Condition—Red: This condition applies when there is a severe risk of terrorist attacks, an attack has occurred in the immediate area which may affect the refinery, or when an attack is initiated on the refinery and its personnel. Normally, this alert is declared as a localized condition at the refinery. In addition to the measures suggested for **Orange**, the following measures could be considered:

Perimeter Protection/Access Control

- Augmenting security forces to ensure control of the refinery and access to the refinery and other potential target areas. Establishing surveillance points and reporting criteria and procedures. Soliciting assistance from appropriate agencies in securing the refinery and access, if possible. Cooperating with authorities if they take control of security measures.

Training/Policies/Procedures/Plans

- Continuing **Orange** and **Yellow** measures or introducing those that have not already been implemented.

- Consider shutting down the refinery and operations in accordance with contingency plans unless there is a compelling reason not to and evaluating security prior to resuming operations if they are temporarily shut down.

- Implementing business contingency and continuity plans as appropriate.

Part III—Security Guidelines for Liquid Petroleum Pipelines

Part III—Security Guidelines for Liquid Petroleum Pipelines

1.0 Introduction

1.1 Purpose and Objectives

The goal of all Owner/Operators of petroleum pipelines is to operate and maintain the pipelines in such a way that there are no adverse effects on employees, the environment, the public, or the customers as a result of the pipeline company's actions or actions from other parties. This document provides guidance in planning, developing, and implementing security guidelines, plans, procedures, and practices in the hazardous liquid pipeline industry. Such guidelines, plans, procedures, and practices are put in place by pipeline Owner/Operators with the objectives of seeking to prevent the loss of human life, preventing or reducing impacts on pipeline operations and the supply of crude oil and petroleum products, and to expeditiously restore supply from critical pipeline facilities in the event of an incident. This guidance document addresses security issues specifically as a result of the changed nature of society after September 11, 2001. Pipeline Owner/Operators have many other objectives related to the safety of operations, accident prevention and response, and protection of the environment, which are not specifically addressed here.

A pipeline security plan provides a means to improve the security of pipeline systems and to allocate operator resources to effectively:

- Identify and analyze actual and potential precursor events that can result in pipeline security related incidents.
- Identify the likelihood and consequence of potential pipeline security related events.
- Provide a comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities available.
- Provide a structured, easily communicated means for selecting and implementing risk reduction activities.
- Establish and track plan performance with the goal of improving that performance.
- Establish standardized security conditions and protective measures for a broad range of security threats.

This guideline outlines a process that an operator of a pipeline system can use to assess risks and make decisions about risks in operating a hazardous liquid pipeline and to make progress towards the goal of reducing the security risks associated with operating a pipeline system. Part I, section 4 describes the framework for creating a pipeline security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 4.1 in Part I.

This guideline is intended for use by individuals and teams charged with creating, implementing, and improving a pipeline security plan. Personnel to consider for team membership might include risk managers, security personnel, engineers, operating personnel, IT (Information Technology) personnel, and technicians or specialists with specific experience or expertise, e.g., risk assessment, threat identification, and risk mitigation. Users of this guide should be familiar with the pipeline safety regulations (Title 49 *CFR* Part 195).

This guideline outlines a Security Vulnerability Assessment (SVA) process that a pipeline operator can use to assess risks and make decisions about risks in operating a pipeline, and to make progress towards the goal of reducing the risks associated with operations.

1.2 Guiding Principles

In developing this guideline on pipeline security, certain guiding principles underlie the entire document. These principles are reflected in many of the sections and are provided here to give the reader the sense of the need to view pipeline security from a broad perspective.

- A pipeline security plan must be flexible.

  A pipeline security plan should be customized to support each operator's unique needs. Furthermore the plan must be periodically evaluated and modified to accommodate changes in the pipeline system, changes in the environment in which the system operates, and new data and other security-related information. Periodic improvement is required to be sure the plan is aware of and takes appropriate advantage of new and improved technology, and that the plan remains integrated with the company's business practices and effectively supports the operator's security goals.

- The integration of information is a key component in managing a pipeline security plan.

  A key element of the security management framework is the integration of all available information in the decision making process. Information that can impact an operator's understanding of the important risks to a pipeline system comes from a variety of sources. The operator is in the best position to gather and analyze this information. By integrating available information, the operator can determine where the risk of an incident is the greatest, and make prudent decisions to reduce the risk.

- Preparing for and conducting a SVA is a key element in managing pipeline system security.

  SVA is an analytical process through which an operator determines the types of threats, events, or conditions which might impact pipeline security, the likelihood that these events or conditions will lead to a security related event, and the nature and severity of the consequences that might occur following an event. This analytical process involves the integration and analysis of the pipeline system and its facilities, the environment in which the pipeline operates, and risk mitigation methods available to the pipeline operator. SVAs can have varying scopes, varying levels of detail, and utilize different methods. However, the ultimate goal of assessing risks is to identify and prioritize the most significant risks so that an operator can make informed decisions about the risks.

- Assessing risks to pipeline security is an iterative process.

The operator will periodically gather additional security related information and system operating experience. This information should be factored into the understanding of system risks. As the significance and relevance of this additional information to risk is understood, the operator may need to adjust its security plan accordingly. This may result in changes to SVA methods or frequency, or additional modifications to the pipeline security plan in response to the data.

- Risk mitigation should be employed to reduce the possibility of pipeline security risks.

  Risk mitigation can reduce the risk to a pipeline system from both known and unknown threats. Risk mitigation methods reduce the vulnerability of a pipeline to threats. Risk mitigation starts with management and must involve all employees. A pipeline operator should have policies that are developed for or modified to include risk mitigation.

- All pipeline Owner/Operators should use a standardized set of security conditions and protective measures.

  Appendix A of this guideline provides a standardized set of security conditions and protective measures for use by Owner/Operators in the liquid pipeline industry. The security conditions and protective measures describe a progressive level of steps that are to be implemented in response to a terrorist threat or more specifically to a terrorist threat directed at critical liquid pipeline facilities, assets, and personnel. The purpose of the security conditions is to establish standardized alert levels for a broad range of threats and to help disseminate appropriate and timely information for the implementation of protective measures by management and company personnel prior to and during a threat crisis.

1.3 Classes of Protective Measures

There are a variety of protective measures available to pipeline Owner/Operators to address threats. Some protective measures are aimed at gathering early warning intelligence while others are aimed at detecting, deterring, and mitigating the consequences of an attack. Protective measures should also be based on developing a robust recovery capability to rapidly return to service after an attack.

2.0 Scope

This guideline is applicable to pipeline systems used to transport hazardous liquids as defined in Title 49 *CFR* 195.2. The use of this guideline is not necessarily limited to pipelines regulated under Title 49 *CFR* 195.1, and the principles embodied in a pipeline security plan are applicable to all liquid pipeline systems.

This guideline is specifically designed to provide the operator with a description of security practices that can be applied to pipeline security management. The guidance is specific to pipeline segments and facilities, and the process and approach can and should be applied to all pipeline facilities including pipeline stations, terminals, pipe segments, valve sites, delivery and receipt locations, and control centers associated with pipeline systems.

3.0 Pipeline Security Plan

3.1 Essential Elements:

All pipeline systems have design features and operating characteristics that are unique to each system. An effective pipeline security plan should have a solid base of several essential elements. This section describes a program that includes the essential elements and is the basis for this guideline. Figure 4.1 of Part I of the API Security Guidelines illustrates a pipeline security plan framework.

The framework provides a common structure upon which to develop an operator specific pipeline security plan. In developing a pipeline security plan, Owner/Operators should consider their unique security risks, and then assess the risks to assure the plan addresses all applicable risks. There are many different approaches to implementing the different elements identified in Figure 4.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no “best” approach that is applicable to all pipeline systems for all situations. This guideline recognizes the importance of flexibility in designing pipeline security plans and provides guidance commensurate with this need.

It is important to recognize that a pipeline security plan will be integrated with other operations processes and will change in an iterative manner as conditions change. Although the elements depicted in Figure 4.1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, while performing a SVA, additional data needs are usually identified to better address potential vulnerability issues.

A brief overview of the individual framework elements is provided in this section, as well as a road map to the more specific and detailed description of the individual elements that comprise the remainder of this guideline.

3.2 Framework Elements

Initial Data Gathering. The first step in understanding the potential risks along the pipeline system is to assemble information about potential risks. In this element, the operator performs the initial collection, review, and integration of data that is needed to understand location-specific risks to the pipeline security. The types of data to support a SVA include information on the operation, surveillance practices, security measures, and the specific security issues and concerns that are unique for each system. Section 5 of Part I provides a summary of useful data sources, common data elements that are typically used in SVA, and approaches to data review and integration. For Owner/Operators that are just formalizing an approach to a pipeline security plan, the initial data gathering may be focused on a limited number of facilities or assets so that a screening for the most significant security risks can be readily identified.

Initial SVA. In this element, the data assembled from the previous step is used to conduct a SVA of the pipeline system. The SVA begins with a systematic and comprehensive search to identify possible security risks to the pipeline system. The identification of potential risks should not be limited to a review of known risk categories, but should also include steps to look for new or unique manifestations of risks. Through the integrated evaluation of the information and data collected in the previous step, the SVA process identifies the location-specific security related events or conditions, or combinations of events and conditions, that could lead to loss of pipeline security, and provides an understanding of the likelihood and consequences of these events. The output of a SVA should include the nature and location of the most significant risks on the pipeline system.

There is a significant variation in the detail and complexity associated with different SVA methods. Some Owner/Operators have found that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. During a screening SVA, an operator may limit the scope of the system to those portions of the system where a failure could have the most severe consequences, e.g., interruption of a strategic or high volume supply or an HCA (High Consequence Area) event. Similarly, SVA and data collection may be focused to support identification of the most likely security targets at those facilities or pipeline segments, without going into extensive detail. Some Owner/Operators may find a screening approach as the most practical approach to prioritize facilities or pipeline segments for SVA.

The quantitative SVA methods are those where the characteristics of segments of the pipeline and the surrounding area are used to derive an actual estimate of the risk for that segment. Likelihood is estimated as the probability of a security related event along the segment over a given period of time. Actual expected levels of consequences in different categories (human, environmental, economic) are estimated and may be combined using some common metric (for example, equivalent dollar cost). The total risk for the segment is estimated as the product of the likelihood of a security related event and the expected consequences given the event. Some SVA methods calculate the likelihood of different security risks, and then estimate the total risk by summing the product of the likelihood of the security event and the expected consequences in that mode.

After identifying the most significant risks on the system, the next step is to determine what mitigation actions or security measures might be desirable to reduce risk, and where assessment techniques such as facility or pipeline security assessments would be of the most value in identifying potential risk-threatening issues. The risk control and mitigation process involves:

- Identification of risk control options that lower the likelihood of a pipeline system incident, reduce the consequences, or both;
- A systematic evaluation and comparison of those options; and
- Selection and implementation of the optimum strategy for risk control.

SVA also helps to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote. A tiered, risk-based approach is the most effective way to evaluate, identify, and prioritize potential targets. There are a number of methods that can be employed to conduct a SVA and identify risk control activities. Section 5 (Part III) provides guidance for developing and implementing a useful SVA approach.

Develop Security Plan. Using the output of the SVA, a plan is developed and maintained to address the most significant risks and assess the security of the pipeline system. This plan should include the mitigation risk control actions, as well as security assessment activities, e.g., inspections and traffic and personnel control. Section 5 (Part III) provides a description of the various risk control options available, guidance to assist Owner/Operators in selecting a security assessment method, establishing a schedule for periodic security assessments, and employment of security mitigations.

Employ Security Mitigations. In this element, the security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that might lead to pipeline system failures are controlled. As noted previously, a SVA may identify other risks that should be addressed. For example, if pipeline exposure was identified as a significant security risk in a particular area, the operator may elect to conduct additional patrolling, increase public communication, and/or actively engage local police agencies to reduce the likelihood of the security threat to the pipeline. A menu of risk control activities and mitigation options to address common security risks is provided in Section 6.

Update, Integrate, and Review Data. After the initial security assessments have been performed, the operator has improved and updated information about the security of the pipeline system. This information should be retained and added to the database of information used to support future SVAs and security evaluations. Furthermore, as the system continues to operate, additional surveillance and other data are collected, thus expanding and improving the historical database and experience levels.

Reassess Risk. SVAs should be performed periodically to factor in recent operating data or threat intelligence; consider changes to the pipeline system design, e.g., new IT systems and new pipeline segments or facilities; and to analyze the impact of any external changes that may have occurred since the last SVA, e.g., adjacent facilities and changes in traffic flow. The results of security assessments, such as inspections and drills, should also be factored into future SVAs to assure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The security plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated SVA results should also be used to support scheduling of future security assessments.

Audit Plan. The operator should collect information and periodically evaluate the success of its security assessment techniques and other mitigation risk control activities. The operator should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions. Section 7 provides guidance for developing performance measures to evaluate plan effectiveness, and guidance for conducting audits and drills of security plans.

Managing Change. Pipeline systems and the environment in which they operate are never static. A systematic process should be used to ensure that changes to the pipeline system are evaluated for their potential risk impacts prior to implementing the changes, and to ensure that changes in the environment in which the pipeline operates are evaluated. Such an evaluation also includes communicating the planned or known changes to all concerned prior to implementation or when first identified. After these changes have been made, they should be incorporated, as appropriate, into future SVAs to be sure the SVA process addresses the system as it is configured.

As this final element indicates, managing pipeline security is not a one-time process. As implied by the loop in the lower portion of Figure 4.1, a security plan involves a continuous cycle of monitoring pipeline conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs must be periodically updated and revised to reflect current pipeline conditions so Owner/Operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

Once a SVA method has been developed, the operator will organize and incorporate the information known about the pipeline system into the SVA process. When assessing the risks of a group of assets operated by a single company, those assets may be divided into distinct segments to enable the comparison of the relative risks of those segments across the company. This will enable the operator to allocate resources using risk-based prioritization to reduce overall risk in the most effective manner. Similarly, when assessing the risks of a single large asset such as a cross-country pipeline, the system may be divided into geographical segments to compare the risks of respective pipeline segments to determine how to allocate resources across the pipeline system. The operator would decide how long the segments will be and the logical location of boundaries between segments. Factors that drive these decisions include:

- Scope of the SVA; that is, which assets are included/excluded from the assessment.
- Equipment boundaries such as pump stations or block valves.
- Geographical boundaries such as state lines or rivers.
- Desired minimum/maximum length of any one segment, e.g., foot-by-foot, mile-by-mile.
- How system databases are set up and organized; this is important since data will be transferred from one or several databases into the SVA method.
- Operation changes, e.g., region, product, and volumes.
- Population density changes.
- The presence of environmentally sensitive or population sensitive areas, e.g., HCA’s, schools, waterways, third party facilities, and government installations.

After completing the SVA for each pipeline segment, the results can be used to analyze risk factors in many different ways. First, the individual segments can be ranked: by total risk level, by individual likelihood category, or by consequence level. A varying risk profile along the pipeline system can be created, highlighting areas susceptible to particular risks. These rankings can be used by an operator to focus attention on potential high-risk areas. A number of comparative analyses can be performed, such as:

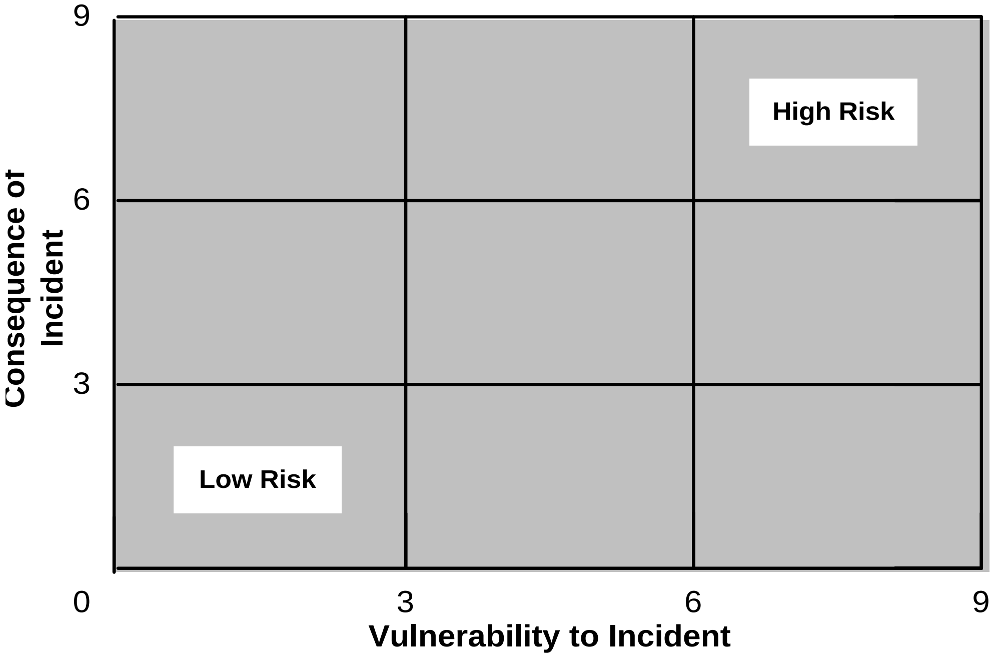
- Comparison of risks from different security risks along the pipeline.
- Comparison of pipeline risks by geographic region.
- Comparison of different pipeline system risks within a company.
- Comparison of a pipeline risk profile with a predefined standard, such as compliance with regulatory directives or an operator defined standard.

4.0 SVA Example

4.1 SVA Matrix

Several companies use the matrix approach in performing a SVA of facilities. One such matrix employed is where the Vulnerability to Incident is plotted against the Consequence of Incident with both factors being given numerical values. In such an example, the higher the Vulnerability and/or the Consequence, the higher the SVA value which leads to increased security measures being employed at the facility. Figure 4.1 shows a simplified SVA matrix using these variables.

Figure 4.1
Simplified Risk Assessment Matrix



In developing the matrix, the Vulnerability to Incident items are developed and assigned numerical values with the weight of each value not necessarily the same but being dependent on the importance of the item. For example, the following items and numerical values might be considered:

Item	Detail	Value
Location	Rural	1
	Small Town/Village	2
	Urban Location	3
Product Characteristic	Heavy Oils/Asphalt	0
	Distillate	1
	Gasoline	2
	HVL	3
	Highly Toxic	4
Size of release	Less than X barrels	1
	X to 10X barrels	2
	More than 10X barrels	3

In this example, each item would be evaluated and the values would be totaled with the total value plotted on the matrix as the Vulnerability to Incident.

In further developing the matrix, the Consequence of Incident items would also be developed and assigned numerical values, and as before, the weight of each value would not necessarily be the same but dependent on the importance of the item. For example, the following items and numerical values might be considered:

Item	Detail	Value
Personnel Exposure	None	0
	Minimal Exposure	2
	Large Exposure	4
Environmental Exposure	None	0
	Land and/or Air	1
	Minor Waterway	2
	Major Waterway	3
Business Interruption	None	0
	Less than $X	1
	$X to $10X	2
	More than $10X	3
Supply disruption	None	0
	Less than X days	1
	X days to 10X days	2
	More than 10X days	3

Likewise, each item would be evaluated and the values would be totaled with the total value plotted on the matrix as the Consequence of Incident. Where the two values cross on the matrix is the overall numerical SVA value for a particular facility or pipeline segment. In conducting such an assessment for a number of facilities or segments, they could thus be ranked in comparison to each other and prioritized.

4.2 Validation and Prioritization of Risks

Independent of the process used to perform a SVA, the operator must perform a quality control review of the output to ensure that the methodology has produced results consistent with the objectives of the assessment. This can be achieved through a review of the SVA data and results by a knowledgeable and experienced individual or, preferably, by a cross-functional team consisting of a mixture of personnel with skill sets and experience-based knowledge of the pipeline systems or segments being reviewed. This validation of the SVA method should be performed to ensure that the method has produced results that make sense to the operator. If the results are not consistent with the operator's understanding and expectations of system operation and risks, the operator should explore the reasons why and make appropriate adjustments to the method, assumptions, or data.

Some additional criteria to evaluate the quality of a SVA are:

- Are the data and analyses handled competently and consistently throughout the system? (Can the logic be readily followed?)
- Is the assessment presented in an organized and useful manner?
- Are all assumptions identified and explained?
- Are major uncertainties identified, e.g., due to missing data?
- Do evidence, analysis, and argument adequately support conclusions and recommendations?

Once the SVA method and process has been validated, the operator has the necessary information to prioritize risks. To determine what risk mitigation actions to take, the operator considers which pipeline systems (or segments of systems) have the highest risks and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

The SVA process or SVA methods can be applied at different stages of the overall security assessment and evaluation process. For example, it can be applied to help select, prioritize, and schedule the locations for security assessments. It can also be performed after the security assessment is completed to conduct a more comprehensive SVA that incorporates more accurate information about the facility or pipeline segment.

4.3 Risk Control and Mitigation

SVA methods are also important tools to help Owner/Operators make cost effective and sound decisions to control security risks on their systems. Once a potential risk has been identified, SVA methods can be used to estimate the expected risk reduction or benefits that will be achieved. The process typically mimics an operator's current workflow when proposing capital or maintenance projects. When combined with project cost estimates, the SVA methods can compare the cost/benefit results of several proposed projects to help a company determine if the project will be the best solution for the time period under consideration. Potential capital and maintenance improvement activities can be prioritized to support management decision-making. This section provides an overview of this process.

After the results of the SVA are available, the next step is to examine the most significant risks on the system, as well as other opportunities to more efficiently control risks and determine what mitigation actions might be desirable. The risk control and mitigation process involves:

- Identification of risk control options that lower the likelihood of a pipeline system security related event, reduce the consequences, or both, i.e., mitigation activities;
- A systematic evaluation and comparison of those options to quantify the risk reduction impact of the proposed project;
- Selection and implementation of the optimum strategy for risk control.

Typically there are many ways to address a particular risk. For example, improvements or modifications can be made to the system hardware or equipment configuration, operation and maintenance practices, assessment practices, personnel training, pipeline control and monitoring methods, emergency response, and interface with the public and other external organizations. Part III, Section 6 of this guideline provides a discussion of risk control options that are frequently used to reduce pipeline security risks. In order to find the optimum approach to risk control, it is important that a variety of options, and perhaps combinations of activities, be considered, rather than just taking the first idea that is proposed or doing what has always been standard practice. This allows management to consider innovative solutions and perhaps new technologies that may be more effective in addressing risk. Many Owner/Operators have found that a structured process for identifying risk control options and encouraging innovative solutions has produced unique insights and contributed to more effective risk management.

After identifying the risk control options available, the next step is to evaluate and compare the effectiveness of the different alternatives. This evaluation and comparison is often performed at more than one level. For example, a company may desire to select the best approach among several options to address a specific risk. However, on a broader scale, the company may need to evaluate the relative benefits of a number of risk-reduction projects and activities as part of its budget process. In each case, the basis for comparison and ranking should consider both the magnitude of risk reduction benefits expected as well as the resources expended. Many Owner/Operators use a benefit-to-cost ratio where the benefit is the expected risk reduction to evaluate and rank potential risk control projects. This can provide a simple, easy-to-understand metric that allows projects with diverse benefits to be compared.

When conducting a ranking of projects based on a benefit-to-cost approach, a comprehensive evaluation and comparison process should also include a review of the pipeline system risks to be sure that relatively high risks are not overlooked simply because the risk control projects proposed don't have a high benefit-to-cost ratio. This may signal the need to consider other risk control options.[2] The process should also consider the amount of risk reduction being achieved to be sure the most effective projects are being proposed. There are many other practical factors that are typically considered when evaluating and prioritizing activities. These can include:

- Uncertainties in both the risk reduction and cost estimates.
- Technological value of a particular option, e.g., employing a new security camera.
- Human resource and equipment constraints.
- Logistical and implementation issues, e.g., delay in ability of vendor to supply necessary equipment.
- Concerns of government organizations and other external constituencies.

Owner/Operators have found that a structured and consistent methodology for evaluating the relative benefits of different options or activities has led to more effective use of resources in their organizations. There are a number of ranking and prioritization tools and approaches that are employed to provide structure and consistency to this evaluation process. These include expert panel reviews, SVA methods, priority matrices, and multi-attribute utility models. Whatever approach is used, it is important that the process consistently uses defined inputs, specific analytical steps, established and clear decision criteria, and documented output.

The security assessment and risk mitigation decisions that are produced by this process are used to develop the security plan, or modify the existing plan, as described in Section 5.

4.4 Periodic Assessment

SVA is not a one-time event and there must be an established process to repeat the SVA at some operator-defined frequency.

The process and methods used to perform the SVA should be reviewed periodically to ensure that the process is appropriately rigorous and yields results consistent with the objectives of the operator's pipeline security plan. The method used to perform the SVA will be adjusted and improved with each use as the operator incorporates more detailed and current information about the pipeline system.

The pipeline operator learns more about the risks of the pipeline system with each SVA. Using this knowledge, the operator must develop a schedule for re-assessment of each pipeline facility or segment.

[2] Although summarized in a linear fashion for this guideline, the risk control and mitigation process, like the risk assessment process, can be highly iterative in nature.

5.0 Security Plan Development and Implementation

5.1 Security Plan

The security plan is developed as a result of the data gathering and SVA (see Part I, Section 5 and Part III, Section 4) and consists of the employment of security mitigation activities including a schedule for these activities to be implemented. To develop the security plan, the most appropriate assessment requirements must be identified for each asset, and the work must be prioritized and scheduled dependent on the ranking of the asset. Assessment of each asset or pipeline segment could be accomplished by experts visiting the facilities, review of an existing database, meetings with operations and maintenance personnel, or a combination of these techniques. The initial SVA will provide guidance to determine what factors to consider (see Part III, Section 4). This section provides information about assessment techniques and security mitigations. The security plan, once developed, tells the operator what to assess, how to assess, and when to assess as well as the security measures to consider in mitigating risks.

The initial security plan will include a list of mitigation activities. These are actions, identified during the initial SVA, that will improve the pipeline security and/or reduce risk, and do not require additional assessment data to determine if they are justified. These actions could include actions that prevent security related events, provide detection of security related events, or minimize the consequences.

The operator should consider the following factors in developing the security plan:

- Security risks that can adversely affect pipeline operations.
- Various security assessment techniques typically used for pipeline systems.
- Methodology for evaluation of assessment data.
- Pipeline security measures, and other mitigation activities that can improve pipeline security.

5.2 Pipeline Security Risks

Pipeline security risks are *possible* deviations from the norm and require an assessment of the threats and vulnerabilities related to and as they pertain to the various risks which a pipeline system is exposed. A thorough understanding of pipeline security risks and under what conditions that they occur is essential in order to select the most appropriate assessment technique(s) and security measures.

5.3 Pipeline System Assessments

This is an overview of the elements that should be considered in a pipeline system SVA. These can be applied to pipeline segments and/or facilities. The listed items should not be considered as all inclusive as there could be other items that are unique to the pipeline segment or facility. In general, a SVA should include as applicable the following elements:

- Existing SVA and prevention strategies

- Existing security policies and practices
- Existing security measures employed such as vehicle and personnel access control, perimeter protection, intrusion detection, security assignments, and backup systems
- Collaboration with other company units and with local, state, and federal police agencies, LEPC's, etc.
- Accessibility and visibility of segment or facility
- Package and material delivery procedures
- Mail handling procedures
- Vehicle routing and parking
- Company patrol practices and police agencies oversight
- Incident reporting systems and investigation strategies
- Employee training and security awareness
- Emergency response and crisis management
- Infrastructure security including those related to utilities and communications
- Employee security measures including hiring practices
- Workplace security practices and response to security related issues
- After hours and week-end staffing and oversight
- Security of forms, papers, tools, and equipment
- Information, computer, and network security including SCADA systems
- Physical assessment of the surrounding area and identification of those facilities which would increase or decrease the risk, e.g., government facilities and police agencies
- Assessment of facility from a target perspective, e.g., visibility, size, consequence
- Shut-down and evacuation plans
- Interviews with company personnel familiar with the physical assets
- Review of information being provided to the public via mails, advertisements, web sites, etc

5.4 Determination of Assessment Interval/Frequency

5.4.1 Initial Assessments

In deciding if and when to conduct an initial security assessment, the operator should consider the results of its SVA and the type or types of risks suspected. The SVA should include a prioritization of pipeline segments and facilities that should be followed in scheduling initial security assessments.

5.4.2 Setting Assessment Intervals

New security related issues including those from external sources as well as internal changes could necessitate repeated assessments. Assessments could be prompted by information flow from government agencies regarding new or different risks or threats directed at the company or pipeline industry. The assessments could be time dependent, and they should be scheduled before they reach a condition that can potentially have a negative impact to the operability and integrity of the pipeline system.

5.5 Assessment Methods

An on-site assessment is a method to validate the security of a pipeline segment or facility. When on-site assessments and other methods are selected to verify the security of a pipeline segment or facility, the method selected should be performed at an interval sufficient to eliminate or prove the absence of critical security risks. On-site assessments are typically conducted by outside security experts or company employees who have received training in security related issues.

5.6 Methodology for Evaluation of Assessment Data

Due to the uniqueness and complexity of assessment data, an inspector typically evaluates the information and provides the pipeline operator with the results and recommendations. It is then the responsibility of the operator to evaluate the results and develop a pipeline security response. The following guidelines will assist the operator in developing a strategy for evaluation of security issues identified by a security assessment.

An operator should develop an action plan to address pipeline security concerns identified during the evaluation of the security assessment data. If a condition exists on the pipeline system that presents a concern, the operator should initiate actions in order to remove the identified risk or alleviate the condition. Mitigation action is based on regulatory requirements, company guidelines, and assessment of risk.

Mitigation action for the above conditions should be based on security assessment data analysis. Temporary mitigation action(s) should be initiated as soon as possible after receipt of the preliminary assessment report and should remain in place until the security risk can be further assessed.

The following items, for example, should be evaluated and mitigated, if necessary, within a specified time frame after receipt of the final assessment report:

- Vehicle access and personnel control
- Perimeter security breaks
- Inadequate lighting in critical areas
- Security response procedures
- Mail delivery and package handling procedures

6.0 Mitigation Options

An operator’s pipeline security plan will include applicable mitigation activities to prevent, detect, and minimize the consequences of security related events. Mitigation actions can also be identified during normal pipeline operation, during the initial SVA, during implementation of the security plan, or during subsequent assessments.

The mitigation activities and risk control measures presented in this section include information on:

- Management Issues
- Security Guidelines
- Collaboration With Others
- Incident Reporting and Analysis
- Employee and Contractor Training and Security Awareness
- Investigations
- Emergency Response and Crisis Management
- Periodic Reassessment
- Physical Security
- Cyber Security

6.1 Management Issues

Company security management should be assigned to a senior level position within the company. This responsibility can be included with the responsibilities of another position. Security responsibility should also be assigned to personnel for specific company facilities and pipeline segments. The persons assuming the security roles can perform a number of important management functions such as promulgating guidelines, establishing relationships with law enforcement agencies and surrounding communities to address security concerns, developing and managing incident reporting systems, boosting employees’ security awareness, referring security breaches for investigation, coordinating emergency response, and periodically directing the reassessment of the security plan.

6.2 Security Guidelines

The introduction of security planning and countermeasures must be accompanied by a strong awareness-training program. It is extremely important to create an awareness of security and inform the users of the procedures they need to maintain for adequate safeguards. One cause of security problems is a lack of management or employee concern. Security is as much a managerial problem as it is a technology problem. To guard against costly and embarrassing breaches of security, management must clearly establish and enforce security guidelines, plans, and procedures. Make sure that the company security guidelines are widely disseminated and discussed. The guidelines should be reinforced with internal education, training for all new hires, ongoing workshops, and review sessions. Make sure that all company personnel clearly understand the guidelines and the language. Evaluation of company security guidelines should include the following items:

- Do the guidelines comply with the law and with the duties to third parties
- Do the guidelines compromise the interest and safety of the employees, the company, or third parties
- Are the guidelines practical, workable, and likely to be enforced
- Do the guidelines address all of the different forms of communication and record keeping within the organization
- Have the guidelines been properly presented and agreed by all concerned

A security plan works best when employees see it as an important part of the company's mission. Employees are more likely to see security as a company priority if management visibly supports security efforts. Among the best ways to demonstrate that support is to include security as one of management's core values and to promulgate official company guidelines regarding security. Guidelines that should be in place and communicated include:

- Vehicle and personnel access control
- Workplace and personnel security
- Physical assets security
- Pre-employment screening
- Information protection
- Reporting of incidents
- Response to risks
- Control center security
- Communications security
- Computer hardware and software security
- Handling of materials
- Contingency and back-up plans
- Crisis management

6.3 Collaboration With Others

The company as well as each of its facilities should establish partnerships with local, state, and federal law enforcement and other public safety agencies. Through such a network, information can be gained regarding risks, dangerous trends, and successful and unsuccessful security measures. It may also be possible to obtain threat and other information from regulatory agencies, LEPC's, community advisory panels, industry associations, mutual aid groups, state chemical associations, and ISAC's. Internal collaboration can also be important. By clarifying relationships and procedures with other management functions, e.g., employee safety and health, legal, and human resources, information channels can open within the company and provide a more coordinated response to security related incidents.

6.4 Incident Reporting and Analysis

Records should be kept of security related incidents. Such records will allow the detection of trends and piecing together facts that can lead to successful investigations and conclusions of security risks. These data can also be shared with peer groups, regulatory agencies, and police agencies for improved evaluation and reporting of security incidents and trends in the industry. Incident data will only be available for analysis if incidents are reported and recorded. Every employee should be encouraged to report security related incidents and events no matter how small or trivial.

6.5 Investigations

Appropriate company and facility personnel should investigate suspicious incidents and security breaches immediately. Facility management should refer such incidents to company security management. Any suspected illegal activity should be reported for referral to law enforcement if appropriate. The following are some examples of security incidents that might warrant investigation:

- Doors or fences including gates not secured with indications of illegal entry
- Unauthorized access by individuals in restricted areas
- Foreign vehicles in areas along the perimeter fencing, near buildings, electrical substations, or security gates
- Individuals requesting information about the facility or company with no apparent need to know the information otherwise
- Unexplained loss of materials or product
- Cyber threats against control or computer systems
- Suspicious packages left at or suspect mail directed to the facility
- Threats directed at a facility
- Misrepresentations on ROW inquiries

6.6 Employee and Contractor Training and Security Awareness

Employees and contractors can serve as the eyes and ears of a company-wide security effort. Employees, contractors, landowners, and customers see and hear most of what occurs around company facilities and pipelines and are in a good position to notice when something or someone out of the ordinary and acting suspicious might be present. Training and awareness programs can transform employees and contractors into a natural surveillance system. Developing security awareness can also reinforce security practices such as the following:

- Securing doors and perimeter fencing
- Looking for and reporting items out of the ordinary
- Reporting strange vehicles and personnel
- Security of controls and computer systems
- Mail, package, and material receipt procedures
- Maintaining security systems such as lighting and intrusion alarms
- Reporting security related events and incidents
- Prohibiting discussions with outsiders concerning company matters

Employees also have a wealth of experience and knowledge that should be garnered concerning security issues at particular facilities and pipelines. Managers can also reinforce personnel training in security practices through mailings and security tips posted on company web sites.

6.7 Emergency Response and Crisis Management

Proper crisis management could prevent a security related event from becoming a major incident. In the petroleum industry, including liquid pipelines, emergency response and crisis management are compounded by the nature of the products handled, however and because of this, the majority of companies are better equipped than most to deal with crisis such as those brought on by security related events. As such, companies have pre-existing crisis management and emergency response procedures in place, which should be modified to include security management and emergency response to security related events. Modifications to existing procedures to include pipeline security events could include items such as the potential legal issues and the possibility of the site being declared a crime scene as well as the potential for hazardous materials being present during and after the event.

6.8 Physical Security

The term “physical security” refers to those measures that are designed to detect and prevent physical attacks against company and facility employees, property, and information. Elements of a physical security plan could include access control, perimeter protection, and security guards.

6.8.1 Access Control

The term “access control” generally refers to physical or behavioral measures for managing the passage of personnel and vehicles into, out of, and within a facility including buildings. Access control strives to exert enough control to protect the facility while still allowing employees and visitors enough freedom of movement to work effectively. The appropriate level of access control varies significantly from facility to facility. It depends on the number of employees, the hazards present, level of personnel and vehicular traffic as applicable, degree to which the facility is controversial, attractiveness of the facility as a target, proximity of the facility to populated areas, and other factors. The following are some measures that should be considered for the purpose of controlling access into, within, and out of a facility. The implementation of these or other measures must be weighed on an individual location cost/benefit basis based on identified risks:

- Post “No Trespassing” and “Authorized Access Only” signs along with signs stating vehicles and visitors are subject to search
- To the extent feasible, employ natural surveillance by arranging space so unescorted visitors and non-company vehicles can be noticed easily
- Install appropriate and secure locks on all asset features which should be secured and control access to the keys or combinations when such locks are used
- Require visitor sign-in logs, verify visitors are expected, and provide escorts

- Institute and maintain vehicle traffic control entering the facility and while in the facility—establish minimum spacing between vehicles and buildings and other assets pending verification of the necessity and intent of the vehicles presence
- Require visitor parking off-site or at some minimum distance from the facility
- Install appropriate penetration resistant openings to the facility, e.g., doors, windows, hinges, gates
- Institute a system of employee and contractor photo ID badges—train employees to question persons who are not wearing badges
- Install an electronic access control system that requires the use of key cards or number pads at main entrances and on appropriate doors and provides an audit trail of ingress and egress—consider electronic access control to motor control centers, switchgear rooms, server rooms, telecommunication rooms, and control centers
- Install a closed-circuit television system to monitor key areas of the facility—where appropriate, install motion sensors
- Institute a system of parcel and mail inspections or consider routing of parcels and mail through off-site facilities
- Require the use of property passes to bring or remove property from the facility

6.8.2 Perimeter Protection

Controlling the movement of people and vehicles within a facility is important, but it is far better to stop intruders at the edge of the facility's property before they reach vital assets and operational areas. Perimeter protection includes where appropriate:

- Fences and exterior walls that make it difficult for intruders to enter the facility
- Bollards and trenches that prevent vehicles from driving into the facility at points other than intended entrances
- Vehicle gates with retractable barriers
- Personnel gates and turnstiles
- Setbacks and clear zones which make it difficult for visitors to approach the facility unnoticed
- Lighting that makes it possible for employees and others to observe and identify visitors before they are in the facility
- Intruder detection systems along the perimeter such as infrared detection and light or sonic beam technology
- Video cameras and audio systems at the entrances to identify visitors before they are in the facility
- Regular patrols with altered patterns that are not recognizable

6.8.3 Security Guards

Security guards can provide a range of useful security services such as patrolling a facility to look for intruders or irregularities, staffing site entrances to check ID's and vehicle manifests, inspection of vehicles, maintaining entry and exit logs, handing out security papers and passes, reminding employees and contractors of security and safety policies, and assisting in crisis management. If it is deemed appropriate for a facility to have security guards, it must be determined whether the guards will patrol the facility or remain at fixed posts; whether they will be contract or in-house guards; and what training and licensing they will have and if they will be armed. "Post Orders" should be developed which are written directions stating what the security guards are required to do on the job as well as the authority limitations and reporting directions that they will have. Security guards, when they are employed, should pass a background screening process, and they should be certified to perform the job functions that will be required of them. Some companies may elect to arrange for an on-call security service for assistance during certain security related events.

6.9 Cyber Security

As organizations increasingly rely on networked computer systems, they lose the control of information processing that was present in the traditional data center. As the control of computing information moves to the desktop and remote sites via networking, it is essential that companies understand the risks to this and create a security plan that will meet this challenge. Computer systems have unique security issues that must be understood for effective implementation of security measures. These issues include:

- Hardware Accessibility
- Software
- Data Communications
- SCADA Systems
- Networking
- Disaster Recovery

Most companies with computer systems have existing computer security systems in place, and unlike physical asset security, computer security has been an issue for many years. As such, most companies may find or conclude that they have systems in place that are adequate to protect their computer systems, and these guidelines will be no more than a review of their practices.

6.9.1 Hardware Accessibility

Several approaches need to be considered in order to provide the necessary security for the physical hardware of computer systems. Locks are available to prevent access to servers, drives, and processing units. Planning and diligent processing are the keys to securing computer systems and the information they process. Companies should maintain accurate and current inventories of their computer system hardware. Guidelines are also needed to provide for the internal movement of computer systems and their parts as well as the security of the systems in their assigned locations.

6.9.2 Software

Most security intrusions to a computer system's software are either by introducing a virus to the system or by a security breach of the computer system allowing an outsider into the system to modify or interrupt the commands of the system or to gain information. Software viruses have left a number of companies sadder but the wiser. A virus can change data within a file, erase a disc, or direct a computer to perform system-slowing calculations. Viruses may be spread by downloading programs off a bulletin board, sharing floppy diskettes, or communicating with an infected computer through a network. Anti-virus products are a necessity for the detection, eradication, and prevention of viruses. The company's computer security guidelines should define permissible software sources, bulletin board use, and the types of applications that can be run on company computers. These guidelines should also provide standards for testing unknown applications and limit diskette sharing. Network security including intrusion prevention is discussed in section 6.9.5.

6.9.3 Data Security and Integrity

Companies are exposed on a continuing basis to piracy of sensitive information through the interception of communications data. Banks, financial institutions, and the government have been using encryption technology to protect communications data for years, but it was not until recently that the technology was made available to others. It is now imperative for companies to protect themselves from the risks of misuse, abuse, or theft of their sensitive information. One type of protection that can be used for communication of sensitive information is cryptography (encryption). The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a new devised algorithm to start communicating with others. The concept of the key is analogous to the combination for a combination lock.

6.9.4 SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems are used for the remote control and monitoring of pipeline facilities. The remote control and monitoring is typically done from a centralized control center that is typically manned on a 24/7 basis. The systems are typically computer based and most have a back-up computer and other redundant features, e.g., multiple man-machine interfaces. The centralized system typically communicates with the field or remote devices through a dedicated communications network such as land telephone lines, satellite system, microwave towers, or directional radio frequencies with most systems having redundant communication features. Security measures that should be employed to protect SCADA systems include:

- Access control to the control center
- Integrity of communication systems
- Verification of transmitted signals
- Status of field devices
- Feedback of control signals
- Database protection
- Back-up plans

6.9.5 Networking

Today's company networks are complex and diverse. They connect mainframes, mini computers, PC's, LAN's, and peripherals over ever widening geographic boundaries. This diversity, both technically and geographically, means that devising an effective company wide network security plan involves adapting security techniques and procedures from the various systems which are available and fitting these measures to the company's system. Considerations for network security should include:

- Ensure that any message sent arrives at its intended destination
- Ensure that any message received was in fact the one that was sent, i.e., nothing was added or deleted
- Control access to the company's network and all of its related parts, e.g., terminals, servers, switches, modems, gateways, routers, and printers
- Protect information in-transit from being seen, altered, or intercepted and removed by an unauthorized person or device
- Any breaches of security that occur on the network should be revealed, reported, and receive the appropriate response
- A recovery plan should both the primary and backup communications fail
- Identification of those involved in the security process
- Identification of resources being protected, i.e., identify the assets
- Identification of the possible threats, i.e., SVA
- Ranking and prioritization on the importance of each of the identified resources

The National Institute for Standards and Technology (NIST) developed a listing for what they refer to as Minimal Security Functional Requirements for Multi-Operational Systems. The major functions are listed as:

- Identification and authentication—Use of a password or some other form of identification to screen users and check their authorization with such being changed on a periodic basis
- Access Control—Keeping authorized and unauthorized users from gaining access to information and data they should not see, e.g., firewalls
- Accountability—Links all of the activities on the network to the users identity
- Audit Trails—Means by which to determine whether a security breach has occurred and what if anything was lost or tampered with
- Object Reuse—Securing resources for the use of multiple users
- Accuracy—Guarding against errors and unauthorized modifications
- Reliability—Protection against the monopolization by any user or users
- Data Exchange—Securing transmissions over communication channels

Making sure the company security measures work is imperative to successfully securing the data and users. The company has to know who is doing what with the system and be able to audit this information. The components of a good audit system will include:

- A log of all attempts to gain access to the system

- A chronological log of all network activity
- Flags to identify unusual activity and variations from established procedures

6.9.6 Disaster Recovery

The primary objective of disaster recovery planning is for the continuity of business activities. There is special consideration for networked systems because the equipment is widely dispersed and many people are involved. System users should also be encouraged to protect themselves by developing and maintaining their own fallback procedures.

7.0 Plan Evaluation

The intent of this section is to provide system Owner/Operators with a methodology that can be used to evaluate the effectiveness of security management. The goal of the operator of any pipeline system is to operate the pipeline in such a way that there are no adverse effects on employees, the environment, the public or its customers as a result of their actions. Evaluations need to be performed on a periodic basis to review the effectiveness of the operator's security plan. In the most basic sense, a plan evaluation should help an operator answer the following questions:

- Did you do what you said you were going to do?
- Was what you said you were going to do effective in addressing the issues of security in your pipeline system?

7.1 Performance Measures

The operator should collect performance information and periodically evaluate the effectiveness of its security assessment methods, and its mitigation risk control activities including response.

7.2 Audits

From time to time, Owner/Operators should audit their security plan to determine the effectiveness of the plan and to ensure that the plan is being conducted according to the operator’s security plan and in compliance with all applicable regulations. Audits may be performed by internal staff or outside consultants. While the audit will be based on local conditions, below are a series of questions that each operator can use as a starting point in developing a company-specific audit program:

- Are there written guidelines for security management?
- Are there written procedures for tasks relating to security management?
- Are activities being performed as outlined in the operator’s plan documentation?
- Is someone assigned responsibility for each subject area?
- Are appropriate references available to those who need them?
- Are the people who do the work trained in the subject area?
- Are qualified people used when required?
- Are activities being performed using an appropriate security management framework as outlined in this guideline?
- Are all required activities documented by the operator?
- Are action items followed-up?
- Is there a formal review of the rationale used for developing the risk criteria used by the pipeline operator?
- Are there established criteria for responding to security events?
- Are criteria established for the activities stated above for terminals, pump stations, associated piping, and pipeline segments?

7.3 Drills

Drills allow for a prepared and organized response to a variety of security related events. Their essential purpose is to demonstrate knowledge and understanding of the security management plan as well as a readiness to respond to security related events. They should be simple, flexible, and robust and should provide for:

- A scripted event indicative of a security related event
- Emergency management and reporting procedures
- Availability of essential resources and response actions
- Review of lessons learned, i.e., critique of drill
- Modifications to plan

A security drill could also be included as a part of other drills. For example, the cause of a product release could be a security incident with consideration given for the legal implications and personnel hazards associated with the incident.

8.0 Managing Change in a Security Plan

Once a pipeline security plan is established, it is critical that the pipeline operator keeps the plan current. Changes to the pipeline system made by the operating company and changes affecting the pipeline system made by others could affect the priorities of the security plan and the risk control measures employed. To ensure continued validity of the plan, Owner/Operators must:

- Recognize changes before or shortly after they occur
- Ensure that those changes do not unnecessarily increase risks
- Update the affected portion(s) of the pipeline security plan

Owner/Operators with an existing MOC plan should verify that the types of changes mentioned in this section are included in their MOC plan. For other Owner/Operators, a system should be established to recognize and manage changes relevant to their pipeline security plan.

8.1 Recognizing Changes That Affect the Security Plan

To keep the pipeline security plan current, the operator should identify the ways a pipeline system may be modified that could impact any of the risk factors identified in the pipeline security plan. Examples of such changes are:

- Adding, deleting, or otherwise modifying the pipeline segments or facilities
- Changes in the fluid transported and/or its operating conditions in the pipe that may also affect the risk prioritization and any mitigation measures employed
- Restarting equipment or systems that have been out of service for an extended time and/or systems that have not been maintained
- Changes to existing procedures, or addition of new procedures
- Changes along the right-of-way, such as changes in land use
- Regulatory changes

The operator is responsible for recognizing these changes and ensuring that the changes are appropriately reviewed.

8.2 Updating the Pipeline Security Plan

A change may impact any or the entire pipeline security plan. Sections 5 through 8 of this section address elements of the plan that may be impacted by a change. As part of managing a change, the operator should evaluate security plan issues such as:

- Has the potential impacts or affected impact zones been altered? (Part I, Section 5)
- Should data be added, deleted, or modified? (Part I, Section 5)
- Does this change impact data that was input or assumptions that were made during the SVA? (Section 5)
- Does this change affect mitigation plans? (Section 6)
- Does this change impact any performance indication or auditing criteria? (Section 7)

- Does this change impact the security plan for pipeline segments or facilities? (Section 8)

Any change that affects the pipeline security plan should be documented. Affected parts of the pipeline security plan should be modified as necessary to reflect the change.

Part III
Appendix A

PIPELINE SECURITY CONDITIONS AND RESPONSE MEASURES

Note: The security conditions describe a progressive level of protective measures that should be implemented in response to the possibility of a terrorist threat or to a terrorist threat directed at pipeline facilities, assets, and personnel. The purpose of the system is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and company personnel prior to and during a threat crisis. The planning guidance provided in this appendix was developed in cooperation with the U.S. Department of Transportation Office of Pipeline Safety, as well as natural gas transmission and distribution pipeline Owner/Operators.

PIPELINE SECURITY CONTINGENCY PLANNING GUIDANCE

This pipeline security contingency planning guidance was developed by the DOT Office of Intelligence & Security, the Research and Special Programs Administration, Office of Pipeline Safety (OPS), the Department of Energy, state pipeline safety agencies, and pipeline industry representatives. It is intended to ensure that pipeline Owner/Operators are able to discourage attacks and respond quickly and effectively if attacks occur.

In general, pipelines are robust and redundant systems. Most sections of pipeline systems are underground and less vulnerable to attack than aboveground facilities. Most damage to line pipes is relatively easy to repair in a few days. Major disruptions in energy supplies can often be avoided by using interconnections between pipelines to move product around the site of a terrorist attack. Therefore, the industry's security efforts should focus on the portions of pipeline systems that are most critical to public safety and reliability of service, including systems for which interconnections may be very limited.

There is broad agreement between government and industry on how to address security. Consensus guidance on industry security practices recommends that each pipeline operator follow three steps: (1) assess the terrorist threats to its system; (2) assess the vulnerabilities of its system to these threats; and (3) develop and implement security, response, and recovery plans that address potential malevolent acts. Federal and state governments should work with Owner/Operators to verify that adequate plans are in place and to test the effectiveness of their plans through exercises.

This document establishes guidelines for protective measures under specified threat conditions to help pipeline Owner/Operators prepare and implement effective security. The protective measures listed in this document are intended to be applied only to critical facilities, although several of the countermeasures require company-wide actions. It is expected that Owner/Operators will use good judgment in incorporating these measures into their security plans, recognizing that not all countermeasures are appropriate for all types of facilities. Unmanned facilities or small, distributed facilities, for example, may require countermeasures different from those required for manned facilities.

The extent to which a facility is critical depends on three main factors: (1) whether it is a viable terrorist target; (2) how important the facility is to the nation's energy infrastructure; and (3) how likely the facility is to be used as a weapon to harm people. Obviously, some facilities are more critical than others, and many facilities are not critical at all. In addition, individual Owner/Operators can deviate from the protective measures listed below by performing and documenting a vulnerability assessment for a facility to estimate the attractiveness of the facility as a terrorist target in accordance with factors other than those just listed. In such cases, the operator would implement protective measures that are appropriate to the facility's specific vulnerabilities and commensurate with its attractiveness as a terrorist target.

Determining whether a specific pipeline facility is a critical facility may require the operator to do some research. To the extent permitted under anti-trust laws, pipeline Owner/Operators should seek out information from the following sources:

- other Owner/Operators in a shared right of way,
- other utilities in the area of the pipeline operator's critical facilities (whose facilities may be critical, too),
- specific customers (e.g., a military base).

Owner/Operators may be hampered in making determinations about specific critical facilities by the willingness of the other party to share information.

For purposes of security planning, a facility is a critical facility if it meets one or more of the following criteria:

1. A pipeline facility or combination of facilities that may be considered a viable terrorist target and (a) intelligence information indicates that the facility, or facilities like it, is being targeted for attack or (b) a release from the facility has the potential for mass casualties or significant impact on public drinking water affecting a major population center;

2. A facility or a combination of facilities that, if damaged or destroyed, would have a detrimental impact on the reliability or operability of the pipeline system, significantly impairing the operator's ability to serve a large number of customers for an extended period;

3. A facility or combination of facilities that, if damaged or destroyed, would significantly impair the operator's ability to serve installations critical to national defense; or

4. A facility or combination of facilities that, if damaged or destroyed, would so impair other modes of transportation or other critical infrastructures (such as electric power generation, telecommunications or public utility) that it would cause major economic disruption.

Under the Homeland Security Advisory System (HSAS) there are five levels of threat conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green
Guarded = Blue
Elevated = Yellow
High = Orange
Severe = Red.

The higher the threat condition, the greater the risks of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat conditions may be assigned for the entire nation, or they may be set for a particular geographic area or industrial sector.

The following threat conditions and protective measures are cumulative. Each successive level assumes that a facility is already implementing the protective measures associated with the preceding threat conditions, as appropriate. The threat conditions and the protective measures associated with each level represent an increasing risk of terrorist attacks. The levels are as follows:

Low Condition (Green). This condition is declared when there is a low risk of terrorist attack. The following measures under Low Condition (Green) should be maintained indefinitely.

Measure 1. All Owner/Operators should verify the identity of all employees and visitors and control access to critical facilities at all times. Visitors should not be allowed access to critical facilities unless the operator is satisfied as to their identity and the visitor has a legitimate business purpose for their visit. The operator should be aware of any contractors working on a critical facility. Owner/Operators should use company-issued photo ID’s or government-issued photo ID’s.

Measure 2. Ensure that existing security measures such as fencing, locks, camera surveillance, intruder alarms, and lighting are in place and functioning. Identify additional security measures and resources that can enhance the security of critical facilities at the higher threat condition levels (e.g., increased surveillance).

Measure 3. Survey surrounding areas to determine how threats to neighboring facilities (e.g., airports, government buildings, industrial facilities, and other pipelines) could affect the facility.

Measure 4. Develop and implement hardware, software, and communications security for computer-based operational systems.

Measure 5. Establish local, regional, and system wide threat and warning dissemination processes, emergency communications capability, and contact information with law enforcement, including local FBI field offices, first responders, and state and regional pipeline safety representatives. Emergency communications should have redundancy for both hardware and means to contact law enforcement agencies.

Measure 6. Develop potential malevolent acts and security awareness and educate employees on security standards and procedures.

Measure 7. Advise all personnel at each facility to report the presence of unknown personnel, unidentified vehicles, vehicles in an unusual manner, abandoned parcels or packages, and other suspicious activities. Be alert to vehicles parked for an unusual length of time in or near a facility.

Measure 8. Provide security awareness information to land owners along the pipeline right of way (ROW) and to emergency response organizations.

Measure 9. Develop procedures for shutting down and evacuating the facility. Facilities located near critical community assets should be especially vigilant.

Measure 10. Ensure contingency and business continuity plans are current and include a response to terrorist threats.

Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. In addition to the measures listed previously, the following measures should be implemented:

Measure 11. Continue all Low condition measures or introduce those that have not already been implemented.

Measure 12. Ensure that a company response can be mobilized and review facility emergency and security plans and procedures. Test security and emergency communication procedures and protocols.

Measure 13. Inspect perimeter fencing and repair all fence breakdowns. In addition, review all outstanding maintenance and capital project work that could affect the security of facilities.

Measure 14. Review all operations plans, personnel assignments, and logistical requirements that pertain to implementing higher threat conditions.

Elevated Condition (Yellow). An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the measures listed previously, the following measures should be implemented:

Measure 15. Continue all Low Condition and Guarded Condition measures or introduce those that have not already been implemented.

Measure 16. Close and lock gates and barriers except those needed for immediate entry and egress at critical facilities. Inspect perimeter fences regularly. Ensure that other security systems are functioning and available for use.

Measure 17. Limit visitation and confirm that every visitor is expected and has a need to be at a critical facility. All unknown visitors should be escorted while in the facility.

Measure 18. Secure all buildings and storage areas not in regular use. Increase frequency of inspections and patrols within the facility, including the interior of buildings and along the facility perimeter.

Measure 19. Check critical unmanned sites and remote valve sites more frequently than usual for signs of unauthorized entry, suspicious packages, or unusual activities. Increase ROW surveillance in critical areas.

Measure 20. Inspect on a more frequent than usual basis the interior and exterior of all buildings, the area around all aboveground storage tanks, and other vulnerable areas in critical facilities.

Measure 21. Direct that all personal, company, and contractor vehicles at critical facility sites be secured.

Measure 22. Do not open suspicious packages. Inspect all mail and packages coming into a facility. Review the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving mail and packages.

Measure 23. Ensure that a company response can be mobilized as appropriate for the increased security level. Review communications procedures and backup plans with all concerned.

Measure 24. Check to ensure that all telephone, radio, and satellite communication systems are in place and operational.

Measure 25. Increase the frequency of warnings required by lower threat conditions and inform personnel of additional threat information as available. Implement procedures to provide periodic updates on security measures being implemented.

Measure 26. As appropriate, review with facility employees the operations plans, personnel safety, security details, and logistical requirements that pertain to implementing increased security levels.

Measure 27. Confirm the availability of security resources that can assist with round-the-clock coverage of critical facilities.

High Condition (Orange). A High Condition is declared when there is a high risk of terrorist attack. In addition to the measures listed previously, the following measures should be implemented:

Measure 28. Continue all Low, Guarded, and Elevated Condition measures or introduce those that have not already been implemented.

Measure 29. Reduce the number of access points for vehicles and personnel to minimum levels at critical facilities and randomly spot-check the contents of vehicles at the access points.

Measure 30. Limit access to critical facilities to personnel who have a legitimate and verifiable need to enter the facility. Require positive identification of all personnel entering the facility, no exceptions.

Measure 31. Assign personnel at critical facilities to assist with security duties by monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, and reporting to facility management as issues surface.

Measure 32. Consult local authorities about control of public roads and access points that might make the facility more vulnerable to terrorist attack if they were to remain open.

Measure 33. Erect barriers to control direction of traffic flow and protect the affected facility from an attack by a parked or moving vehicle. Company vehicles may be used for this purpose. Implement centralized parking and shuttle bus service where feasible.

Measure 34. Move automobiles and other nonstationary items at least 30 yards from critical facilities, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security measures in place at the facility. Identify areas where explosive devices could be hidden.

Measure 35. Resurvey the surrounding area to determine if activities near a critical facility (e.g., airports, government buildings, industrial facilities, railroads, other pipelines) could create hazards that could affect the facility.

Measure 36. Secure critical facilities round-the-clock using either contract or company personnel; ensure that all security personnel have been briefed on policies governing the use of force and pursuit (as appropriate).

Measure 37. Advise local police agencies that the alert level is at a High Condition (Orange) and advise them of the security measures being employed. Request police agencies to increase the frequency of their patrols of the facility.

Measure 38. Review all outstanding maintenance and capital project work that could affect the security of facilities.

Measure 39. Cancel or delay all nonvital facility work conducted by contractors, or have company personnel continuously monitor the contractors’ work.

Measure 40. Schedule more frequent visits to remote valve sites and other locations that could be affected.

Measure 41. Instruct employees working alone at remote locations or on the ROW to check in periodically.

Measure 42. Check all security systems such as lighting and intruder alarms to ensure that they are functioning. Modify lighting levels, as appropriate, to address changing security needs.

Measure 43. Implement frequent inspection of critical facilities including the exterior and roof of all buildings and parking areas. Increase patrolling at night and ensure that all vulnerable critical points are fully illuminated and secure.

Measure 44. Caution employees not to talk with outsiders concerning their facility or its operations.

Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. This condition represents the highest threat condition and, in all cases, this condition will require rapid response by Federal, state, and local agencies and departments. In addition to the measures listed previously, the following measures should be implemented:

Measure 45. Continue all Low, Guarded, Elevated, and High Condition measures or introduce those that have not already been implemented.

Measure 46. Activate emergency response plans for the critical facilities.

Measure 47. Reduce facility access points to the absolute minimum necessary for continued operation.

Measure 48. Augment security forces to ensure control of the facility and access to the facility and other potential target areas. Establish surveillance points and reporting criteria and procedures.

Measure 49. Inspect all vehicles entering critical facilities including the cargo areas, undercarriage, glove compartments, and other areas where dangerous items could be concealed.

Measure 50. Identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.

Measure 51. Increase security patrol activity at critical facilities to the maximum level sustainable. Increase perimeter patrols and inspections of facility.

Measure 52. Increase the frequency of call-ins from remote locations. Employees should not work alone in such areas.

Measure 53. Shut down affected facilities and operations in accordance with contingency plans unless there is a compelling reason not to, and evaluate the situation before resuming operations.

Measure 54. Request assistance from the local police agencies in securing the facility and access. Cooperate with local police or other authorities if they direct security measures.

Measure 55. Evacuate all nonessential personnel.

Measure 56. Implement business contingency and continuity plans as appropriate.

Part IV—Security Guidelines for Petroleum Products Distribution and Marketing

Part IV—Security Guidelines for Petroleum Distribution and Marketing

1.0 Introduction

These guidelines are intended to assist petroleum product transporters and distributors in assessing security needs. Security measures can increase the safety involved with the transportation of petroleum products. This guidance document outlines some elements of security programs and suggests security practices managers could consider and tailor to their company's specific transportation needs. The purpose of this guidance is to address security considerations during transportation and to reduce the risk of harm posed by the distribution of petroleum products to retail gasoline stations and terminals. These guidelines apply to highway and rail transportation of petroleum products. This guidance does not attempt to provide an all-inclusive list of transportation security considerations, but does provide a basis for measures that could be implemented when evaluating and implementing security measures.

Contractors should have policies and practices in place that are consistent with the petroleum company's security needs. Companies either have, or should consider developing, qualification programs that contractor's must pass prior to becoming an acceptable contractor. The American Chemistry Council's "Transportation Security Guidelines" may serve as a basis for developing alternative guidelines.

This guideline outlines a Security Vulnerability Assessment (SVA) process that a Products Distribution and Marketing operator can use to assess risks and make decisions about risks in operating their operations, and to make progress towards the goal of reducing the risks associated with operations. Part I, Section 4.0 describes the framework for creating a generic security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 4.1. Section 5 describes the basic features of a SVA, using the SVA risk variables at a facility level to provide a risk screening at a facility level, and describes the SVA approach.

2.0 Overview of Segment Operations

The petroleum distribution and marketing sector includes over 1,400 terminals, 7,500 bulk stations, 170,000 gasoline stations and an estimated 35,000 trucks. Each day the petroleum industry transports and purchasers consume over 350 million gallons of gasoline and more than 150 million gallons of diesel and home heating oil. The loss of any one terminal, bulk station, truck or gasoline station would not significantly affect U.S. energy supplies. Further, in the unlikely event of attack, these marketing and distribution facilities have been designed with extensive safety precautions that provide considerable mitigation to criminal or terrorist attack.

Since September 11, a number of companies have recognized that increased security is prudent for their particular facilities, and have been deploying significant resources to develop and implement improved security procedures. They have found that procedures to deter theft and vandalism can also help thwart potential attacks.

For example, terminals implemented card-in procedures that only allow authorized drivers access to the facility in order to provide safeguards against potential acts of terrorism. These cards contain driver information that reveals to terminal personnel who is entering a facility and the product scheduled to be received (e.g., gasoline, diesel, kerosene). Once inside the terminal, the driver uses the card and a personal identification number to start the appropriate product pump. This process prevents unauthorized access to petroleum products at terminals. A number of facilities have taken additional security procedures. For example, some have stationed guards to further protect the facility. These decisions have been based on the risk to the community or to sensitive environmental areas from a potential attack.

Once a truck is loaded with product at a terminal, the driver delivers the product to a retail gasoline station (wholesale and aviation accounts also). The driver, in accordance with Department of Transportation (DOT) rules, must follow designated hazardous material routes where possible. There has been an increase in security training and awareness by transportation personnel. A DOT rule issued on March 25, 2003 now requires most hazardous materials shippers and carriers, including those distributing bulk shipments of most petroleum products, to implement security training and security plans. Security plans must address personnel security, unauthorized access, and en route security. Transportation personnel have also implemented additional security procedures throughout the transportation process.

Underground storage tanks at gasoline stations pose minimal risk, because they are difficult to ignite since vapors in the tanks are too rich to burn. Gasoline stations are also built to the National Fire Protection Association (NFPA) code 30A (Code for Motor Fuel Dispensing Facilities and Repair Garages) that specifies conservative requirements to ensure consumers can safely dispense motor fuels safely. This code includes requirements for shear valves under the gasoline and diesel dispensers that close and prevent a mass release of motor fuel if a vehicle is driven over the dispenser.

3.0 Relevant Operational Standards and Industry Practices

API member companies comply with Department of Transportation Hazardous Materials Regulations governing transportation, inspection, and tank car/cargo tank construction standards (49 *CFR* 172, 173, 179, 180, and 181). In addition, petroleum rail transporters comply with the AAR "Manual of Standards and Recommended Practices" (Sections C.II. Specifications for Design, Fabrication and Construction of Freight Cars, C.III. Specifications for Tank Cars M-1002, and Section J. Specification for Quality Assurance M-1003).

Besides the regulatory framework governing transportation of hazardous materials, API maintains a number of design and operational standards and recommended practices that address aspects of safety and security in the distribution and marketing segment. While most of these were not developed specifically for security reasons, aspects of them are directly applicable. In many cases, prudent safety procedures would also serve to address appropriate security precautions. These recommended practices provide a starting point for developing guidance on security at distribution and marketing facilities.

The following list of standards and recommended practices address operational practices:

- Standard 2610, *Design, Construction, Operation, Maintenance, & Inspection of Terminal and Tank Facilities* (Addresses fire prevention and protection at terminal and tank facilities).

- Recommended Practice 1621, *Bulk Liquid Stock Control at Retail Outlets* (Primarily applied to underground storage of motor fuels and used oil at retail and commercial facilities).

- Recommended Practice 1004, *Bottom Loading and Vapor Recovery for MC-306 and DOT-406 Tank Motor Vehicles* (Provides an industry practice for bottom loading and vapor recovery of proprietary and hired carrier DOT MC-306 and DOT-406 tank vehicles at terminals operated by more than one supplier. Guides the terminal to implement primary and independent secondary shutdown devices in the case of an overfill

- Recommended Practice 1007, *Loading and Unloading of MC306/DOT 406 Cargo tank Motor Vehicles* (This document provides details on how tank trucks can be safely loaded when all equipment is used properly and when the person responsible for the loading follows prescribed safety procedures. It provides a short list of the equipment that should be available in case of an emergency).

The following recommended practices address prevention, safety and emergency response:

- Recommended Practice 1112, *Developing a Highway Emergency Response Plan for Incidents Involving Hazardous Materials* (Provides minimum guidelines for developing and emergency response plan for incidents involving hazardous liquid hydrocarbons such as gasoline or crude oil).

- Recommended Practice 1626, *Storage and Handling Ethanol and Gasoline-Ethanol Blends at Distribution Terminals and Service Stations* (Provides safety and fire protection guidelines for emergency response personnel and the facility).

- Recommended Practice 1627, *Storage and Handling of Gasoline-Methanol/CoSolvent Blends at Distribution Terminal and Service Stations* (Provides safety and fire protection guidelines for emergency response personnel and the facility).

The following document was written to address security needs at offshore facilities:

- Recommended Practice RP 70, *Security for Offshore Oil and Natural Gas Operations*, March 2003 (Provides recommendations for security plans for offshore facilities)

4.0 Security Guidelines

The following elements provide general security guidance for petroleum distribution and marketing operations relative to potential malevolent acts:

- Each operator should assess the potential risk of a terrorist attack. The assessment may include a determination of the likelihood of an act or attack, the type of terrorist action likely, and the consequences of an attack. The assessment should take into account the hazards of the material carried, volume of the shipment for tank trucks and rail cars or the type, size, the routes taken and location of the facility for terminals or gas stations. The assessment may include: 1) the potential risk to workers, 2) the potential risk to the environment and surrounding community, 3) the potential impact to the local, regional and national energy supply, and 4) the potential risk to adjacent and/or interdependent facilities and infrastructure.

- If, after conducting the assessment, the operator determines that a security plan is needed (All hazardous materials shippers and carriers subject to DOT's March 25, 2003 security rule, must develop a plan.), the operator should develop a facility security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, theft, or event, and 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets, actual or attempted incidents, terrorist tactics and major process system changes, and periodically audited or tested, as appropriate.

- Owner/Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout its organization. Owner/Operators should respond appropriately to this information to safeguard potential targets. Owner/Operators should also, as appropriate, report to the appropriate agencies suspicious persons, suspicious activities and behaviors, attempted or suspected incursions, terrorists' threats, or actual events that may suggest a terrorist link.

- Owner/Operators should be aware of the DOT unsatisfactory carrier reports and on the licensing status of their drivers.

- Each operator should establish clear communication channels and responsibilities for receiving, assessing, preparing for, responding to and recovering from potential or actual threats.

- Owner/Operators should be aware of existing regulations, standards and operating practices as they relate to transportation and facility security.

5.0 Elements of a Security Plan

In developing a security plan, the operator should consider several basic elements. The security plan framework shown in Figure 4.1 provides a common structure upon which an operator may develop a security plan. In developing a security plan, an operator, to the extent possible, should consider its unique security risks, and then, if possible, assess the risks to ensure the plan addresses these risks. There are many different approaches to implementing the different elements identified in Figure 4.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no “best” approach that is applicable to all situations. This guidance recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 4.1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, the selection of a SVA approach depends in part on what risk related data and information are available. Conversely and while performing a SVA, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and SVA elements could be highly integrated and iterative.

A brief overview of the individual framework elements is provided in the following section, as well as a road map to the more specific and detailed description of the individual elements that comprise the remainder of this guidance.

6.0 Security Plan Framework

Initial Data Gathering. The first step in understanding the potential risks that may occur during transportation or at a facility is to assemble information about potential risks. In this element, the operator performs the initial collection, review, and integration of data that is needed to understand location-specific and route sensitive risks to security. The types of data to support a SVA may include information on the operation, hazardous material assessments, transportation vehicle selection, surveillance practices, security measures, and the specific security issues and concerns that are unique. For Owner/Operators that are just formalizing an approach to a security plan, the initial data gathering may be focused on a limited number of facilities, vehicles, routes or assets so that a screening for the most significant security risks can be readily identified.

Initial SVA. In this element, the data assembled from the previous step is used to conduct a SVA. The SVA begins with a systematic and comprehensive search to identify possible security risks to the facility. Through the integrated evaluation of the information and data collected in the previous step, the SVA process identifies the location-specific security related events or conditions, or combinations of events and conditions, that could lead to loss of security, and provides an understanding of the likelihood and consequences of these events. If possible, the output of a SVA should include the nature and location of the most significant risks. There is a significant variation in the detail and complexity associated with different SVA methods. Some Owner/Operators without formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Other Owner/Operators may find a screening approach as the most practical means to prioritize facilities for SVA. After identifying the most significant risks, the next step is to determine what mitigation actions or security measures might be desirable to reduce risk, and where assessment techniques such as facility security inspections would be of the most value in identifying potential risk-threatening issues. The risk control and mitigation process involves:

- identification of risk control options that lower the likelihood of an incident, reduce the consequences, or both;
- a systematic evaluation and comparison of those options; and
- selection and implementation of a strategy for risk control.

SVA also helps to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote. A tiered, risk-based approach can be the most effective way to evaluate, identify, and prioritize potential targets. There are, however, a number of methods that can be employed to conduct a SVA and identify risk control activities.

Develop Baseline Security Plan. Using the output of the SVA, a plan is developed to address the most significant risks and assess the security of the facility. This plan should include the mitigation risk control actions, as well as security assessment activities, e.g., inspections and traffic and personnel control.

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that

might lead to system failures are controlled. As noted previously, a SVA may identify other risks that should be addressed.

Update, Integrate, and Review Data. After the initial security assessments have been performed, the operator has available improved and updated information about the security of the facility. This information should be retained and added to the database of information used to support future SVAs and security evaluations. Furthermore, as operations continue, additional surveillance and other data are collected, thus expanding and improving the historical database and experience levels.

Reassess Risk. SVAs should be performed periodically to factor in recent operating data, consider changes to the facility design, change in transportation routes, carrier changes and to analyze the impact of any external changes that may have occurred since the last SVA, e.g., adjacent facilities and changes in traffic flow. The results of security assessments, such as inspections and drills, should also be factored into future SVAs to ensure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The baseline security plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated SVA results should also be used to support scheduling of future security assessments.

Audit Plan. The operator should collect information and periodically evaluate the success of its security assessment techniques and other mitigation risk control activities. The operator should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions.

Managing Change. A systematic process should be used to ensure that changes to a facility (or transportation vehicle) are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future SVAs to be sure the SVA process addresses the facility as it is currently configured.

As this final element indicates, managing security is not a one-time process. As implied by the loop in the lower portion of Figure 4.1, a security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs must be periodically updated and revised to reflect current vehicle or facility conditions so Owner/Operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

7.0 Security Conditions and Potential Response Measures

This section describes a progressive level of protective measures that may be implemented in response to the possibility of a terrorist threat or to a terrorist threat directed at terminals, assets, transportation vehicles (trucks, rail cars) and personnel consistent with the National Threat Advisory System (HSAS) developed by the Department of Homeland Security. (A comparable system was established by the Coast Guard; in the event that a company uses "MARSEC" levels, these guidelines have tried to properly correspond MARSEC with the HSAS alert levels). The purpose of the HSAS is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and operator personnel prior to and during a threat crisis. The associated response measures may be implemented for each security alert level at each designated facility and for each transportation vehicle.

These potential measures do not apply to all marketing and distribution operations and facilities, but to those that the operator, after reviewing potential security threats and risks, designates as requiring a higher state of preparedness. Also, since each is unique, the measures below represent a variety of measures that could be considered. All of these measures may not be appropriate for all transportation vehicles or at all designated facilities and there may be measures, not listed here, that should be implemented. The operator's own security plan should be the basis of security for transportation operations and at terminals.

Each operator should develop a means to advise and communicate to operator personnel and transportation personnel and others as warranted the security condition at such designated facilities and otherwise as applicable. The potential measures associated with each alert level are not prioritized but those implemented should be initiated concurrently where practical and as applicable. Local facility management should maintain a record of specific actions taken for each alert level. Following is a detailed explanation for each alert level and the potential response measures associated with each level:

Low Condition—Green: This condition exists when there is a low risk of possible terrorist activity or civil unrest. **Green** condition is for normal operating conditions. All measures under **Green** should be maintained indefinitely. Potential measures to consider implementing include:

<u>Access Control/Perimeter Protection</u>

- Having all contractors and visitors check or sign in and out of designated facilities at the designated location(s) within the facility.

- Ensuring existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting. Ensuring that transportation vehicles implement security measures to prevent tampering and theft while parked, in transit or while loading or unloading. Identifying those additional security measures and resources that could enhance the security at the higher alert levels, e.g. increased surveillance or lighting.

Communications

- Establishing emergency communications and contact information with appropriate agencies. Considering redundant emergency communications in both the hardware and the means for contacting appropriate agencies.

Training/Policies/Procedures/Plans

- Developing terrorist and security awareness information and providing education to employees on security measures and procedures. Cautioning employees not to talk with third parties concerning facility operations and security measures or any related issues. Each company should have a system in place to track unsatisfactory carriers and driver licensing status.

- Advising all personnel to report to the appropriate agencies the presence of unidentified individuals and transportation vehicles including those being operated out of the ordinary, abandoned parcels or packages, and other suspicious activities.

- Developing procedures for shutting down and evacuating the facility, if considered necessary, in case of imminent attack. Developing procedures for returning vehicles to secure locations.

- Incorporating security awareness and information into public education programs at onshore facilities and notifications to emergency response organizations as appropriate.

- Surveying surrounding areas and along transportation routes to determine if activities exist that may pose security risks to the facility, e.g., airports, government buildings, industrial facilities, railroads and other facilities.

- Ensuring contingency and business continuity plans are current and include a response to terrorist threats.

- Reviewing existing emergency response plans and modifying them, if required, in light of potential threats.

Cyber Security

- Developing and implement hardware, software, and communications security for computer based operational systems.

Guarded Condition—Blue (MARSEC I): This condition exists when there is an increased general threat of possible terrorist activity against personnel, transportation vehicles and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher alert measures. It may be necessary to implement certain selected measures from higher alert levels to address information received or to act as a deterrent. All measures under **Blue** should be maintained as long as the **Blue** threat exists. In addition to the measures suggested by **Green**, the following measures could be considered:

Perimeter Protection/Access Control

- Securing all facilities, buildings and storage areas not in regular use, if possible. Increasing frequency of inspections and patrols within the facility including the interior of buildings and along the facility perimeter.

- Inspecting perimeter fencing and repairing all fence breakdowns. Routinely inspect vehicles for suspicious items. In addition, reviewing all outstanding maintenance and capital project work that could affect the security of facilities.

- Reducing the number of access points, if possible, for transportation vehicles and personnel to minimum levels. Periodically spot checking the contents of vehicles and rail cars at the access points. Being alert to vehicles or watercraft parked or moored for an unusual length of time in or near a facility.

- Checking designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increasing surveillance in designated areas.

- Requiring visitors to check in at the designated facility office or to designated personnel and verifying their identification - being especially alert to repeat visitors or outsiders who have no apparent business at the facility and are asking questions about the facility or transportation operations or related issues including personnel. Familiarizing facility personnel with vendors who service the facility or transportation vehicles and investigating unusual changes in vendor personnel.

- Inspecting all packages/equipment coming into a facility. Not opening suspicious packages. Reviewing the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving packages.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.

- Testing security and emergency communications procedures and protocols.

Training/Policies/Procedures/Plans

- Reviewing all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.

- Ensuring that an operator response can be mobilized appropriate for the increased security level. Reviewing communications procedures and back-up plans with all concerned.

Elevated Condition—Yellow (MARSEC II): This condition exists when there is an elevated risk of terrorist activity against personnel, transportation vehicles, railcars and facilities. All measures under **Yellow** should be maintained as long as the **Yellow** threat exists. In addition to the measures suggested by **Blue**, the following measures could be considered:

Perimeter Protection/Access Control

- Closing and locking gates and barriers except those needed for immediate entry and egress. Inspecting perimeter and perimeter fences on a regular basis. Ensuring that other security systems are functioning and are available.

- Inspecting on a more frequent basis the interior and exterior of all buildings and around all storage tanks and other designated critical areas and access points.

- Dedicating personnel to assist with security duties for transportation vehicles, railcars, and at designated facilities with duties to monitor personnel entering the facility and to inspecting the area on a regular basis, reporting to facility management as issues surface.

- Limiting visitors and confirming that the visitor has a need to be and is expected at the facility. Escorting visitors while at the facility.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.

- Advising appropriate agencies that the facility is at an **Yellow** level and advising the measures being employed - requesting appropriate agencies to increase the frequency of their routine patrol of the facility if possible.

- Checking to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirming availability of security resources that can assist with extended coverage, if needed.

- Identifying locations where explosive devices could potentially be hidden near sensitive or vital areas.

- Instructing employees working alone or in transit to check-in on a periodic basis.

- Directing that all personal, operator, and contractor vehicles at designated facility sites are secured.

High Condition—Orange (MARSEC III): This condition applies when there is a high risk of terrorist attacks or an incident occurs or information is received indicating that some form of terrorist action against personnel and facilities is imminent. In addition to the measures suggested for **Yellow**, the following measures could be considered:

Perimeter Protection/Access Control

- Reducing facility access points to the absolute minimum necessary for continued operation.

- Securing a trained and knowledgeable security workforce to man the impacted facilities or transportation vehicles - ensuring that all security personnel have been briefed concerning policies governing the use of force and pursuit.

- Increasing security patrol activity to the maximum level sustainable. Increasing perimeter patrols and inspections.

- Checking all security systems such as lighting and intruder alarms to ensure they are functioning. Installing additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.

- Prohibiting unauthorized or unidentified vehicles/personnel entrance to designated facilities.

- Inspecting all vehicles and railcars entering facilities, if possible, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed.

- Limiting access to designated facilities to those personnel who have a legitimate and verifiable need to enter the facility. Implementing positive identification of all personnel. Evacuating all non-essential personnel.

- Implementing frequent inspection of designated facilities. Increasing patrolling or inspections at night and ensuring all vulnerable critical points are fully illuminated and secure.

- Protecting the impacted facility from an attack by a parked or moving vehicle - operator vehicles may be used for this purpose. Implementing centralized parking and shuttle service where feasible.

- Canceling or delaying all non-vital facility work conducted by contractors, or continuously monitor their work with operator personnel.

Communications

- Advising appropriate agencies that the facility is at an **Orange** alert level and advise the measures being employed - requesting an increase in the frequency of their patrol of the facility.

- Consulting with local authorities about control of public roads and accesses that might make the facility more vulnerable to terrorist attack if they were to remain open. Inform them of the location of the hazardous material transportation vehicles.

Training/Policies/Procedures/Plans

- Continuing **Green**, **Blue**, and **Yellow** measures or introducing those that have not already been implemented.
- Activating emergency response plans.
- Scheduling more frequent visits to remote sites that are potentially impacted.
- Ensuring employees not work alone in remote areas or increasing the frequency of call-ins from remote locations or while in transit.

Severe Condition—Red (MARSEC III): This condition applies when there is a severe risk of terrorist attacks, an attack has occurred in the immediate area which may affect the facility, or when an attack is initiated on the facility and its personnel. Normally, this alert is declared as a localized condition at the affected facility. In addition to the measures suggested for **Orange**, the following measures could be considered:

Perimeter Protection/Access Control

- Augmenting security forces to ensure control of the facility and access to the facility and other potential target areas. Establishing surveillance points and reporting criteria and procedures. Soliciting assistance from appropriate agencies in securing the facility and access, if possible. Cooperating with authorities if they take control of security measures.

Training/Policies/Procedures/Plans

- Continuing **Orange** and **Yellow** measures or introducing those that have not already been implemented.
- Consider shutting down impacted facilities and operations in accordance with contingency plans unless there is a compelling reason not to and evaluating security prior to resuming operations if they are temporarily shut down. Consider returning all vehicles to a secure location if the threat extends to actual transport vehicles if this is determined to be the most appropriate action.
- Implementing business contingency and continuity plans as appropriate.

Part V—Security Guidelines for Oil and Natural Gas Production Operations

Part V—Security Guidelines for Oil and Natural Gas Production Operations

1.0 Introduction

These guidelines are intended to assist oil and natural gas producing Owner/Operators in assessing security needs during the performance of oil and natural gas operations. Additionally, the oil and natural gas industry uses a wide variety of contractors to assist in drilling, production, and construction activities. Contractors typically are in one of the following categories: drilling, workover, well servicing, construction, electrical, mechanical, transportation, painting, operating, and catering/janitorial. Contractors should have policies and practices in place that are consistent with the operator's security needs.

2.0 Overview of Upstream Operations

Onshore, oil and natural gas are produced at over 300,000 sites across the United States, and nearly 30,000 new wells are drilled each year. The overwhelming majority of these sites are located in rural areas. There are only a few cities, such as Houston and Los Angeles that have oil and natural gas production within the city limits. These urban facilities already employ more security measures than typical E&P facilities.

According to the Department of Energy, small Owner/Operators, those typically employing 10 full-time and 3 part-time employees, drill 85 percent of U.S. wells. Small Owner/Operators also produce 65 percent of the natural gas and 40 percent of the oil consumed by Americans.

- *Oil wells*. Over 75% of oil wells in the U.S. produce less than 10 barrels of oil daily. Most of these wells also produce large volumes of water, making the oil/water mix that comes to the surface a low risk for ignition. Over 95% of oil wells require artificial lift (pumping unit, electrical pump, etc) to bring the oil to the surface. If the pumping unit, for example, is not working, oil is not coming to the surface. While most of these sites have a tank for storage of the oil, the volume of oil stored on-site is limited.
- *Natural Gas wells*. Similar to oil wells, the majority of onshore natural gas wells are remotely located and produce marginal volumes of gas. Natural gas produced by any single well would not be significant in terms of total U.S. consumption.

About 28 percent of U.S. oil and natural gas production is from offshore sources, but this production is spread over more than 4,000 oil and natural gas platforms. Even the platforms with the highest daily production total only around 3 percent of U.S. production and an even lower percentage of consumption. The loss of any one platform would not significantly affect U.S. oil and natural gas supplies. Increasingly, however, larger platforms are the norm, and used for development of several fields in deep water. These larger platforms mean a greater concentration of personnel, often 100 to 150 people.

Offshore platforms are designed with redundant safety systems to stop the flow of oil or natural gas in case of any unusual event. Platforms use sophisticated subsurface safety valves that close automatically to prevent oil spills when sensors detect any drop in pressure at the surface. These automatic fail-safe devices are installed in wells below the sea floor, protecting seabeds, sea life, the environment, workers and the public. Manual safety shut-off switches are also accessible in a number of locations around platforms for the wells and pipelines. In the event of a fire or attack on the platform, the valves would shut off the flow of oil or natural gas. Any release would be limited to the amount of oil in the flowlines from the sea floor to the platform.

3.0 Relevant Operational Standards and Industry Practices

API maintains a number of design and operational recommended practices that address aspects of safety and security in the E&P industry. While none of these were developed specifically for security reasons, aspects of them are directly applicable. In many cases, prudent safety procedures would also serve to address appropriate security precautions. These recommended practices provide a starting point for developing guidance on security, if needed, at E&P sites.

The following list of recommended practices address operational measures:

- Recommended Practice 2A, *Planning, Designing, Constructing Fixed Offshore Platforms* (Contains engineering design principles and practices for fixed offshore platforms including assessment of existing platforms, and fire, blast, and accidental overloading).
- Recommended Practice 2FPS, *Planning, Designing, Constructing Floating Production Systems (FPSOs)* (This recommended practice provides guidelines for design, fabrication, installation, inspection and operation of floating production systems).
- Recommended Practice 2T, *Planning, Designing, and Constructing Tension Leg Platforms (TLPs)* (Summarizes available information and guidance for the design, fabrication and installation of a tension leg platform).
- Recommended Practice 14B, *Design, Installation, Repair and Operation of Subsurface Safety Valve Systems* (Provides guidelines for safe operating practices of equipment used to prevent accidental release of hydrocarbons to the environment in the event of unforeseen circumstances).
- Recommended Practice 14C, *Analysis, Design, Installation and Testing of Basic Surface Safety Systems on Offshore Production Platforms* (Describes processes and systems for emergency well shut-ins on offshore platforms).
- Recommended Practice 14H, *Installation, Maintenance and Repair of Surface Safety Valves and Underwater Safety Valves Offshore* (Provides guidelines for safe operating practices of equipment used to prevent accidental release of hydrocarbons to the environment in the event of unforeseen circumstances).
- Recommended Practice 14J, *Design and Hazardous Analysis for Offshore Production Platforms* (Provides procedures and guidelines for planning, designing, and arranging offshore production facilities and for performing a hazardous operations analysis).
- Recommended Practice 75, *Development of a Safety and Environmental Management Program for Outer Continental Shelf Operations and Facilities* (Provide guidance in preparing safety and environmental management programs for offshore facilities).
- Recommend Practice 750, *Management of Process Hazards* (Provides assistance in helping to prevent the occurrence of, or minimize the consequences of catastrophic releases of toxic or explosive materials).
- An Overview of Petroleum Industry Operations and An Assessment of Current Security Practices & Standards

The following recommended practices address prevention, safety and emergency response:

- Recommended Practice 49, *Drilling and Well Servicing Operations involving Hydrogen Sulfide* (Describes response plans for wells involving hydrogen sulfide).

- Recommended Practice 54, *Occupational Safety for Oil and Gas Well Drilling and Servicing Operations* (Describes emergency response plans for oil and natural gas well drilling and servicing).
- Recommended Practice 74, *Occupational Safety for Onshore Oil and Gas Production Operations* (Describes general occupational safety and emergency response plans).
- Publication 761, *Model Risk Management Plan for E&P Facilities* (Provides a guideline on how affected facilities develop a risk management plan including hazard assessment, prevention and emergency response).

4.0 Security Guidelines

The following elements provide general security guidance for production operations relative to potential security threats:

- Each operator should assess the potential security risk at its facilities. This informal assessment may include a determination of the likelihood of an act or attack, the type of action likely, and the consequences of an attack. The assessment should take into account the type, size, and location of the facility. The assessment may consider: 1) the potential risk to workers, 2) the potential risk to the environment and surrounding community; 3) the potential impact to the local, regional and national energy supply; and 4) the potential risk to adjacent and/or interdependent facilities and infrastructure.

- If, after conducting the informal assessment, the operator determines that additional security planning is needed, the operator should develop a facility security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, or event, and; 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets and terrorist tactics, actual or attempted incidents, major process changes, and periodically audited or tested, as appropriate.

- Owner/Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout the organization. Owner/Operators should respond appropriately to this information to safeguard potential targets. Owner/Operators should also report, as appropriate, suspicious activities and behaviors, attempted incursions, terrorist threats, or actual events to the appropriate agencies.

- Each operator should establish clear communication channels and responsibilities for receiving, assessing, preparing for, responding to and recovering from potential or actual threats.

- Each operator should establish and maintain effective liaison with local emergency response agencies and organizations, as appropriate.

- Owner/Operators should be aware of existing regulations, standards and operating practices as they relate to facility security.

5.0 Elements of a Security Plan

In developing a security plan, the operator should consider several basic elements. The security plan framework shown in Figure 1 provides a common structure upon which an operator may develop a security plan. In developing a security plan, an operator, to the extent possible, should consider its unique security risks, and then, if possible, assess the risks to ensure the plan addresses these risks. There are many different approaches to implementing the different elements identified in Figure 1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 1 are shown sequentially for ease in illustration, there is a significant amount of information flow and interaction between the different steps. For example, the selection of a SVA approach depends in part on what risk related data and information are available. While performing a SVA, additional data needs may be identified that can be used to better address potential vulnerability issues. These data gathering and SVA elements should be highly integrated and iterative, as appropriate.

A brief overview of the individual framework elements is provided in this section, as well as a roadmap to the more specific and detailed description of the individual elements that comprise the remainder of this guideline.

6.0 Security Plan Framework

Initial Data Gathering. The first step in understanding the potential risks at a facility is to assemble information about potential risks. In this element, the operator performs the initial collection, review, and integration of data that is needed to understand location-specific risks to security. The types of data to support a SVA may include information on the operation, surveillance practices, security measures, local incident history, and the specific security issues and concerns that are unique for each facility. For Owner/Operators that are just formalizing an approach to a security plan, the initial data gathering may be focused on a limited number of facilities or assets so that a screening for the most significant security risks can be readily identified.

Initial SVA. In this element, the data assembled from the previous step is used to conduct a SVA of the facility. The SVA begins with a systematic and comprehensive search to identify possible security risks to the facility. Through the integrated evaluation of the information and data collected in the previous step, the SVA process identifies the location-specific security related events or conditions, or combinations of events and conditions, that could lead to loss of security, and provides an understanding of the likelihood and consequences of these events. If possible, the output of a SVA should include the nature and location of the most significant risks on the facility. There is a significant variation in the detail and complexity associated with different SVA methods. Some Owner/Operators without formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Other Owner/Operators may find a screening approach as the most practical means to prioritize facilities for SVA. After identifying the most significant risks, the next step is to determine what mitigation actions or security measures might be desirable to reduce risk, and where assessment techniques such as facility security inspections would be of the most value in identifying potential risk-threatening issues. The risk control and mitigation process involves:

- identification of risk control options that lower the likelihood of an incident, reduce the consequences, or both;
- a systematic evaluation and comparison of those options; and
- selection and implementation of a strategy for risk control.

SVA also helps to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote. A tiered, risk-based approach can be the most effective way to evaluate, identify, and prioritize potential targets. There are, however, a number of methods that can be employed to conduct a SVA and identify risk control activities.

Develop Baseline Security Plan. Using the output of the SVA, a plan is developed to address the most significant risks and assess the security of the facility. This plan should include the mitigation risk control actions, as well as security assessment activities, e.g., inspections and traffic and personnel control.

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that

might lead to system failures are controlled. As noted previously, a SVA may identify other risks that should be addressed.

Update, Integrate, and Review Data. After the initial security assessments have been performed, the operator has available improved and updated information about the security of the facility. This information should be retained and added to the database of information used to support future SVAs and security evaluations. Furthermore, as the facility continues to operate, additional surveillance and other data are collected, thus expanding and improving the historical database and experience levels.

Reassess Risk. SVAs should be performed periodically to factor in recent operating data, consider changes to the facility design, and to analyze the impact of any external changes that may have occurred since the last SVA, e.g., adjacent facilities and changes in traffic flow. The results of security assessments, such as inspections and drills, should also be factored into future SVAs to ensure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The baseline security plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated SVA results should also be used to support scheduling of future security assessments.

Audit Plan. The operator should collect information and periodically evaluate the success of its security assessment techniques and other mitigation risk control activities. The operator should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions.

Managing Change. Production facilities and the environment in which they operate are never static. A systematic process should be used to ensure that changes to the facility are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future SVAs to be sure the SVA process addresses the facility as it is currently configured.

A security management program involves a continuous cycle of monitoring facility conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs must be periodically updated and revised to reflect current facility conditions so Owner/Operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

Part VI—Security Guidelines for Marine Transportation

Part VI—Security Guidelines for Marine Transportation

1.0 Introduction

This guideline outlines a Security Vulnerability Assessment (SVA) process that a Marine Transportation system operator can use to assess risks and make decisions about risks in operating their marine operations, and to make progress towards the goal of reducing the risks associated with operations. Part I, Section 4.0 describes the framework for creating a generic security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 4.1. Section 5 describes the basic features of a SVA, using the SVA risk variables at a facility level to provide a risk screening at a facility level, and the SVA approach.

2.0 Overview of Segment Operations

The Marine Transportation Segment represents the transportation by water of crude oil, its products and derivatives, petroleum gases and liquefied natural gas. This includes marine operations at terminals at the ship-to-shore interface.

Every day, Americans use nearly 20 million barrels of oil and petroleum products. Of that, about 10 million barrels are imported by tankers. Tankers make more that 20,000 port calls to the U.S. each year. Tankers and barges not only carry crude oil, but with pipelines transport petroleum products like gasoline, diesel fuel and home heating oil from refineries to consumers.

Regulations relating to the Marine Segment were put in place to promote the safe, environmentally sound, secure, and efficient marine transportation of petroleum and petroleum products. Since the September 11 events, the marine segment has placed new emphasis on security, and is working closely with the U.S. Coast Guard to ensure maritime transportation security at both U.S. ports and abroad. API is also working with the U.S. Coast Guard to develop appropriate security guidelines for the Marine Segment. Once finalized, these guidelines will be included in this guidance document.

3.0 Relevant Operational Standards and Industry Practices

U.S. Regulations

Since the passage of the Oil Pollution Act of 1990 (OPA), the petroleum industry has made vast improvements in reducing the number of vessel casualties, reducing the number of spills and the quantity of oil spilled, improving overall safety and increasing the effectiveness of response efforts. Although these regulations were put in place primarily for other purposes, in many cases they also serve to address appropriate security precautions. These regulations provide a starting point for developing guidance on maritime security elements.

The following is a list of relevant U.S. regulations:

- 59 FR 34070 Facility Response Plans
- 62 FR 13991 Response Plans for Facilities Located Seaward of the Coast Line
- 61 FR 30533 Facility Response Plans for Pipelines (Interim Final Rule)
- 57 FR 7640 Coastwise Oil spill Response Cooperatives
- 60 FR 65478 Criminal Record Reviews in Renewals
- 60 FR 45006 Designation of Lightering Zones
- 59 FR 42962 Escorts for Certain Tankers
- 60 FR 13318 Establishment of Double Hull Requirements for Tank Vessels
- 59 FR 40186 Existing Tank Vessel Requirements – Lightering requirements and Advanced Notification
- 62 FR 1622 Existing Tank Vessel Requirements – Structural Requirements
- 61 FR 39770 Existing Tank Vessel Requirements – Training, Survey and Maneuverability Measures
- 61 FR 7890 Facility Response Plans for Marine and Non-Marine Transportation Facilities
- 58 FR 48434 Lightering Requirements
- 59 FR 47384 National Contingency Plan Revisions
- 58 FR 13360 Pilotage in Prince William Sound

- 58 Fr 27628 Second Person Required (on bridge)

- 61 FR 1052 Tank Vessel Response Plans

- 59 Fr 49294 Term of Licenses, Certificates of Registry and Merchant Mariners Documents

- 57 FR 14483 Vessel Communication Equipment Regulations

- 59 FR 36316 Vessel Traffic Service

International Conventions and Treaties

The International Maritime Organization (IMO), a body of the United Nations, was organized in the late 1950s to effectively promote maritime safety. Throughout the years, IMO has led international efforts to develop conventions and treaties aimed at increasing safety and reducing marine pollution. Recently, at the request of the Commandant of the U.S. Coast Guard, the IMO nations approved a resolution calling for the organization to seek ways to enhance maritime security on a global basis. Activities are underway to meet the goals of this resolution. To learn more about IMO, see www.imo.org. Detailed information on each of the IMO Conventions can be found within the IMO web page at IMO's Conventions.

4.0 Ongoing Initiatives/Additional Measures Implemented Since September 11

The U.S. Coast Guard has taken the lead in improving America's maritime security by coordinating a multi-agency, private sector, and international effort to prevent malevolent acts. Immediately following the September 11 attack, the U.S. Coast Guard undertook the following:

- Identified high interest vessels and prioritized critical infrastructure so that its limited resources could be applied in an efficient manner.

- As part of the Homeland Security Plan, the U.S. Coast Guard established Maritime Security (MARSEC) levels (MARSEC I – III) for assessing security response capabilities, activities, and equipment inventories.

- Increased the Advanced Notice of Arrival Information (NOA) time for commercial vessels arriving from foreign ports from 24 to 96 hours, to provide more analysis of crew and passenger lists, etc.

- Instituted a Sea Marshal program for high-risk ports on the west coast (San Francisco, San Diego, and Los Angeles).

- Held a three-day public workshop (January 28 – 30, 2002) to discuss/assess security procedures, programs, and capabilities within marine transportation systems, in an effort to ascertain whether improvements (i.e., new regulations, the development of industry standards) are necessary.

Part VII—Security Guidelines for Cyber/Information Technology (IT) in the Petroleum Industry

Part VII—Security Guidelines for Cyber/Information Technology (IT) in the Petroleum Industry

1.0 Introduction

The petroleum industry is a worldwide industry that is highly dependent on technology for communications and operations, much of which are in remote or politically unstable areas. Therefore, a key goal of the petroleum industry is to protect the industry's cyber/information technology infrastructure and information against cyber terrorism that would disrupt operations.

A cyber/information technology security program provides a means to improve the security of the petroleum industry from cyber terrorism and allocate resources to effectively:

- Identify and analyze actual and potential precursor events that can result in cyber security-related incidents.
- Identify the likelihood and consequence of potential cyber security-related events.
- Provide a comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities.
- Provide a structured, easily communicated means for selecting and implementing risk reduction activities.
- Establish and track program performance with the goal of improving that performance.
- Establish alert and response measures for a broad range of security threats.
- Establish a communications program to share threat information between federal agencies and industry.

ISO/IEC International Standard 17799, ***Information technology—Code of practice for information security management***, describes a framework for creating a cyber security program and forms the basis of this guideline. This framework has been endorsed by API's Information Technology Security Forum (ITSF) as voluntary guidance to protect the petroleum industry against acts of cyber terrorism. Information on how to obtain this standard is provided at http://webstore.ansi.org/ansidocstore/iso.asp.

The guidance provided herein and in ISO/IEC International Standard 17799 does not attempt to provide an all-inclusive list of cyber security considerations, but does provide a basis for measures that should be considered when evaluating and implementing cyber security measures. The standard attempts to ensure preservation of confidentiality, integrity and availability of user access, hardware, software and data. The Standard identifies eight steps in the security process: create an information security policy, select and implement appropriate controls, obtain upper management support, perform Security Vulnerability Assessments (SVA), create statement of applicability for all employees, create an information security management system, educate and train staff, audit.

It must be recognized that some of the information that would be part of a cyber security program needs to remain confidential. Cyber security management may want to develop a confidentiality program to ensure it is understood what information can be shared and what should remain confidential.

2.0 Ongoing Security Management

The changing business environment has posed new threats to the security of the petroleum industry. In addition to physical concerns, companies need to take steps to ensure cyber security as well. As technology advances, making the petroleum industry more streamlined and efficient, cyber security has become an increasingly important job.

Petroleum industry cyber initiatives that are currently underway include:

- Companies recognize that effective security is a combination of layered security processes, policies, procedures, education, awareness and assessments to ensure compliance. Companies currently use a combination of firewalls, intrusion detection, antivirus and risk assessment programs, host intrusion detection systems and other audit programs to safeguard their computer systems. Each company analyzes and assesses its needs based on individual vulnerability and probability assessments.

- Companies are clued into efforts at the local and/or national level such as the Energy Information Sharing and Analysis Center (ISAC), FBI InfraGard, National Infrastructure Protection Center (NIPC), SANS, CERT, I4, ISF and other API committees to receive security threat and monitoring information.

- In November 2000, the API Information Technology Security Forum (ITSF) was formed to address the cyber security of the petroleum industry. Committee members possess a high level of cyber security knowledge and have been focusing on activities and initiatives to increase security awareness within the industry; privacy; policies; risk management and mitigation; and emerging technologies. The ITSF developed and delivered a Framework for a Computer Security Incident Response Plan (November 2001) to provide guidance on how to structure a cyber-related incident response program. This document is provided in Appendix A.

- Companies have individually taken steps to reduce computer incidents such as confidential information being given out by employees, use of weak passwords, unauthorized access to facilities and networks, telephone fraud, spread of computer viruses, software piracy and unauthorized email or Internet usage.

- Endorsement of ISO/IEC International Standard 17799, ***Information technology—Code of practice for information security management***, to ensure preservation of confidentiality, integrity and availability of user access, hardware, software and data. The Standard involves eight steps in the security process: create an information security policy, select and implement appropriate controls, obtain upper management support, perform security risk assessment, create statement of applicability for all employees, create an information security management system, educate and train staff, audit.

3.0 Security Guidelines

Accountability/Ownership

It is important to establish an owner for all hardware, software, data and other information assets. While typically not the legal owner of the asset, having identifiable responsibility for these assets within a company is fundamental to the control process. Some of the key responsibilities of an owner include:

- Define the business requirements for which the asset is needed.
- Establish the value, criticality and sensitivity of the asset.
- Establish, maintain, document and verify cost effective controls commensurate with the risk.
- Establish policies and procedures to deal with issues related to the asset.

Since the business unit is typically in a better position to effectively assess business requirements, value and sensitivity of an asset, it is recommended that ownership be placed within the business unit under most circumstances, not in the IT function. However, it would be appropriate for the IT function to own computing infrastructure and services that support the entire company, such as the company's network, etc. In any case, it is important to have a single owner for each asset. The responsibility for many owner tasks can be delegated to custodians but the owner remains accountable for the asset.

Security Policies, Standards and Procedures

The development and implementation of Information Security policies, standards and procedures focused on protecting a company’s information and information technology assets is foundational to the implementation of a Security Management process. Policies are a prerequisite for defining the acceptable behaviors that a company desires to promote in protecting its critical information and information technology infrastructures. The policies should be simple, enable business success, and enable protection of the company as well as the employees. Since the policies set the tone for the company’s culture and management processes relative to protecting information and information technology, the policy must have executive management sponsorship, clearly articulate accountabilities and responsibilities, and be communicated to every employee and system user in the entire company. The company policies should cover areas such as:

- Business Conduct and Appropriate System Usage
- E-mail and Internet Usage
- Virus and Malicious Code
- Remote Access and Third Party Connectivity
- Legal Notice and Legal Compliance (Logon Banner, Privacy, etc)
- Identity Management (Employee and Contractors)
- System Monitoring
- Technology Security (Wireless, PDA’s, Operating Systems)

- Physical Security (Laptops, Computer Rooms, etc)
- Incident Reporting and Response
- Risk Management
- Security Awareness, Education and Training

Each policy should be accompanied by a set of standards and procedures that provide a foundation for the operational implementation and compliance assessment of the policies on a routine basis. The standards and operating procedures should be derived from industry technology standards and/or “best practices” and clearly define “mandatory” requirements to which adherence is not an option.

The company Information Security Officer or Manger is generally accountable for leading the development, implementation and maintenance of a company’s information security policies, standards and procedures. However, it is recommended that this be accomplished by working in “partnership” with representatives from the functional areas of: IT Audit, Human Relations, Legal, Physical Security and Information Systems at a minimum; and under the guidance of an executive steering team comprised of the Chief Information Officer, Chief Legal Counsel, Chief Auditor, Chief HR Officer, and key executive business unit representative(s) at a minimum.

Security Vulnerability Assessments

Performing a Security Vulnerability Assessment (SVA) is fundamental to cost-effectively reducing risks to acceptable levels. An owner-approved SVA establishes the priorities for further action by:

- Identifying the most significant exposures or potential negative consequences of events.
- Documenting the owner's judgment on the exposures and risks in the absence of controls.
- Documenting follow-on action plans or the justification for accepting residual risks.

Some of the potential consequences associated with computer systems that should be evaluated include:

- The loss of information integrity and its impact on business decisions, transactions, etc.
- The disclosure of sensitive information and its impact on the company's competitive position or legal obligations.
- The loss of processing capability or information and its impact on the company's continued viability.
- Violation of regulations or contract/agreement provisions and its impact on the company's reputation, legal standing, etc.
- The extent the company's network could be impacted.
- The financial impact associated with these potential consequences.
- The impact of the system on health, safety or the environment.

Data and Information Asset Classification

Data and information asset classification is done primarily to identify assets that require protection and hence focus protection efforts and budget on that purpose. Classification of assets is generally based on the business unit impact of their loss, unauthorized disclosure, corruption or lack of availability. Classification and access controls work together to provide protection to assets that are identified as critical and to ensure access to them is monitored.

Typical components of a classification program include:

- Policy defining the classification program
- Levels of ownership and stewardship
- Awareness training
- Standards for asset labeling
- Handling, storage, transmission, access
- Compliance monitoring program
- Business continuity maintenance—an on-going process that identifies ownership, as well as ongoing re-assessment and maintenance of the business continuity strategy.

Using the processes identified above, an organization should:

- Identify critical business processes
- Prepare a plan for business continuation

Next the organization needs to think about educating its employees and IT system users on security protections and practices.

Security Awareness Education

Companies will want to invest some time and resources into developing a Security Awareness Program. Personnel must have the knowledge to understand the significance of their actions. Human interaction may act in ways that undermine security controls, causing security breaches. A Security Awareness Program is chartered to:

- Clarify why security is important
- Identify who should attend Security Awareness Training
- Identify the responsible department or point of contact for providing Security Awareness Training
- Identify existing security controls and measures being taken to protect personnel and assets
- Identify existing security concerns
- Identify security controls that are needed
- Clarify employee security responsibilities
- Serve as a forum to discuss security questions

The Security Awareness Program should be included in "new hire" orientations, as well as ongoing refresher activities. Incentive programs may also be developed to aid in company awareness and training adoption.

The Security Awareness Program should include both physical and cyber security initiatives.

Physical and Environmental Security

It is important to prevent unauthorized access, theft, damage and interference to systems, media and information. Therefore, critical or sensitive information processing facilities should be housed in separate secure areas, protected by a defined security perimeter. The nature of this perimeter should be commensurate with the identified risks. Protection should be extended to supporting facilities such as electrical supply and cabling infrastructure. Placement of systems should take into account environmental risks and should provide protection and detection of hazards like fire.

A policy requiring desks to be left clear of classified documents and media, and screens left clear of information when unattended should be put in place where feasible.

Change Control Methodology

It is important to establish a methodology to evaluate system changes and configuration controls to ensure the secure operation of the networking infrastructure and the continued confidentiality, integrity and availability of information systems. A change control process should be chartered and empowered to manage change within the information technology environment. This change control process should include features such as a change submission request and evaluation, recovery and back-out procedures, and a mechanism to monitor and project the organizations capacity to ensure uninterrupted availability. Segregation and rotation of duties will minimize the potential for collusion and uncontrolled exposure of information resources.

Intrusion Detection and Incident Management

Systems should be implemented and qualified specialists should be assigned to log and monitor for inappropriate network activities. Electronic firewalls should be set up and properly configured to detect intrusions or other hostile activity at all external network access points, and between certain internal networks as appropriate. Mechanisms should be implemented to monitor system access and system use to detect unauthorized activities. An incident response plan (see Appendix A) should be developed to ensure the timely and effective response to relevant exploits and report information of concern to appropriate Information Technology and business contacts. An incident response team should be assigned to respond to security events such as virus outbreaks, network penetration attempts, denial of service, intrusions and data theft or compromise.

Malicious Code

Malicious code (viruses, worms, trojans, etc) continues to become more complex and sophisticated so it is essential to implement effective controls to mitigate the risks associated with it. To effectively combat this worsening threat, multiple solutions should be employed. Standard anti-virus software should be installed throughout the enterprise, on personal computers, data file servers, centralized application servers such as e-mail and web servers, and in the firewall complex. Anti-virus solutions should scan all protocols that could contain malicious code, such as SMTP, FTP and HTTP. Anti-virus software should be centrally administered within the corporation, taking the end-user out of the equation, to ensure desktops are updated quickly. Operating system and application security patches should be evaluated based on the risk they reduce and installed as appropriate to minimize the effectiveness of malicious code. Finally, it is important to maintain employee awareness efforts since users are typically the first to receive malicious code and most often the cause of its dispersal.

Network Security

A range of controls is required to achieve and maintain security in computer networks. This includes the establishment of controls on access to internal networks and, in some cases, outward-bound connections to external networks. The extent of networks managed by a company should be known. The network security perimeter should be defined by appropriately configured and managed control devices, such as security gateways and firewalls. Simple router controls in many cases are insufficient.

These network controls should be defined by a clear policy that defines:

- The networks and network services which are allowed to be accessed;
- Authorization procedures for determining who is allowed to access which networks and networked services;
- Management controls and procedures to protect the access to network connections and network services;
- The degree of testing, monitoring and security detection (such as intrusion detection) that is required to ensure required security levels are maintained.

Where the security of access to applications, data or systems is dependent on some trust being present in the network, the path from the user terminal to the computer service may need to be protected or controlled.

Access to networks by remote users should be subject to an appropriate level of authentication, as should access to network management facilities and remote diagnostic ports on network equipment.

The introduction of controls within the network to segregate groups of information services, users and information systems should be considered where different levels of trust or security requirements exist.

Shared networks, and those linking to third parties, require particular access control policy requirements, traffic filtering and routing controls to ensure that computer connections and information flows do not breach the access control policy of business applications.

Network devices should be maintained to the necessary patch levels to ensure their security.

These security policies should be tested from time to time to ensure adequate protections are in place. When new information assets are introduced, the policies should be updated to reflect any changes that may be necessary to secure them. Finally, these policies should be kept “evergreen” based on IT audit assessments and findings.

Access Controls and Identity Management

Controlling access to information systems is essential for the preservation of their confidentiality, integrity and availability. Access control systems must allow authorized use of systems and resources while preventing direct access by unauthorized users. Authorized users may be employees, contractors, third parties or the general public, but should be defined.

Access controls include:

- Administrative controls such as policy, procedures, training, background checks and supervision.
- Logical or technical controls to restrict access to systems and information such as passwords, tokens, encryption, system hardening and protected protocols.
- Physical controls such as locks, cables, security cameras, guards and fences.

These controls are typically applied to Network, Host, Application and Physical access through separate control systems that provide accountability for individuals through mechanisms that require identification authentication. The resulting audit trails are typically monitored to detect anomalies.

Identity Management or User Management is also essential in access control systems since an individual may be identified to multiple systems in different ways. Therefore, the change in an individual's status must appropriately affect the access allowed to that individual. Identity Management is the process and technology used to create, remove or modify an individual's access to systems in an appropriate fashion and in compliance with policy.

Systems Development

As with any component of an information technology environment, information security planners must be involved with “all” aspects of the systems development life cycle management process, regardless of whether the type of system under consideration is a business application or a supporting infrastructure component. It is always most beneficial to incorporate information security requirements up front in the process versus retrofitting it after the system is operational.

Prior to recommending any solutions, consideration must be given to understanding potential threats to the system and the businesses expectations. Based on these analyses, a risk mitigation strategy must be developed and acceptable controls must be identified. Additional details concerning both application development and supporting infrastructure are provided for consideration below:

Application Development: An application that processes sensitive data or requires protection because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure must be provided protection appropriate to its sensitivity. The following should be considered as the minimum controls to be applied to sensitive applications, with additional controls or safeguards to be imposed if appropriate:

- Security requirements should be defined and security specifications approved before starting development or making a change in existing applications.
- Periodic design reviews should be conducted during the developmental process to ensure that the design satisfies the security requirements specified.
- Modifications to applications should be thoroughly tested to ensure application integrity is maintained and implemented controls meet expectations.
- Production data or files should not be used to test application software until software integrity is assured.
- Application software should not be placed in a production status until the system tests have been successfully completed and the application has been properly certified and accredited.

Supporting Infrastructure: Infrastructure that supports applications that process sensitive data must be provided protection appropriate to the sensitivity of the data. The following should be considered as the minimum controls to be applied to the infrastructure, with additional controls or safeguards to be imposed if appropriate:

- Specific security requirements (i.e. intrusion detection, anti-virus, etc.) should be defined for both hardware platforms and operating systems being utilized during the application development phases.
- Appropriate change management and application remediation processes should be implemented to ensure the application of newly released security patches.
- Development and production environments should be continuously monitored to ensure controls put in place during the systems development process function as intented.

Business Continuity Management

Business Continuity Management processes should address an organization's ability to counteract interruptions to normal operations, including:

- Business continuity planning: A business continuity strategy should be developed based on a business impact analysis undertaken by the company’s operating units.

- Business continuity testing: Companies should regularly test their business continuity strategy and revise their documentation in order to ensure the long-term effectiveness of their business continuity strategy.

Regulatory Compliance

With the formation of the Department of Homeland Security and in the wake of recent corporate financial scandals, US based companies have entered into a new era of governmental legislation and legal requirements. Companies may have to establish a regulatory baseline to measure and provide corporate wide visibility to legal compliance requirements. To establish this baseline, many applications, systems and infrastructures will need to be identified and documented.

Corporate information security planners should initiate communication with other corporate business units to ensure proper attention, visibility and guidance is provided concerning electronic information. Key organizations to include are:

- Legal
- Human Resources
- Records Management
- Chief Information Officer
- Privacy Officer

Major legislation has been passed in the following areas. Therefore, all relevant statutory, regulatory and contractual requirements associated with these areas should be identified and documented for each information system.

- Intellectual property (Copyright and Software copyright)
- Safeguarding of organizational records (records retention)
- Data protection and privacy of personal information
- Import and Export (Regulation of cryptographic controls)
- Law enforcement (Rules for evidence)

Standards Compliance and Assurance (Audit)

Security standards and policies can be very effective in safeguarding information assets and employees. However, in order to be effective, the standards and policies need to be enforced. One way to ensure adequate protections are in place is through a standards compliance and assurance audit.

A company’s executive management and Audit Committee have become increasingly interested in how well the company is doing in protecting critical information and the information technology infrastructure from unauthorized access, cyber terrorism and inappropriate use. One of the key assurance indicators utilized is compliance reporting against published policies, standards and procedures based on IT Audit reviews. Unsatisfactory reviews are discussed with management and/or the Audit Committee and require the clear definition of actions to be taken to prevent reoccurrence and clear accountability for ensuring the actions are executed in a timely manner.

Other metrics that can be routinely evaluated and reported as indicators of the quality of health of the Information Security Management process and the associated policies, standards and procedures are the following:

- Internet and E-mail Appropriate Use
- Intrusion Detection Reporting
- Password Strength
- Change Management Compliance
- User Account Administration (Modifications, Additions, Deletions)

Glossary and Terms[13]

Glossary and Terms

Adversary: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

Alert Levels: Describe a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different fixed or variable security measures may be implemented based on the level of threat to the facility.

Asset: An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site.

Asset category: Assets may be categorized in many ways. Among these are:

- Activities/Operations
- Environment
- Equipment
- Facilities
- Hazardous materials (used or produced)
- Information
- People

Computer incident*:* refers to an adverse event in an information system and/or network, or the threat of such an occurrence, which could cause loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include: unauthorized use of another user's account, unauthorized use of system privileges, or execution of malicious code that destroys data. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response teams and should be addressed in the business continuity (contingency) and Disaster Recovery plans. For the purpose of *Incident Response*, therefore, the term "computer incident" refers to an adverse event that is related to Information Security.

Consequences*:* The amount of loss or damage estimated to result from a successful attack against an asset. This should include consideration of casualties, facility damage, environmental impacts, and business interruption as appropriate.

Control center: A location from where a pipeline system is remotely monitored and operated. A control center is typically staffed on a 24/7 basis and is the location for continuous and centralized control of a pipeline system.

Countermeasures: An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

Damage: Impairment of the usefulness or value of information or computer resources (e.g., when a virus scrambles a file or makes a hard disk inoperable).

Delay: A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

Detection: A countermeasures strategy to that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

Deterrence: A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

Energy ISAC*:* The Energy Information Sharing and Analysis Center is an industry organization that provides a secure database, analytic tools, and information gathering and distribution facilities designed to allow authorized individuals to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions.

Event*:* any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash and packet flooding within a network. Events sometimes provide indication that an incident is occurring. In reality, events caused by human error (e.g., unintentionally deleting a critical directory and all files contained therein) are the most costly and disruptive. Computer security-related events are attracting an increasing amount of attention among Information Security Professionals and within the general computing community**.**

Hazard: A situation with the potential for harm.

Intelligence: Information to characterize specific or general threats including the motivation, capabilities, and activities of adversaries.

Intent: A course of action that an adversary intends to follow.

Likelihood of adversary success: The potential for causing a catastrophic event by defeating the countermeasures. Likelihood of adversary success is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

MOC (Management of Change): An internal company management system to define, document, and communicate changes to a process as applicable.

Operator: A person or company who owns and/or operates petroleum facilities. For a person or company who owns or operates pipeline segments and/or facilities, the definition of operator is based on Title 49 CFR Part 195.

Pipeline security plan: Documentation that describes an operator's plan to address security issues and related events including security assessment and mitigation options and includes security condition levels and protective measures to security threats.

Pipeline system: Pipeline or pipeline segment and pipeline facilities such as a terminal, pump station, or other remote site plus the control center.

Response: The act of reacting to detected criminal activity either immediately following detection or post-incident via surveillance tapes or logs.

Risk: A measure of loss in terms of both the incident likelihood of occurrence and the magnitude of the consequences.

Risk management: An overall program consisting of: identifying potential threats to an area or equipment; assessing the risk associated with those threats in terms of incident likelihood and consequences; mitigating risk by reducing the likelihood, the consequences, or both; and measuring the risk reduction results achieved.

Risk mitigation: Those security measures employed at a facility to reduce the security risk to that facility.

Safeguard: Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.[1]

SCADA: Supervisory Control and Data Acquisition used for the remote control and monitoring of a pipeline system

Security plan: A document that describes an operator's plan to address security issues and related events including security assessment and mitigation options and includes security alert levels and response measures to security threats.

Security risk management: An overall plan consisting of: identifying potential security threats to pipeline segments and facilities; assessing the risks associated with those threats in terms of incident likelihood and consequences; mitigating the risk by reducing the likelihood, the consequences, or both; and evaluating the risk reduction results achieved.

Security risk mitigation: Those security measures employed on a pipeline system to reduce the security risk to the pipeline system.

Security Vulnerability Assessment (SVA): A systematic, analytical process in which potential security threats and vulnerabilities to facility or system operations are identified and the likelihood and consequences of potential adverse events are determined. SVAs can have varying scopes and can be performed at varying levels of detail depending on the operator's objectives - see Section 5.

Segment: an aspect of the petroleum industry that represent one of the steps needed to find, produce, process and transport petroleum from where they are found deep below the earth’s surface to where they will be consumed. For purposes of this guidance document, the petroleum segments are defined as petroleum exploration and production, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing.

Should: The term “should” is used in this document to indicate those practices which are preferred, but for which Owner/Operators may determine that alternative practices are equally or more effective or those practices for which engineering judgment is required.

Terrorism: “The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives” - (FBI).

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Threat categories: Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

Vulnerability: Any weakness that can be exploited by an adversary to gain access to and damage or steal an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.

APPENDIX A

FRAMEWORK FOR A COMPUTER SECURITY INCIDENT RESPONSE PLAN

American
Petroleum
Institute

Framework for a *Computer Security Incident Response Plan (CSIRP)*

prepared by:

API IT Security Forum

Security Operations and Best Practices Sub-Team

November 2001

Table of Contents

1.0 Background
2.0 Mission Statement
3.0 Scope
4.0 Incident Types
5.0 Incident Escalation Criteria and Security Level
6.0 Priorities in Incident Handling
7.0 Computer Security Incident Reporting Flow
8.0 CSIRT Team Member Identification and Contact List
8.1 CSIRT Coordinators
8.2 CSIRT On-Site Technical Team Members
8.3 Executive Decision Team Members
8.4 Public Relations Team Members
8.5 Law Enforcement Agency Contacts
9.0 Incident Investigation and Response Steps
9.1 Preparation, Training and Testing
9.2 Event Documentation
9.3 Incident Identification
9.4 Containment
9.5 Eradication
9.6 Recovery
9.7 Follow-up
9.8 Archive
10.0 Resources

Acronyms, Definitions and Terms

APPENDICES
I. Emergency Action Quick Reference Guide
II. CSIRT Incident Response Worksheet
III. User Incident Report Form
IV. Incident Investigation Report Form
V. Incident Tracking
VI. NIPC Incident Reporting Form

1.0 Background

Responding to computer security incidents is generally not a simple matter. This activity requires technical knowledge, detailed communication and close coordination among the personnel assigned to respond to the incident. Incidents over the last few years indicate that, if anything, responding to incidents is increasingly more complex. Intrusions into machines are a serious concern, and increasing sophistication and collaboration among network attackers pose a considerable threat to the integrity and availability of computing resources.

2.0 Mission Statement

The ongoing mission of <Company Name> Computer Security Incident Response Team is to improve the security of the corporate infrastructure and to minimize the threat of damage from malicious activities. The primary goal of the CSIRT is to maintain and/or restore business continuity. This will be accomplished through an ongoing effort to enhance our knowledge base of global security threats with the coordination of all <Company Name> business units. Analysis and a flexible design throughout the CSIRT life cycle will facilitate an increasingly predictive and effective system.

3.0 Scope

This document does not comprise an exhaustive set of incident handling procedures. Because so much is yet to be learned about handling incidents, these guidelines will lack some degree of sophistication and detail. This document contains basic information about responding to incidents, and can be used regardless of hardware platform or operating system. For the specific technical details necessary to implement many of the recommendations in these guidelines, consult your system administrator or vendor.

4.0 Incident Types

Compromise of Integrity—An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred causing accidental or malicious alteration or destruction of information (e.g., when a virus infects a file).

Denial of Resources—An action(s) which prevent any part of any equipment (software, firmware, and hardware) of an interconnected system or subsystem used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data from functioning in accordance with its intended purpose. When an attacker sets a system to single user mode, locking out all other users.

***Disruptions of Service*—**Users rely on services provided by network and computing services. Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

***Espionage*—**Espionage is stealing information to subvert the interests of a corporation or government. Many of the cases of unauthorized access to U.S. Government systems during Operation Desert Storm and Operation Desert Shield were the manifestation of espionage activity against the United States.

Hoaxes**—**Hoaxes occur when false information about incidents or vulnerabilities is spread. In early 1995, for example, several users with Internet access distributed information about a virus called the Good Times Virus, even though the virus did not exist.

Intrusion—An action that attempts to or successfully compromises the integrity, confidentiality or availability of information or computer resources.

Malicious code attacks**—**Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs. Malicious code is particularly troublesome in that it is typically written to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem.

Misuse—The use of a computer system by an authorized or unauthorized user for other than its intended purpose or an activity engaging tools and techniques known to exploit system vulnerabilities. For example, using a corporate resource to operate a personal business, using tools and techniques that exploit system vulnerabilities or unauthorized use of an account.

Penetration**—**The successful unauthorized access to a computer network or system.

***Unauthorized access* -** Unauthorized access encompasses a range of incidents from logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage. Unauthorized access could also entail access to network data by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point.

Unauthorized utilization of services—It is not necessary to access another user's account to perpetrate an attack on a system or network. An intruder can access information or plant Trojan horse programs by misusing available services. Examples include using the network file system (NFS) to mount the file system of a remote server machine, the VMS file access listener to transfer files without authorization, or inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain.

5.0 Incident Escalation Criteria and Security Level

Escalation is often confused with prioritization. Although the activities are similar, escalation is concerned with further raising the importance of an activity regardless of its priority. There is a continuous need to review the criteria and to adapt to changing needs and new developments, such as new attack styles and incident types. The initial Severity Level assessment will be made by the triage coordinator and documented on the Computer Security Incident Report.

By its very nature, incident escalation is driven by similar issues as those involved in the incident prioritization. However escalation criteria can be applied to the incident response service as a whole as well as to a given incident. The following table and associated criteria will be used to help define an incident’s severity level.

Incident Severity Level	
Severity Level	**Evaluative Criteria**
1	Incident could have long-term effects on business; incident affects critical systems.
2	Incursion on non-critical system; detection of precursor to a focused attack; believed threat of an imminent attack.
3	Threat of a future attack; detection of reconnaissance.
4	Unsubstantiated rumor of security incident.

6.0 Priorities in Incident Handling

It is important to prioritize the CSIRT Team's actions to be taken during an incident in advance of the time an actual incident occurs. Sometimes an incident may be so complex that it is impossible to respond to everything at once; priorities are essential. Priorities will vary from one organization to the next. The following priorities are suggested as a starting point for defining an organizations response. Human life and national security should take first precedence and it is generally more important to save data than to save system hardware and software.

Priority one—protect human life and people's safety: human life always has precedence over all other considerations.

Priority two—protect company confidential and/or sensitive data; national safety and security is second only to protecting human life.

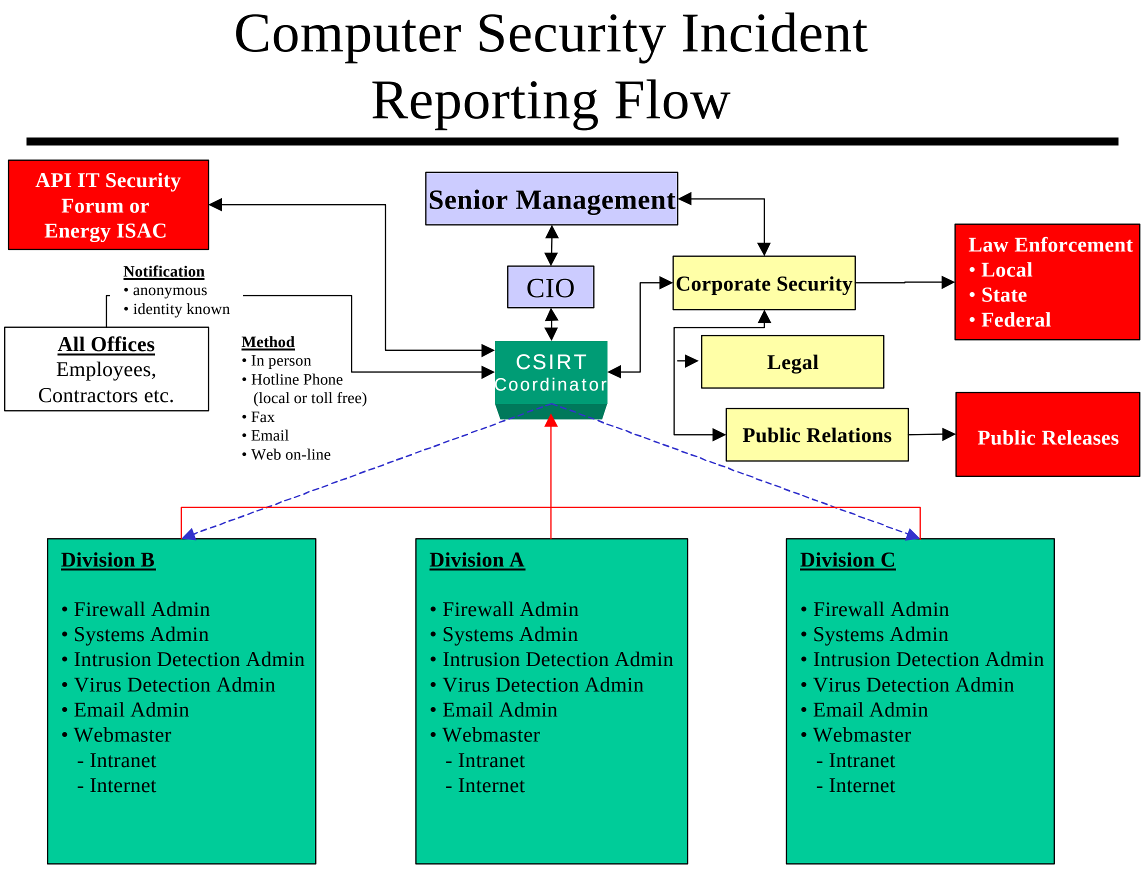
Priority three—protect other data, including proprietary, scientific and managerial data, because loss of data is costly.

Priority four—prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.); damage to systems can result in costly down time and recovery.

Priority five—minimize disruption of computing resources; it is better in many cases to shut a system down or disconnect from a network than to risk damage to data and/or systems.

7.0 Computer Security Incident Reporting Flow

7.1 Information Security is the responsibility of every employee and contractor that uses <Company Name> information technology resources.



Computer Security Incident Reporting Flow

API IT Security Forum or Energy ISAC

Senior Management

CIO

Corporate Security

Law Enforcement
- Local
- State
- Federal

Notification
- anonymous
- identity known

All Offices
Employees, Contractors etc.

Method
- In person
- Hotline Phone (local or toll free)
- Fax
- Email
- Web on-line

CSIRT Coordinator

Legal

Public Relations

Public Releases

Division B
- Firewall Admin
- Systems Admin
- Intrusion Detection Admin
- Virus Detection Admin
- Email Admin
- Webmaster
  - Intranet
  - Internet

Division A
- Firewall Admin
- Systems Admin
- Intrusion Detection Admin
- Virus Detection Admin
- Email Admin
- Webmaster
  - Intranet
  - Internet

Division C
- Firewall Admin
- Systems Admin
- Intrusion Detection Admin
- Virus Detection Admin
- Email Admin
- Webmaster
  - Intranet
  - Internet

7.2 When an incident or infraction is noted, whether known or suspect, it must be immediately reported to the CSIRT Coordinator and the employee’s supervisor (incident may also be reported to Help Desk, who in turn reports incident to CSIRT Coordinator).

7.3 Ideally, the identity of the individual reporting the incident is provided when the report is filed with the CSIRT. However, incidents may also be reported anonymously.
Note: Confidentiality will be strictly maintained.

7.4 The preferred communication methods for reporting an incident to the CSIRT are: in person, hotline phone number (local or toll free), Fax, Email and Web-based. In the event of a system compromise, electronic-based (email, web) communications is not recommended unless it is encrypted since such methods of communication are easily intercepted.

7.5 Incidents detected by system administration personnel will be immediately reported direct to the CSIRT.

7.6 The CSIRT Coordinator will assess the severity of a reported incident and notify the CIO, other division IT Security Advisors and IT Management, as necessary.

7.7 The CIO will report incident summary information to senior management.

7.8 The CSIRT Coordinator will notify Corporate Security of the incident.

7.9 Senior Management, Corporate Security, Legal and Public Relations will determine whether to contact law enforcement agencies, issue official press releases, or contact members of the API IT Security Forum. *Note: Any incident determined to be a violation of local, state, or federal law must be reported to the appropriate law enforcement agency.*

8.0 CSIRT Team Member Identification and Contact List (Identify the CSIRT Team personnel—subject matter experts from different departments: Networking, System Administration, IT Security- and assign roles).

8.1 ***CSIRT Coordinators***. CSIRT Coordinators serve as the central liaison to conduct an initial triage assessment to determine which team members are deployed in response to a reported incident. The CSIRT Coordinators also manage the response teams' activity, escalate incident notification to Executive Management and Corporate Security, coordinate communications with team members for other divisions, coordinate activities during an incident investigation and coordinate efforts to document the incident.

	1	**2**	**3**	**4**	**5**
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.2 ***CSIRT On-Site Technical Team Members***. The On-Site Team members are the subject matter experts that are deployed to the location(s) of the incident. They are responsible for securing the area, surveying the situation and initiating the containment, eradication, recovery and resumption of normal business operations. Team members should have special skills and experience in handling incidents of varying types (e.g. Unix, Microsoft NT/Win2K, Virus eradication etc.)

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.3 ***Management Decision Team Members***. This CSIRT Coordinator translates the technically oriented assessments of the On-Site CSIRT Team into recovery steps for the Management Decision team to determine business decisions affected by the incident and direct actions to be taken by the team. The Management Decision Team works with the organization’s public affairs, corporate security and legal departments to coordinate information statements that would be provided to stock holders, outside organizations or public media. They are also responsible for communicating the status of the incident with corporate executives.

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.4 ***Public Relations Team Members***. The Public Relations team is responsible for answering questions from the public regarding corporate activities. When a security-related incident occurs, it is this team's responsibility to disseminate appropriate information to the public.

	1	**2**	**3**	**4**	**5**
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.5 ***Law Enforcement Agency Contacts*** (local, state and federal).

Agency/Name	Agency Functions and Responsibilities	**Phone #**	**Phone #**	**E-mail**

9.0 Incident Investigation and Response Steps

9.1 ***Incident handling*** starts with *preparation, training and testing*. Preparation involves establishing a program to identify critical resources and information that if disrupted, damaged or lost would impact the organizations ability to conduct business. Once the critical resources and information have been identified, the organization must determine the necessary protection controls and implement them. Additional steps include preparing incident handling guidelines or contingency response plans to minimize the impact of an incident when one occurs, training staff to respond to various incidents and testing the response capability. Paragraphs 9.2 – 9.8 are the generic life-cycle steps of Incident Investigation and Response. Each organization should develop appropriate processes to handle security breaches (perimeter and firewall intrusions, operating system attacks, Distributed Denial of Service (DDoS) attacks, malicious code attacks etc. These processes should be considered living entities that require continual updates and improvement.

9.2 ***Event documentation*** is a critical aspect of incident investigation and handling. Documentation directs the investigation life cycle. Without an accurate and verifiable account of events, the investigation will be rendered useless. This process begins with the Computer Security Incident Report and the assignment of a relevant Incident Tracking Number.

9.3 ***Incident identification*** involves a quick-response triage assessment of the situation to determine exactly what the problem is and the severity of it.

9.3.1 Systems should be checked for the following symptoms:

9.3.1.1 System crashes
9.3.1.2 New user accounts

9.3.1.3 System access points
9.3.1.4 New files
9.3.1.5 Accounting discrepancies
9.3.1.6 Changes in file lengths or dates
9.3.1.7 Attempts to write to system files
9.3.1.8 Modified or deleted data
9.3.1.9 Unexplained poor system performance
9.3.1.10 Other anomalies

9.3.2 Identify and document all evidence.

9.3.3 Study and review the system and network logs.

9.4 ***Containment*** should occur only if the indications observed during the Identification stage conclusively show that an incident has or is occurring. The primary goal is to minimize the breadth of the incident and isolate it from causing wide-spread damage.

9.4.1 Do not alter the system until an image backup is performed.

9.4.2 Do not try to contact the attacker with ping, telnet or other tools.

9.4.3 Backup the system to new media and safely store it before proceeding.

9.4.4 Determine the necessity of disconnecting and isolating a system component(s) from other system components.

9.5 ***Eradication*** is the time in the process when infected files are fully deleted or the system(s) is restored to its normal operational state.

9.6 ***Recovery*** involves returning the system back to normal.

9.6.1 Change passwords on compromised system.

9.6.2 Consider changing system’s IP address or name.

9.6.3 Restore the system from the most recent clean backup.

9.7 ***Follow-up*** involves performing a post-incident analysis. Document exactly what happened and when.

9.7.1 After recovering, evaluate the system again to verify normal operational functions.

9.7.2 Perform system and network vulnerability assessments using special tools.

9.7.3 Study the attack and try to learn how it was executed.

9.7.4 If vulnerability is determined, check if it exists on other similar systems within the enterprise.

9.7.5 Evaluate the incident response process and document lessons learned. Follow-up activities may include asking some of the following questions:

- Was there sufficient preparation for the incident?
- Did detection occur promptly? If not, why not?
- Could additional tools have helped the detection and eradication process (how to avoid further exploitation)?
- Was the incident sufficiently contained?
- Was communication adequate or could it have been better?

- What practical difficulties were encountered?
- How much is the associated monetary cost? (personnel time, time to restore systems, etc.)
- How much did the incident disrupt ongoing operations?
- Were any data irrecoverably lost, and, if so, what was the value of the data?
- Was any hardware damaged?

9.7.6 Determine the retention period for the documentation.

9.7.7 Review external communication flow and SVA process.

9.8 ***Archive*** the incident file and all supporting evidence related to the investigation in an access-controlled environment in the event it is needed to support legal or other action. Strict “Chain of Custody” must be maintained.

10.0 Resources

Energy Information Sharing and Analysis Center (Energy ISAC) http://energyisac.com/

National Security Agency (NSA) Glossary of Terms, http://www.sans.org/newlook/resources/glossary.htm

National Infrastructure Protection Center “Incident Reporting Form (Print Version – pdf file) http://www.nipc.gov/incident/incident.htm

National Institute of Standards and Technology “Establishing a Computer Security Incident Response Capability” NIST Pub 800-3, November 1991 http://csrc.nist.gov/topics/incidentNIST/index.htm

The SANS Institute “Incident Handling Step By Step” version 1.5, May 1998 http://www.sans.org

University of California, Lawrence Livermore National Laboratory “Responding To Computer Security Incidents: Guidelines for Incident Handling”. Schultz, Eugene Jr.; Brown, David S; Longstaff, Thomas A., July 23, 1990.

Framework for a Computer Security Incident Response Plan (CSIRP)

Acronyms, Definitions and Terms

ACRONYM**—**A Contrived Reduction Of Nomenclature Yielding Mnemonics

API**—**American Petroleum Institute

Computer incident—refers to an adverse event in an information system and/or network, or the threat of such an occurrence, which could cause loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include: unauthorized use of another user's account, unauthorized use of system privileges, or execution of malicious code that destroys data. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response teams and should be addressed in the business continuity (contingency) and Disaster Recovery plans. For the purpose of *Incident Response*, therefore, the term "computer incident" refers to an adverse event that is related to Information Security.

Damage**—**Impairment of the usefulness or value of information or computer resources (e.g., when a virus scrambles a file or makes a hard disk inoperable).

Energy ISAC**—**The Energy Information Sharing and Analysis Center is an industry organization that provides a secure database, analytic tools, and information gathering and distribution facilities designed to allow authorized individuals to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions.

Event—any observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash and packet flooding within a network. Events sometimes provide indication that an incident is occurring. In reality, events caused by human error (e.g., unintentionally deleting a critical directory and all files contained therein) are the most costly and disruptive. Computer security-related events are attracting an increasing amount of attention among Information Security Professionals and within the general computing community.

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDICES

APPENDIX I

Emergency Action Quick Reference Guide

Step #1: Remain calm. Even a fairly mild incident tends to raise everyone's stress level. Communication and coordination become difficult. Your calm can help others avoid making critical errors.

Step #2: Take good notes. Keep in mind that your notes may become evidence in court. Make sure you answer the four Ws - Who, What, When, and Where- and, for extra credit, Why and How. You may find a small hand-held tape recorder to be a valuable tool.

Step #3: Notify the right people and get help. Begin by notifying your security coordinator and your manager and asking that a coworker be assigned to help coordinate the incident handling process. Get a copy of the corporate phonebook and keep it with you. Ask your helper to keep careful notes on each person with whom he or she speaks and what was said. Make sure you do the same.

Step #4: Enforce a "need to know" policy. Tell the details of the incident to the minimum number of people possible. Remind them, where appropriate, that they are trusted individuals and that your organization is counting in their discretion. Avoid speculation except when it is required to decide what to do. Too often the initial information in an incident is misinterpreted and the "working theory" has to be scrapped.

Step #5: Use out of band communications. If the computers may have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail, talk, chat, or news; the information may be intercepted by the attacker and used to worsen the situation. When computers are being used, encrypt all incident handling e-mail.

Step #6: Contain the problem. Take the necessary steps to keep the problem from getting worse. Usually that means removing the system from the network, though management may decide to keep the connections open in an effort to catch an intruder.

Step #7: Make a backup of the affected system(s) as soon as practicable. Use new, unused media. If possible make a binary, or bit-by-bit backup.

Step #8: Get rid of the problem. Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.

Step #9: Get back in business. After checking your backups to ensure they are not compromised, restore your system from backups and monitor the system closely to determine whether it can resume its tasks.

Step #10: Learn from this experience, so you won't be caught unprepared the next time an incident occurs.

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDIX II

CSIRT Incident Response Worksheet Sample

The incident response worksheet is designed for use by the response team to ensure uniformity of the documented information gathered by each team member. This will make the review of information by the CSIRT Coordinator easier. Also keep in mind that an incident should be investigated as though it were going to be presented as evidence for legal action.

Date MM/DD/YY		
ncident Tracking Number 000X – YYY/MM/DD/HH:MM		
ime	Observation	Action Taken

NAME (print)	SIGNATURE
1)	
2)	
3)	

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDIX III

User Incident Report Form Sample

The user incident report form should be used by the general user population to report all suspected incidents. At a minimum, the following information must be obtained, whether the user submits the report or the report is filled out by a third party.

Date:	
Name:	
Department:	
Phone Number:	
Nature of Incident:	<Describe briefly what you observed, where the incident occurred and name(s) of persons involved (if applicable)>

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDIX IV

Incident Investigation Report Form Sample

The incident investigation report form is a detailed report that provides details of the incident and investigative information. The form is initiated by the CSIRT Coordinator and periodically updated throughout the duration of the incident investigation until closure. Depending on the nature and severity of the incident, this report may remain open for as little as an hour or as long as several days or weeks.

Report Date August 1, 2001	Incident Tracking Number 000X - YYYY/MM/DD/HH:MM

Reported By:

Name		Date / Time Reported	
Title			
Organization		Phone Number	
Description			
Details	**August 1, 2001:**		
Open Actions			
August 1, 2001: **The following items remain open Actionee**			
Closure			

Submitted By:

Name		Phone Number	
Title			
Organization			

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDIX V

Incident Tracking Form Sample

The incident tracking form is a spreadsheet or database for the purpose of maintaining a log of incidents reported during the year. Each organization should decide what the severity or frequency guidelines are for documenting this information. For instance you may not want to track every virus detected and eradicated.

					Type of Incident						
Incident Tracking Number	**Date Opened**	**Date Closed**	**Description**	**Loc.**	**Access**	**e-mail**	**Unauthorized Use**	**Loss or Theft**	**Intrusion**	**Denial of Service**	**Other**
000X – YYYY/ MM/ DD/ HH:MM											

Framework for a Computer Security Incident Response Plan (CSIRP)

APPENDIX VI

NIPC Incident Reporting Form

The National Infrastructure Protection Center (NIPC) incident reporting form may be found at http://www.nipc.gov/incident/incident.htm. The NIPC was established to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response to threats or attacks against the critical infrastructures of the United States. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services.

References

[1] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) *Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites*, August, 2002

[2] “The Sociology And Psychology Of Terrorism: Who Becomes A Terrorist And Why?”, A Report Prepared under an Interagency Agreement by the Federal Research Division, ,Rex A. Hudson, et. al., Library of Congress, September,1999.

[3]*Patterns of Global Terrorism 2001*, May, 2002, U. S. State Department

[4] Testimony Before the Senate Committee on Governmental Affairs, United States General Accounting Office, October 31, 2001, “A Risk Management Approach Can Guide Preparedness Efforts,” Statement of Raymond J. Decker, Director, Defense Capabilities and Management.

[5] CCPS, 2002

[6] The National Infrastructure Protection Center ,”Suggested Guidance on Protective Measures”, Information Bulletin 03-002, February 7, 2003.

[7] COMDTPUB P 16700.4, U.S. DOT, USCG, NVIC 11-02, 13 January 2003.

[8] Ibid, AIChE

[9] Ibid, AIChE

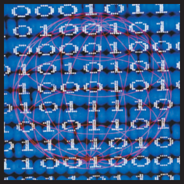
[10] Ibid, AIChE

[11] Ibid, AIChE

[12] National Infrastructure Protection Center, Homeland Security Information Update, “Potential Al-Qa’ida Operational Planning,” Information Bulletin 03-001, February 7, 2003.

[13] Ibid, AIChE

API Creative Services: 23055 | 05.03



Petroleum Refineries

Liquid Petroleum Pipelines

Petroleum Products Distribution and Marketing

Oil and Natural Gas Production Operations

Marine Transportation

Cyber/Information Technology for the Petroleum Industry

Additional copies are available through Global Engineering Documents at 1-800-854-7179 or 303-397-7956.

Information about API Publications, Programs and Services is available on the web at www.api.org.

American
Petroleum
Institute

1220 L Street, NW
Washington, DC 20005-4070
USA
202-682-8000

Product No. OS0001