Third 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 2005

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

Third 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 2005

SPECIAL NOTES

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

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 health and safety risks and precautions, nor undertaking their obligations under local, state, or federal laws.

Information concerning safety and health risks and proper precautions with respect to particular materials and conditions should be obtained from the employer, the manufacturer or supplier of that material, or the material safety data sheet.

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. Sometimes a one-time extension of up to two years will be added to this review cycle. This publication will no longer be in effect five years after its publication date as an operative API standard or, where an extension has been granted, upon republication. Status of the publication can be ascertained from the API Standards department telephone (202) 682-8000. A catalog of API publications, programs and services is published annually and updated biannually by API, and available through Global Engineering Documents, 15 Inverness Way East, M/S C303B, Englewood, CO 80112-5776.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this standard or comments and questions concerning the procedures under which this standard was developed should be directed in writing to the Director of the Standards department, American Petroleum Institute, 1220 L Street, N.W., Washington, D.C. 20005. Requests for permission to reproduce or translate all or any part of the material published herein should be addressed to the Director, Business Services.

API standards are published to facilitate the broad availability of proven, sound engineering and operating practices. These standards are not intended to obviate the need for applying sound engineering judgment regarding when and where these standards should be utilized. The formulation and publication of API standards is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

FOREWORD

This document is intended to offer security guidance to the petroleum industry. 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 company 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.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any federal, state, or municipal regulation with which this publication may conflict.

Suggested revisions are invited and should be submitted to API, RASA department, 1220 L Street, NW, Washington, DC 20005.

TABLE OF CONTENTS

Figures

Tables

EXECUTIVE SUMMARY

Safe and reliable energy is a vital link in the nation's critical infrastructure. Petroleum products play an important role in our national economy, national security and are integral to the American way of life. As such, security has always been and continues to be a priority across the petroleum industry. The American Petroleum Institute is the petroleum industry's primary trade association. API provides a forum for the industry to come together and discuss important issues with Government, develop industry guidelines and share best practices. From developing industry safe operating practices, to assessing vulnerability at facilities, to coordinating emergency response training, API and its members are committed in taking a leadership role to ensure the safety and security of our workers, our surrounding communities and to provide a transparent flow of reliable energy that we have all come to expect in our daily lives.

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, government and private companies to prepare this 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, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing. This document provides general security guidance and other reference data on applicable regulatory requirements, which can be tailored to meet the differing security needs of the petroleum industry.

This security guidance is by necessity general in nature. It is intended to provide an overview of security issues in the petroleum industry and provide general guidance on effective policies and practices. Individual companies, working cooperatively with local officials, are best suited for conducting detailed assessments of their own facilities and assets and determining how to protect them. This is because both potential threats and appropriate security measures vary based on size, location, facility type and existing security measures already in place. Due to the sensitive nature of this information, security screenings, site-security plans and vulnerability assessments should be protected under the company's confidentiality program to ensure that detailed information regarding vulnerabilities, threats and countermeasures is available only to those who need such information.

Security Guidelines for the Petroleum Industry

1.0 Introduction

In order to assist petroleum companies evaluate and respond to security threats, the American Petroleum Institute has:

- Assessed the general types of security risks to the public and to petroleum supplies that each sector may face due to terrorism;
- Identified existing standards, recommended practices, guidance and other operational practices, as well as ongoing initiatives that may mitigate these risks;
- Developed guidance on conducting Security Vulnerability Assessments (SVA)[a] in the petroleum and petrochemical industries;
- Developed Recommended Practices for security for offshore oil and gas operations.[b]
- Worked with the Federal Government, other industry associations and petroleum companies to prepare appropriate guidance.

1.1 Scope and Objective

The objective of this document is to provide general guidance to owners and operators of U.S. domestic petroleum assets for effectively managing security risks and provide a reference of certain applicable Federal security laws and regulations that may impact petroleum operations.

Domestic petroleum assets are widely distributed, consisting of over 300,000 producing sites, 4,000 offshore platforms, 600 natural gas processing plants, 160,000 miles of liquid pipelines, numerous crude oil and liquefied natural gas (LNG) offloading ports and terminals, 144 refineries, 1,400 finished product terminals, 7,500 bulk stations and 170,000 gasoline retail stations. The vast majority of these assets are small and geographically remote and do not present a significant security risk to the national economy, national security or public safety. However, the petroleum industry supports taking prudent measures to effectively minimize security risks posed by acts of terrorism where warranted.

Certain petroleum facilities are covered by the Maritime Transportation Security Act of 2002 (MTSA), which was signed into law on November 25, 2002. In compliance with MTSA, the U.S. Coast Guard has promulgated federal rules under 33 *CFR* Subchapter H, Parts 101 – 106 that cover port, OCS and vessel security. These regulations require certain vessels and port facilities that could be involved in a transportation security incident prepare a vessel or facility security plan and submit it to the USCG. See Appendix A for a reference table of Federal security regulations that affect the U.S.

1.2 Organization of the Document

This document is organized into seven chapters plus three Appendix items for reference. Chapter 1.0 describes the objectives, intended audience, and scope of the guidance and the various references for other security regulations. Chapter 2.0 includes an overview of terrorism and the petroleum industry. Chapter 3.0 describes a process for a threat assessment including the use of security intelligence and threat-based countermeasures systems such as the Department of Homeland Security Alert System (HSAS) and the USCG Maritime Security (MARSEC) levels. Chapter 4.0 describes the elements of a

[a] American Petroleum Institute/National Petrochemical and Refiner's Association Guidance "Security Vulnerability Assessment Methodology, October, 2004"

[b] API RP 70 *Security for Offshore Oil and Natural Gas Operations,* First Edition, March 2003 and RP 70I *Security for International Oil and Natural Gas Operations*, First Edition, May 2004.

security plan and provides a plan outline. Chapter 5.0 includes an overview of security vulnerability assessment. Chapter 6.0 includes security conditions and potential response measures. Chapter 7.0 provides an overview of information (cyber) security. The Appendix items provide useful reference information such as a matrix of certain Federal laws and regulations on security and a glossary of terms and references used to develop this document.

1.3 Underlying Basis of this Guidance

Owners and operators in the petroleum industry can enhance the security of their assets and continuity of business operations through the effective management of security risks. By considering site-specific circumstances, security risks can be managed through a risk-based, performance-oriented management systems approach. The foundation of a security management systems approach is to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of countermeasures provided to mitigate the threats. Security Vulnerability Assessment (SVA) is a management tool that is flexible and adaptable to a wide range of applications and can be used to assist management is identifying and prioritizing security risks and determining the appropriate type and level of protection required at the local asset level.

The need for and type of security enhancements will be determined based on site-specific factors such as the degree of the threat, the degree of vulnerability, the potential consequences of a security event, and the attractiveness of an asset to an adversary. In the case of the terrorist threat, higher-risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of potential consequences, where assets are vulnerable and the threat is great. In these high-risk situations, security enhancements/countermeasures should be considered that reduce one or several of these items to an acceptable level.

Appropriate strategies for managing security risk can vary widely depending on site-specific factors such as the type of facility (fixed or mobile/remote or urban), the operation involved, the type of substances being stored and processed, and the threats facing the facility. As a result, this guidance does not prescribe specific security measures but provides a means of identifying, analyzing, and reducing vulnerabilities based on the unique needs of the location. Each facility should be evaluated individually by management using the best judgment of applicable practices and appropriate security risk management decisions should be made commensurate with the risks. This recognizes that there isn't a uniform approach to security in the petroleum industry, and that resources should be used effectively to reduce high-risk situations on a priority basis. It is recognized that while all security risks cannot be completely eliminated it can be significantly reduced through implementing an effective security risk management program. 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 as applicable. Owner/Operators can also obtain and share intelligence, coordinate training, and utilize other resources to help deter attacks and to manage emergencies.

1.4 Other Guidelines and Security References

API has developed this guidance for the petroleum industry as a reference to be used with other available sources. This document does not attempt to provide an all-inclusive list of security considerations, but more as a basis for what might be considered when evaluating and implementing security measures. Additionally, it is recognized that certain information included in a security program needs to remain confidential. Petroleum companies should consider a confidentiality

program to understand what information can be shared and what should remain confidential. Other available resources on security include:

- American Petroleum Institute RP 70, *Security for Offshore Oil and Natural Gas Operations*, 1st Ed., April 2003.
- American Petroleum Institute RP 70I, *Security for Worldwide Offshore Oil and Natural Gas Operations*, 1st Ed., May 2004.
- American Petroleum Institute Std 1164, *SCADA Security*, 1st Ed., September 2004.
- American Petroleum Institute / National Petrochemical and Refiners Association, "Security Vulnerability Assessment Methodology," October 2004.
- American Chemistry Council, "Site Security Guidelines for the U. S. Chemical Industry," 2001.
- American Chemistry Council, "Implementation Resource Guide for Responsible Care Security Code® of Management Practices: Value Chain Activities," 2003.
- American Chemistry Council, "Transportation Security Guidelines for the U.S. Chemical Industry," 2001.
- 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]
- DOT, Office of Pipeline Safety, "Pipeline Security Information Circular, Information of Concern to Pipeline Security Personnel, *Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities*," September 5, 2002.
- Sandia National Laboratories, "Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)".
- U.S. Coast Guard NVIC 11-02 (and other NVICs).

In addition to these references, owners and operators should be aware of applicable local and national laws and regulations. See the reference table included in Appendix A for a list of final security regulations impacting the petroleum industry that were enacted prior to the release of this document.

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." The number of international terrorist incidents has increased in recent years and the potential threat posed by terrorists has increased[2]. All sectors of the U. S. economy are potentially subject to these illicit activities.

2.2 Threat to the Petroleum Industry

Reports from the Department of Homeland Security (DHS), the U. S. Department of State[3], the Federal Bureau of Investigation (FBI), have indicated that the petroleum industry may be a target of terrorism due to the inherent nature of the products used and its importance on the national infrastructure. Specifically, the petroleum industry may be a target for terrorism due to the following characteristics:

- The physical and chemical properties of the products handled at petroleum sites
- The importance of petroleum to the national economy
- The importance of petroleum to national security
- The symbolism of the industry as a cornerstone of capitalism and western culture.

Fortunately there is little experience with actual terrorism in the U.S. However, this fact poses a challenge for domestic petroleum owners/operators. As a result, government and industry are working together to better protect the national infrastructure and our national security. Facility owners and operators should establish a close relationship with various sources of intelligence, both at the local and national levels. Certain key sources of intelligence include: the local law enforcement, regional FBI offices, emergency response organizations, USCG Office of Intelligence and Investigations and the Energy ISAC. By providing certain basic awareness training, employees and members of the pubic can act as the watchful eyes and ears for the company by reporting suspicious activity in and around the facility. Lastly, most domestic petroleum companies operate internationally and in remote regions of the world where security has historically been a significant concern. Domestic firms should where possible, tap that experience to help strengthen its domestic security program.

3.0 Threat Assessment

3.1 The Value of Threat Assessment

Threat assessment is an important part of a security management system. This chapter describes a threat assessment approach as part of a security management system process. In chapter 5.0 the use of threat assessment in the SVA is explained in greater detail.

A threat assessment is used to evaluate the likelihood of an attack 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, intent, and impact.

Threat assessment is a process that should be systematically performed and kept current to be useful. 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 localized 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.

Certain 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. It should be noted that other agencies and groups (e.g., the USCG MARSEC Levels) have established threat levels other than HSAS. While these systems differ in the number and description of the threat levels, they provide essentially the same information and may be correlated. The threat assessment determines the estimated general threat level, which forms a baseline. Then

intelligence and threat assessment helps to evaluate situations as they develop. Depending on the increased threat level, different security measures above baseline may be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated 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.

Intelligence and law enforcement agencies assess the foreign and domestic 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. However, it should be understood that much of this information is classified and will not be readily accessible without a security clearance. A company should attempt to identify threats in order to decide how to manage risk in a cost-effective manner. Many 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, where such information is available and accurate;
2. the recognition and analysis of their intent, 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 have the intent and capability 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, and 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 national, regional, and local industrial groups 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 threat assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat.

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 given additional information and assessment of vulnerabilities.

3.3 Security Alert Level Systems

3.3.1 Introduction

Flexibility provides the basis of operational security due to the dynamic threat environment and the need to apply variable security measures are employed accordingly. Alert levels describe a progressive measure of the likelihood of terrorist actions, from normal to imminent risk of attack or action, based on government or company intelligence information. There are three relevant alert level systems that have been developed by the government and international sources to warn of potential acts of terrorism:

1. **Homeland Security Advisory System (HSAS)**—This five-level alert system is based on the National Threat Advisory System developed by the Department of Homeland Security.
2. **Maritime Security Levels (MARSEC)**—This three-level alert system was developed by the U.S. Coast Guard for use by marine vessels, ports and port facilities.
3. **International Ship and Port Facility Security (ISPS) Code**—This three-level alert system is similar to the MARSEC system and applies to foreign flagged vessels and ports.

The purpose of these systems is to provide clear information to both the private and public sectors about the potential for a terrorist action and to help implement appropriate response measures during a threat crisis.

3.3.2 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. Section 6 of this publication provides an in-depth discussion of specific protective measures that owners/operators of petroleum facilities should consider when the national alert level changes.

Following is the HSAS five level alert system and their general protective measures.

Table 3.1—Homeland Security Alert System
Severe Condition—Red: Severe risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
o Assign emergency response personnel and pre-position specially trained teams;
o Monitor, redirect or constrain transportation systems;
o Close facilities;
o Increase or redirect personnel to address critical emergency needs.
High Condition—Orange: High risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
o Coordinate necessary security efforts with armed forces or local law enforcement;
o Take additional precautions at public events;
o Prepare to work at an alternate site or with a dispersed workforce;
o Restrict access to essential personnel only.
Elevated Condition—Yellow: Significant risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
o Increase surveillance of critical locations;
o Coordinate emergency plans with local jurisdictions;
o Assess further refinement of protective measures within the context of the current threat information;
o Implement, as appropriate, contingency and emergency response plans.
Guarded Condition—Blue: General risk of terrorist attacks. In addition to the previous protective measures, the following may be applied:
o Check communications with designated emergency response locations;
o Review and update emergency response procedures;
o Provide the surrounding community with necessary information.
Low Condition—Green: Low risk of terrorist attacks. The following general protective measures may apply:
o Refine and exercise preplanned protective measures;
o Ensure personnel receive training on HSAS, corporate and facility specific protective measures;
o Regularly assess facility vulnerability and take measures to reduce them.

The National Infrastructure Protection Center, U.S. Coast Guard and other agencies publish guidance on protective measures that are recommended for the different threat levels[6].

3.3.3 U. S. Coast Guard Maritime Security Levels

The U.S. Coast Guard has developed a three-level Maritime Security (MARSEC) alert system for use by marine vessels, certain energy facilities 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 used 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 essentially 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 is 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, if necessary, 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]

Section 6.0 provides in-depth discussion of specific protective measures that owners/operators of petroleum assets may consider when the national alert level changes.

3.3.4 International Ship and Port Facility Security (ISPS) Alert Levels

The ISPS code is a three-level alert system similar to the MARSEC system.

Security level 1: (Normal) The level at which the ship or port facility normally operates. Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

Security level 2: (Heightened) The level applying for as long as there is a heightened risk of a security incident. Security level 2 means the level where appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

Security level 3: (Exceptional) The level applying for the period of time when there is the probable or imminent risk of a security incident. Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Setting security level 3 should be an exceptional measure, used only when credible intelligence indicates that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from level 1, through level 2 to level 3, it is possible that the security levels will change directly from security level 1 to security level 3.

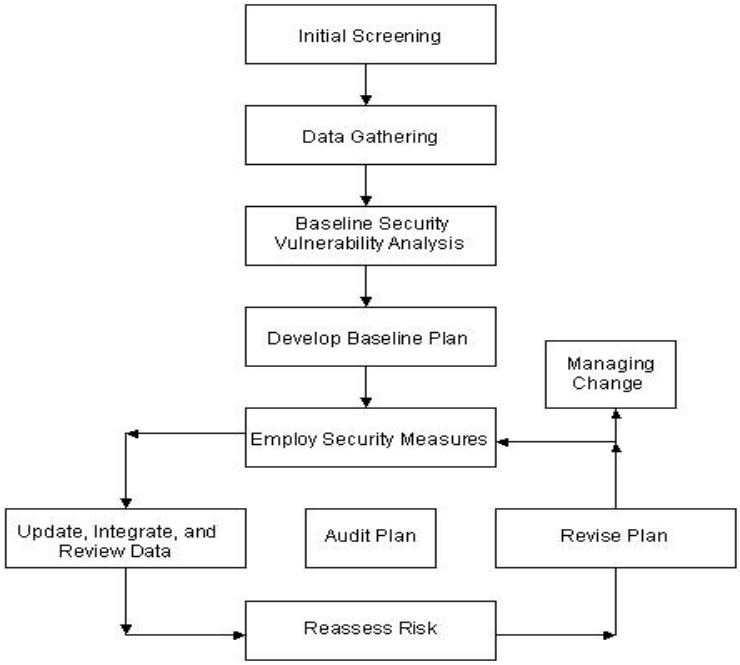
4.0 The Security Management System Process

There is a significant variation in the detail and complexity associated with different SVA methods. Many companies without a formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Companies may find that a screening approach is the most practical means to prioritize facilities for SVA. Depending on the nature of the location and its operations, not all facilities may require a formalized SVA and security plan.

Each owner/office should establish a security management system to effectively manage security risks as appropriate. Since all petroleum operations have unique characteristics, the management system should provide for flexibility and continuous improvement due to changing conditions. However, an effective security management system should have a solid base of several essential elements.

Figure 4.1 illustrates an example of a security management system. The decision flow provides a common process to develop and maintain a site-specific security plan. Owner/operators should consider their unique security risks and then assess those risks to ensure that the plan effectively addresses the highest risks first. There are many different approaches to implementing the elements identified in Figure 4.1, ranging along a continuum from simple to complex. There is no "best" approach that is applicable to all petroleum operations for all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

Figure 4.1—Security Management System Process



4.1 Initial Screening

An initial evaluation should be conducted prior to launching a formal SVA. The screen should evaluate petroleum facilities at a "systems level" (high level) by considering the potential economic ramifications, public safety and health impacts, national security and the effects on the value chain (interdependencies) as a result of a significant event. If done at a corporate level, screening can be used to help prioritize which facilities would be candidates for further analysis. Screening can also be helpful when evaluating regional impacts. For those facilities that are identified for further evaluation, a formal SVA should be considered that looks at individual assets within the facility and helps to identify and prioritize vulnerabilities that should be addressed.

4.2 Data Gathering

After the initial screening, the first step in an SVA is to assemble information about the location, its assets and any potential threats to those assets. 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 assets so that a screening for the most significant security risks can be readily identified.

Table 4.1—Examples of petroleum facility assets subject to potential security risk
Buildings:
Administration offices, corporate offices, control rooms
Equipment:
Process units and associated control systems; product storage tanks; surge vessels, boilers, turbines, process heaters, sewer systems
Support systems:
Utilities such as natural gas lines, electrical power grid and facilities (including back-up power systems), water-supply systems, wastewater treatment facilities
Transportation interface:
Railroad lines and railcars, product loading racks and vehicles, pipelines entering and leaving facility, marine vessels and dock area, off site storage areas
Cyber systems and information technology:
Computer systems, networks, all devices with remote maintenance ports, SCADA systems, laptops, PDAs and cell phones.

4.3 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 companies without a formal SVA processes may find that an initial screening level SVA can be beneficial in terms of focusing resources on the most important areas. Companies may find a screening approach as the most practical means to prioritize facilities for SVA.

Table 4.2—Examples of security risks or threats in the petroleum industry
• Intentional release (loss of containment) from a process unit or storage tank
• Loss of a critical management team or member
• Destruction or disruption of support systems, such as:
o Electrical power; water supply, sewer systems
o Communications systems, computer systems
o Raw material (crude oil) supply, finished product distribution
• Contamination of raw material or finished product
• Bomb threat or discovery of an Improvised Explosive Device (IEDs) or Vehicle Borne Explosive Devices (VBED)
• Bio-terrorism or eco-terrorism
• Cyber attack
• Vandalism or theft

After identifying the most significant risks next determine what countermeasures should be implemented to reduce or eliminate the risk, and where additional assessment techniques would be of the most value in identifying future risk-threatening issues. The risk control and mitigation process may involve:

- 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;
- Selection and implementation of a strategy for risk control.

A SVA may also help 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 may 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 or asset. 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 ensure 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 may include, but are not limited to:

- Controlling access into, within and out of a facility or critical asset areas;
- Perimeter protection including immediately beyond the perimeter;
- Security personnel;
- Redundant systems (electrical, water, computing, communications, sewer, gas);
- Mail and package screening system.

Update, Integrate, and Review Data. After the initial security assessments have been performed, the facility will have 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.

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 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. Companies should collect information and periodically evaluate the success of their security assessment techniques and other mitigation risk control activities.

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. 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 system involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. SVAs should be reviewed and revised to reflect current conditions.

It is important to emphasize that a security plan should 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.

4.4 Example Elements of a Security Plan

Security plans should address a number of key elements related to an organization's security policies, practices, and procedures as well as describe the physical and cyber security features being employed to protect a particular asset. Figure 4.2 is an example of certain key elements that may be considered as part of a security plan. Figure 4.2 was created to be consistent with the Maritime Transportation Security Act (MTSA) as required under the U.S. Coast Guard regulations, 33 *CFR* 105.405. If you are a MTSA covered facility, your FSP requirements may be significantly more stringent than those outlined in this document in Figure 4.2. You are therefore encouraged to review USCG Regulations 33 *CFR* Parts 101-106 for more detailed information about your obligations. For a more comprehensive reference of federal laws and security regulations, please refer to Appendix A.

Figure 4.2—Example Elements of a Security Plan	
1.	Security Administration & Organization
2.	Personnel Training
3.	Drills and Exercises
4.	Records and Documentation
5.	Response to Change in Alert Level
6.	Communications
7.	Security Systems & Equipment Maintenance
8.	Security Measures for Access Control, Including Designated Public Access Areas
9.	Security Measures for Protected/ Controlled/Restricted Areas
10.	Security Measures for Monitoring
11.	Security Incident Procedures
12.	Audits & Security Plan Amendments
13.	Security Vulnerability Analysis (SVA) Report

In general, the security plan should be customized to support each owner/operator's unique needs therefore, not all of the items listed in Figure 4.2 may be necessary at a particular location. It is up to the company determine its security needs based on a sound risk-based decision making process. For more information about security risk-based decision-making, please refer to section 5.0.

The security plan should be periodically evaluated and updated to account for changes in operation, the environment in which the system operates, new data and other security-related information. Periodic plan review and improvement is helpful to take advantage of new information, improved technology, and changes in the operating plan of a facility. For example, the availability of new threat information may require a change in strategy for access control. An effective security plan should be flexible to account for changes in the operating environment and to meet the goals of an organization's management system.

4.4.1 Security Administration and Organization of the Facility

This section of the security plan should identify the Security Officer and/or the person(s) primarily responsible for administering the security program at the location. Other site/company personnel with security responsibilities should also be identified, along with a description of their duties and responsibilities (e.g., a guard force supervisor, other guards, receptionists that confirm the identification of visitors, etc.).

4.4.2 Personnel Training

This section of the security plan should describe the security-related training provided to the Security Officer(s) and/or the person(s) primarily responsible for administering the security program at the location. Training for other site/company personnel with security responsibilities should also be identified as well as other security awareness training provided to employees at the location.

For efficiency purposes it is noted that many EHS-training topics, have a direct or peripheral relationship to security (e.g., emergency response, particularly in a petroleum handling/processing facility). These topics should also be described as appropriate. For MTSA facilities, the USCG Regulations under 33 *CFR* 105.205 provide a list of qualifications for Facility Security Officers (FSOs), other persons with security duties, and all other employees respectively. Note that these comprehensive lists of skills do not all have to be explicit training topics. They can be obtained

through either training and/or experience. The training for all other employees of the site is orientation and security awareness, stressing the notion that all employees need to develop a healthy level of skepticism about what they see and hear on or adjacent to the site while performing their normal duties.

4.4.3 Drills and Exercises

This section of the security plan should describe the planned activities that rehearse aspects of the security plan and any procedures that support the plan. Each location should determine the extent and frequency required to conduct security drills and exercises. Based on a security risk assessment, a specific location may find that no drills or exercises are warranted, others may find that short, focused activities that test one portion of the security program and involve one person or group and their duties (e.g., vehicle searches by main gate guards) will be sufficient, while higher risk sites may require full-scale roll-out or table-top exercises involving multiple groups and offsite responders.

Many of these activities may share the same goals, the same onsite personnel and the same offsite responders as those required for environmental, health, or safety (EHS) related events. Again, efficiency should be considered to minimize any duplication and to leverage existing programs and activities.

For MTSA facilities, the USCG regulations require certain drills and exercises at defined maximum intervals. Many EHS laws and regulations have similar requirements. For example, a petroleum processing facility may be covered by the Oil Pollution Act, SARA Title III regulations, and possibly OSHA and EPA requirements. It is suggested that the EHS and security staffs at the site and corporate levels reconcile these requirements and devise a drill and exercise plan that meets all regulatory requirements simultaneously, including documentation. This plan should then be incorporated into or referenced by the security plan. The security plan should describe, in general terms, the follow-up process for drill and exercise critique action items. If this is the same process that used to resolve EHS-related recommendations and action items, this information can be referenced to the appropriate procedures, databases, or other documents.

In addition to facility drills and exercises, the company's crisis management plan (CMP), if applicable, should also be described in this section of the security plan, to the extent that the security program of the site will rely on the CMP as part of its security program, and what information and support the CMP describes will be provided by the individual site(s). The site emergency response plan(s) and the company CMP are also described and referenced in the security incident procedures section of the security plan.

4.4.4 Records and Documentation

This section of the security plan should describe what security-related records will be kept and how they will be protected from unauthorized disclosure. To the extent possible, existing EHS, quality, and other recordkeeping systems should be utilized to avoid duplication and overlap. Many petroleum facilities have thorough recordkeeping systems already in place for EHS and/or ISO purposes. Therefore, this section of the security plan should describe how the existing documentation systems will be modified to include security-related matters, and who has the responsibility for maintaining the security records, as well as record retention policies for security-related records. MTSA facilities have eight (8) specific types of records that must be kept.

4.4.5 Response to Change in Alert Level

This section of the security plan should describe the security alert system in use at the site or company, whether it is the Department of Homeland Security (DHS) Homeland Security Advisory

System color-coded system, U.S. Coast Guard Maritime Security (MARSEC) levels, International Ship & Port Security (ISPS) Code Security Levels, or a company-specific system. Specifically, the security plan should describe what the site would do at each level in the alert system. For example, if the site uses the DHS HSAS alerts, the plan should describe what additional security measures will be employed if the alert level is elevated from Yellow to Orange. Since most of the alert systems are maintained by external government organizations, the security plan should also describe how changes in alert levels are recorded and the time taken to achieve the declared level. Even in the absence of direct regulatory requirements (e.g., the MTSA 12 hour limit to achieve declared level), the site or company might be asked to report this time interval to external organizations. Refer to section 3.4 of this guidance for a more thorough discussion of alert levels. Refer to section 6.0 for certain example response measure related to changes in the alert level.

4.4.6 Communications

This section of the security plan should describe the necessary communications capabilities of the facility with respect to implementing the security plan. Certain elements to consider are:

- Communications capabilities between employees (e.g., radio, telephone, etc.).
- Communications between the facility and offsite responders or support (e.g., 911).
- Communications between vessels and the facility, if applicable.
- Communication of data, including which computer systems and networks are critical to security (e.g., process control systems; electronic access control systems, etc.), including a general description of the cyber security provisions for these systems.

It should be noted that not all of these elements might be appropriate for a specific location. For example, a small low-risk, unmanned, remote facility may require periodic checks on a weekly or monthly basis.

4.4.7 Security Systems and Equipment Maintenance

This section of the security plan should describe the inspection, test, and preventive maintenance program for security equipment (e.g., camera systems, lighting fencing, etc.).

4.4.8 Security Measures for Access Control, Including Designated Public Access Areas

This section of the security plan should include the policies, practices, and procedures that are important to effectively implement the security plan. The following is a list of items to consider. It should be cautioned that not all of these elements may be appropriate for a specific location.

- Identification requirements for employees, visitors, contractors, truck drivers, railroad crews, government employees/law enforcement and other who may seek access.
- Sign-in or documentation of access procedures.
- Escorting policies for visitors, contractors, and government employees. (Circumstances when escorts are required and the procedures to be followed under each situation.)
- Screening and searching procedures for vehicles, baggage (accompanied and unaccompanied), hard-carried articles.
- Physical security measures applicable to access control (Fencing/barriers, locks, lighting, intrusion detection, etc.).
- Physical barriers that prevent vehicles from being used as weapons.
- The escalation in the implementation of access control procedures as alert levels escalate (How vehicle search procedures change as alert levels rise).

4.4.9 Protected/Controlled/Restricted Areas

If the location designates certain areas as protected, controlled or restricted, then the physical security measures pertinent to those areas should be described this section of the plan.

4.4.10 Security Measures for Monitoring

This section of the plan should describe how the facility is monitored for unauthorized access. Monitoring can be done through a variety of methods to meet the needs of a particular location. For remote facilities that are considered less attractive, frequency of operational checks may be sufficient. For more sophisticated facilities, a combination of personnel monitoring (gaurds and dogs) and technology (intrusion detection) may be more appropriate. As with access control measures, the security plan should describe how the monitoring equipment, personnel, and procedures change as alert levels escalate. For example, if the facility employs off-duty law enforcement officers at "Orange" alert, then this arrangement should be described in the security plan.

4.4.11 Security Incident Procedures

This section of the plan should define what events constitute a breach of security, who is to be notified and the order of such notification. Additionally, the plan should describe the procedure to conduct an investigation of security breaches and incidents (note that this procedure may require some modification to include security related incidents within its scope and to define unique requirements for such investigations). This section should also generally describe or reference the site emergency response plan and the company crisis management plan, if applicable.

4.4.12 Audits and Security Plan Amendments

This section of the security plan should describe how the plan should be audited, including periodicity, audit team leadership/membership, documentation, and follow-up of findings. For MTSA facilities, the USCG regulations contain specific provisions for security plan audits. Non-MTSA facilities may wish to develop their own or use existing HES auditing.

Following an audit, or for other reasons, the security plan may require amending. The process for generating security plan amendments, how they are approved (both internally, and possibly by external organizations) should be described. The USCG regulations contain a defined interface process between the Coast Guard and the facility to amend a security plan. If the facility is not USCG regulated and is ISO-9000 certified, the ISO process for maintaining controlled documents, or an equivalent may be used.

4.4.13 Security Vulnerability Analysis (SVA) Report

This section of the plan may include the SVA report as an attachment, a summary of the SVA, or reference the SVA report. The SVA contains the basis for many of the other items described in the security plan and hence becomes a part of the plan. This includes the need to keep the SVA current, as well as the security plan itself. If the facility is Coast Guard regulated, the SVA is referred to as a Facility Security Assessment (FSA) and accomplishes the same purpose as a SVA. Additionally, if the facility is Coast Guard-regulated, the completed Facility Vulnerability and Security Measures Summary (Form CG-6025) must also be included in the security plan. (Refer to Chapter 5.0 for more information on security vulnerability assessment.)

5.0 Security Vulnerability Assessment (SVA) Concepts

5.1 Security Vulnerability Assessment Overview

Security Vulnerability Assessment (SVA) is a systematic process that evaluates the likelihood that a threat against a facility or asset will be successful and considers the potential severity of consequences to the facility itself, to the surrounding community and on the energy supply chain. One purpose of an SVA is to identify countermeasures that may reduce the risk of an attack and its potential consequences.

There are several SVA techniques and methods available, all of which share common elements. Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the facility's needs. Differences in geographic location, type of operations, and on-site quantities of hazardous substances, if any, all play a role in determining the level of SVA and the approach taken. Examples include:

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.
3. ***Identify potential security vulnerabilities*** that threaten the system's service or integrity.
4. ***Determine the 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*** and re-assess risk.

The objective of conducting an SVA is to identify security hazards, threats, vulnerabilities and countermeasures that will provide for the protection of the public, workers, national interests, the environment, and the company.

Owner/operators may use any appropriate security vulnerability assessment methodology that effectively achieves this objective. Following are a few published methodologies that are currently available for this use:

- API RP 70 *Security for Offshore Oil & Natural Gas Operations*, 1st Ed., March, 2003
- API RP 70I *Security for International Oil and Natural Gas Operations*, 1st Ed., April 2004
- API/NPRA *Security Vulnerability Assessment Methodology*, September 2004
- 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"[8]
- Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)
- USCG NVIC 11-02

This guidance should also be considered in light of any applicable governmental security regulations and other guidance as outlined in Appendix A, Regulatory Matrix.

The SVA process may be used to assess a wide range of security issues such as those listed in Figure 5.1.

Figure 5.1—Security Events Evaluated During the API 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. *Theft* of toxic substance or flammable hydrocarbons with the intent to cause severe harm at the facility or offsite. 3. *Contamination* or spoilage of products to cause workers 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.

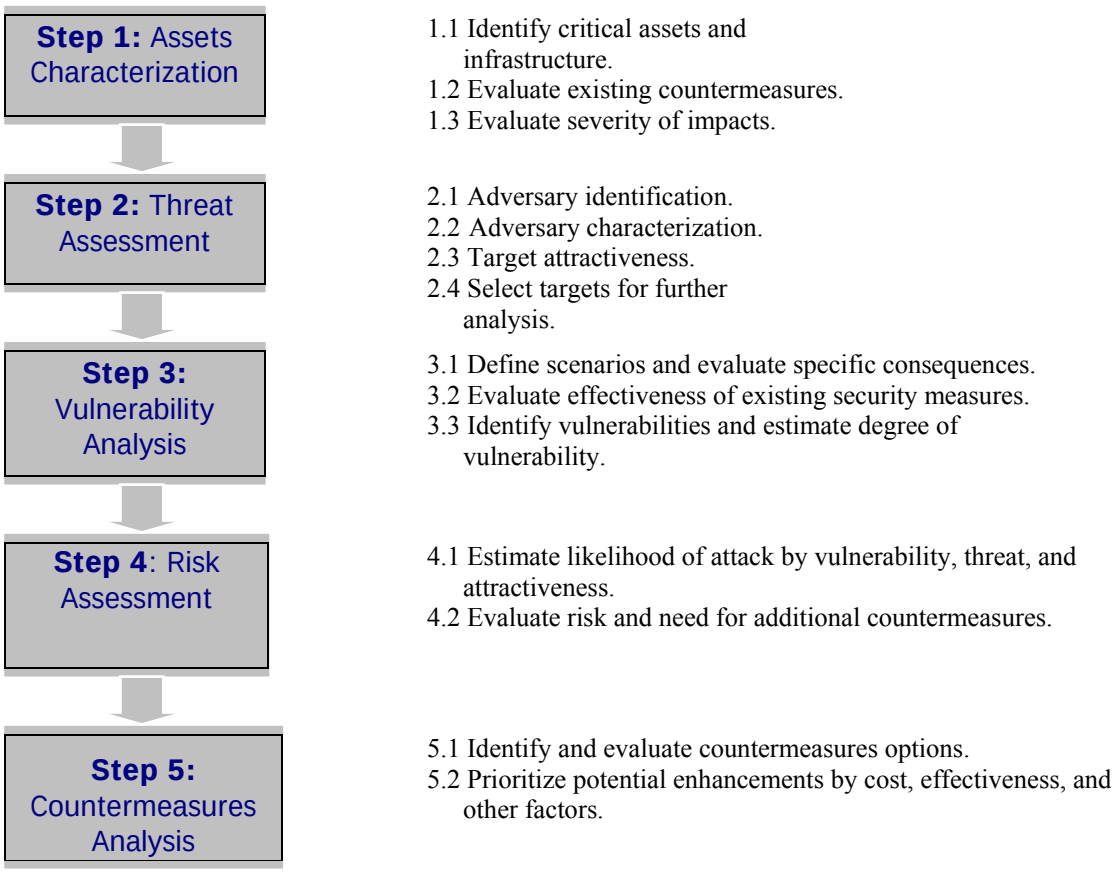
If a facility is covered under USCG regulations 33 *CFR* 101 through 106, there are specific security events that need to be evaluated as part of the SVA. Please refer to the applicable parts of the regulation and U.S. Coast Guard NVIC 11-02 for details on these events, as they are specific to the type of vessel/facility/operation.

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 and petrochemical industries. Other valid approaches, such as outlined in API RP 70 and RP 70I, 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) 682-8000 www.api.org	National Petrochemical and Refiners Association 1899 L. Street, N.W. Washington, D.C. 20036 (202) 457-0480 Attn: Maurice McBride

Figure 5.2—API/NPRA Security Vulnerability Assessment Methodology



5.3 Estimating Risk Using SVA Methods

Risk management principles recognize that risk generally cannot be eliminated, however by enhancing protection from known or potential threats it can be reduced. 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, 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. Much of the threat information that the Government possesses is classified and is not generally available to the public.

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. In the security realm, this traditional model begins to break down. In the absence of specific intelligence, it is impossible to be

specific about the likelihood of an attack. One conclusion of this reasoning is that there is no risk – a potentially 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, 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."[9]

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

Figure 5.3—Example Risk Matrix

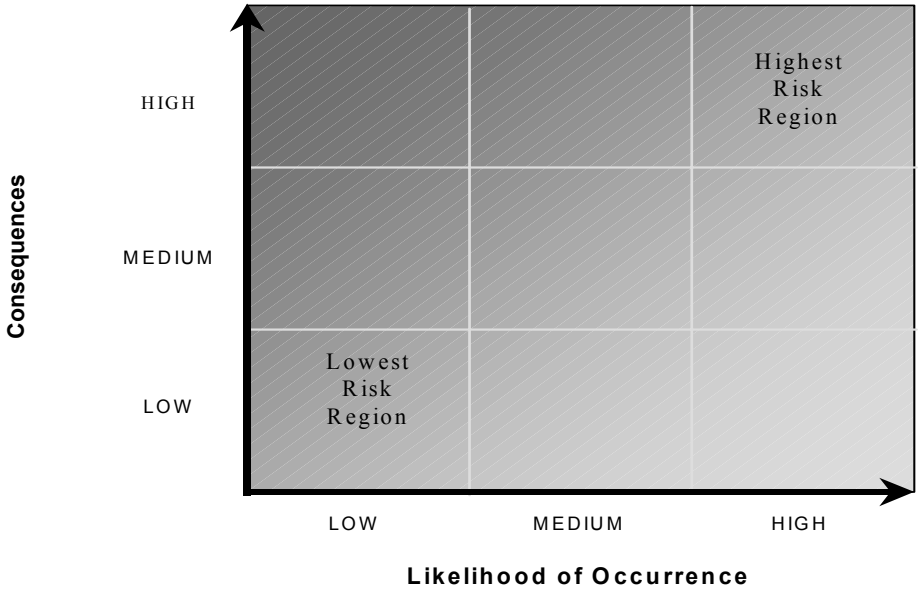


Figure 5.4—SVA Risk Definition
Security risk is a function of the consequences of an attack and the likelihood of the attack.
The likelihood of damage or loss of an asset is a function of the target's attractiveness, the degree of threat, and the degree of vulnerability to the attack.

The risk variables are defined as shown in Figure 5.5.

Figure 5.5—SVA Risk Variables[10]	
Consequences	Consequences are the potential impacts of the event.
Likelihood	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 the three variables below.
Threat	Threat 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	Vulnerability is a 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 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 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 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 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 to make sound risk management decisions. The company 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 (C)

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. Several examples of relevant consequences in a SVA include:

- Injuries to the public or to workers.
- Severe environmental damage (such as contamination of drinking water).
- Direct and indirect significant financial losses to the company.
- Disruption to the national, regional, or local operations and economy.
- Loss of 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 worst case credible security event should be defined. Critical infrastructure 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 initial screening, consequences and attractiveness are used to screen low value assets from further consideration.

5.4.3 Threat (T)

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset.[11] 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.

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

5.4.4 Vulnerability (V)

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset.[12] 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 (A_T)

Not all targets are of equal value to adversaries. A basic assumption of the SVA process is that target attractiveness 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 if known. 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 to cause collateral damage
• Proximity to a national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Target recognition

5.5 Characteristics of a Sound SVA Approach

It is important to distinguish between a security risk management process and a SVA method. Security 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 may 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 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.

5.6 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, and outside experts if needed, to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the company'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 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.

5.7 SVA Strengths and Limitations

Each of the SVA methods commonly used has its strengths and limitations. Qualitative methods are well suited for making good sound security management decisions at the local asset level. In selecting an appropriate SVA method, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

Table 5.1—Questions to determine SVA Approach Needed
• Does the scope of the SVA method 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?
• 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 is available to the company? Do 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?

5.8 Recommended Times for Conducting and Reviewing the SVA

Figure 5.7—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 significant new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the owner/operator of the facility (revision or rework)
5	After a significant security incident, at the discretion of the owner/operator of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

5.9 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. Potential capital and maintenance improvement activities may 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 a combination 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.

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. 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.[c] 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.

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 "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.

5.10 Risk Screening

Security issues potentially 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.[13]

It is likely that most facilities have no specific threat history. A screening process may contain the following factors:

1. Target attractiveness or target value,
2. Degree of threat,
3. Difficulty of attack (function of adversary, current security 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.

Arguably target attractiveness is the dominant factor in determining terrorist risk. 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.

[c] 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.

6.0 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 directed at a petroleum facility, facility assets, and 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 facility.

In addition to HSAS, there are several other threat level systems used by both industry and other agencies. While the MARSEC levels utilize only a 3 Tier system, it may essentially be compared to HSAS with:

- MARSEC 1 equivalent to HSAS Green, Blue and Yellow.
- MARSEC 2 equivalent to HSAS Orange.
- MARSEC 3 equivalent to HSAS Red.

If a system other than HSAS or MARSEC has been implemented by an individual company it most likely has been developed based on HSAS, MARSEC or both and specific guidance contained below should be considered where appropriate.

Each company should be able to advise and communicate to company personnel and others as warranted the security condition at the facility. The potential measures associated with each alert level are not always prioritized but those implemented should be initiated concurrently where practical and as applicable. Facility management should maintain a record of specific actions taken for each alert level. Less attractive facilities, remote facilities, unmanned facilities may employ less stringent measures. Following is a detailed explanation for each alert level and the potential response measures associated with each level:

6.1 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:

Access Control/Perimeter Protection

- Have all contractors and visitors check or sign in and out of the facility at designated location(s).
- Ensure existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting as appropriate.

Communications

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

Training/Policies/Procedures/Plans

- Develop terrorist and security awareness information and provide relevant education to employees on security standards and procedures. Caution employees not to talk with outsiders concerning their facility or related issues.

- Advise all facility personnel to report the presence of unknown personnel, unidentified vehicles, aircraft or watercraft, vehicles, watercraft or aircraft operated out of the ordinary, abandoned packages, and other suspicious activities.
- Incorporate security awareness and information into public education programs and notifications to emergency response organizations as appropriate.
- Survey surrounding areas to determine those activities that might increase the security risks that could affect the facility (e.g., airports, government buildings, other industrial facilities).
- Ensure contingency and business continuity plans are current and include a response to terrorist threats.
- Review existing emergency response plans and modifying them, if required, in light of potential threats.

IT Security

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

6.2 Guarded Condition—Blue

This condition exists when there is an increased general threat of possible terrorist activity against the facility or facility 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:

Perimeter Protection/Access Control

- Secure 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.
- Inspect perimeter fencing and repairing all fence breakdowns. Review all outstanding maintenance and capital projects that could affect the security.
- Reduce the number of access points for and spot-check the contents of vehicles, aircraft, watercraft and personnel. Be alert to vehicles or watercraft parked or moored for an unusual length of time in or near a facility.
- Check designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increase surveillance in designated areas.
- Require visitors to check in at a facility office and verifying their identification. Be especially alert to repeat visitors or outsiders who have no apparent business at the facility and are asking questions about the facility or the facility's personnel. Familiarizing facility personnel with vendors who service the facility and investigate unusual changes in vendor personnel.
- Inspect all packages/equipment coming into the facility. Do Not open suspicious packages. Consider reviewing the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving packages.

Communications

- Inform personnel of the change in alert status. Review with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implement procedures to provide periodic updates to employees on security measures being implemented that are considered confidential.
- Test security and emergency communications procedures and protocols as appropriate.

Training/Policies/Procedures/Plans

- Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.
- Review communications procedures and back-up plans with all concerned.

6.3 Elevated Condition—Yellow

This condition exists when there is an elevated risk of terrorist activity against the facility or facility 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

- Close and lock gates and barriers except those needed for immediate entry and egress. Inspect perimeter and perimeter fences on a regular basis. Ensure that other security systems are functioning and are available.
- Inspect on a more frequent basis the interior and exterior of all critical buildings and around all storage tanks and other designated critical areas.
- Dedicate personnel to assist with security duties to monitor personnel entering the facility and to inspecting the area on a regular basis, reporting to facility management as issues surface.
- Limit visitors and confirm that the visitor has a need to be and is expected at the facility. Escort visitors while at the facility pursuant to the specifics outlined in the security plan.

Communications

- Inform personnel of the change in alert status. Review with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level as appropriate. Implement procedures to provide periodic updates to employees on security measures being implemented.
- Check to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirm availability of security resources that assist with extended coverage.
- Identify areas where explosive devices could be potentially hidden.
- Instruct employees working alone to check-in on a periodic basis.

6.4 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 facility or facility 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 facility and its personnel. In addition to the measures suggested for **Yellow**, the following measures could be considered:

Perimeter Protection/Access Control

- Reduce facility access points to the absolute minimum necessary for continued operation.
- Increase security patrol activity such as perimeter patrols and inspections.
- Check security systems such as lighting and intruder alarms to ensure they are functioning. Install additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.
- Prohibit unauthorized or unidentified vehicles/personnel entrance to the facility.

- Inspect vehicles entering the facility, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed pursuant to the specifics outlined in the security plan. Inspect all packages and cargo being delivered by aircraft or watercraft in the same manner.
- Limit access to the facility to those personnel who have a legitimate and verifiable need to enter. Implementing positive identification of all personnel.

Communications

- Advise appropriate agencies that the facility is at an **Orange** alert level and advise of the measures being employed—requesting an increase in the frequency of their patrol of the facility.
- Consider consultation with local authorities about control of public roads and accesses by waterway that might make the facility more vulnerable to terrorist attack if they were to remain open.

Training/Policies/Procedures/Plans

- Continue **Green**, **Blue** and **Yellow** measures or introduce those that have not already been implemented.
- Develop procedures for shutting down and evacuation of the facility, if considered necessary, in case of imminent attack.
- Ensure that employees not work alone in remote areas or increasing the frequency of call-ins from remote locations.

6.5 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 facility, or when an attack is initiated on the facility and its personnel. Normally, this alert is declared as a localized condition at the facility. In addition to the measures suggested for **Orange**, the following measures could be considered:

Perimeter Protection/Access Control

- Augment security forces. Establish surveillance points and reporting criteria and procedures. Solicit assistance from appropriate agencies in securing the facility and access, if possible. Cooperate with authorities if they take control of security measures.

Training/Policies/Procedures/Plans

- Continue **Orange** and **Yellow** measures or introduce those that have not already been implemented.
- Consider shutting down the facility and operations in accordance with security contingency plans and evaluating security prior to resuming operations if they are temporarily shut down.
- Implement business contingency and continuity plans as appropriate.

7.0 Information (Cyber) Security

7.1 Introduction

The petroleum industry is a worldwide industry that is highly dependent on technology for its communications and operations. Technological advances that promote better efficiency and more automation within the petroleum industry also make information security an increasingly important issue. Technology is an important component of information security but without the integration of policies, procedures, processes and people, technology alone can not provide adequate information security.

It is widely understood that information security is important for office computing systems such as desktop PCs, laptops, servers, software programs, etc. What is less recognized is that computer technology has become pervasive throughout the entire organization, including network access to plant equipment to allow vendors to maintain systems remotely, and remote access connections to process control systems (SCADA) to allow engineers to trouble-shoot problems. In all of these environments, improper controls could allow unauthorized individuals to accidentally or intentionally harm the information assets of the petroleum industry.

To ensure that adequate and appropriate resources are allocated within the information security program, information security activities should be based on a thorough analysis of risks to the confidentiality, integrity and availability of the information assets. A comprehensive information technology security program implemented by member companies improves the security of the petroleum industry as a whole by effectively:

- Identifying and analyzing actual and potential precursor events that could result in cyber security-related incidents;
- Identifying the likelihood and consequence of potential cyber security-related events;
- Providing a comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities;
- Providing a structured, easily communicated means for selecting and implementing risk reduction activities;
- Monitoring program performance with the goal of improving that performance;
- Establishing alert and response measures for a broad range of security threats.

Additionally, the establishment of a communication program between federal agencies and the industry to share threat information also improves the security of the industry by providing an early warning mechanism so appropriate action can be taken in a timely manner.

ISO/IEC International Standard 17799, ***Information technology—Code of practice for information security management***, describes a framework for creating an information security program and forms the basis of this guideline. ISO/IEC 17799 attempts to ensure preservation of confidentiality, integrity and availability of user access, hardware, software and data. The standard describes eight steps of an information security process: create an information security policy; select and implement appropriate controls; obtain upper management support; perform security vulnerability assessments (SVAs), create statements of applicability for all employees; create an information security management system; educate and train staff; and perform regular audits.

This framework has been endorsed by API's Information Technology Security Forum (ITSF) as voluntary guidance to protect the petroleum industry's information assets. The guidance contained herein and in ISO/IEC International Standard 17799 does not attempt to provide an all-inclusive list of information security considerations, but rather a framework for the evaluation and implementation of information security measures. The concepts mentioned in this Introduction are expounded upon in the following section.

7.2 Specific Security Guidelines

7.2.1 Security Policies, Standards and Procedures

Information Security policies, standards and procedures that focus on protecting a company's information technology assets are the foundation 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 technology assets. Since policies set the tone for the company's culture relative to protecting information and information technology, a policy must have executive management

sponsorship, clearly articulate accountabilities and responsibilities, and be communicated to every employee and system user in the company. Company policies should address topics such as:

- Assignment of management responsibilities
- Business conduct and appropriate system use
- E-mail and internet use
- Remote access & third party connectivity
- System monitoring and compliance (audit)
- Physical security (laptops, computer rooms, etc)
- Incident reporting and response
- Data retention
- Business continuity and disaster recovery

The company Information Security Officer or Manager is generally accountable for the development, implementation and maintenance of a company's information security policies. However, it is recommended that this be accomplished by working in "partnership" with representatives from the functional areas of IT Audit, Human Resources, Legal, Corporate Security and Information Technology.

Each policy should be accompanied by a set of standards and procedures that provide guidance for the operational implementation and compliance assessment of the policies. The standards and procedures should be derived from industry technology standards and/or "best practices" and where appropriate, clearly define "mandatory" requirements to which adherence is not an option. Security policies should be tested from time to time to ensure adequate protections are in place. When new information assets are introduced, policies should be updated to reflect any changes that may be necessary.

7.2.2 Security Awareness and Education

Companies should invest time and resources on an Information Security Awareness Program. To help safeguard company assets, employees must have the knowledge to understand the significance of their actions. A Security Awareness Program should designate responsibility for security training, clarify why security is important, identify who should attend Security Awareness Training, explain employee responsibilities, discuss existing security controls being taken to protect personnel and assets, and serve as a forum to discuss security questions.

Security awareness education should include "new hire" orientations, multi-media campaigns, and ongoing refresher activities. Incentive programs may also be utilized to bolster awareness and training efforts. Comprehensive security awareness programs will include both physical and cyber security initiatives.

7.2.3 Accountability and Ownership

It is important to establish an owner for all policies, procedures, hardware, software and information assets. Having identifiable responsibility for these assets within a company is fundamental to the control process. The responsibility for many owner tasks can be delegated to custodians, but the owner remains accountable for the asset. Some of the key responsibilities of an owner include:

- Defining the business requirements for which the asset is needed,
- Establishing the value, criticality and sensitivity of the asset,
- Establishing, maintaining, documenting and verifying cost effective controls commensurate with the risk,

- Establishing 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.

7.2.4 Data/Information Classification

Information classification is the process of assigning protection categories or labels to information materials such as hardcopy documents and computer files. Classification of assets is generally based on the impact to the business if the information is lost, disclosed, corrupted or made unavailable. It is important to identify an organization's most critical information assets so that protection efforts and budget can be focused on those resources.

Typical components of a classification program include a policy that defines the classification program, identification of asset owners, definitions for various classifications, guidelines for handling, storing, transmitting and accessing information with various classifications, and an education program for employees. An information classification framework was developed by the API IT Security Forum. For more information call 202-682-8590.

7.2.5 Security Vulnerability Assessments

Security Vulnerability Assessments (SVA) are a cost-effective method to identify risks and reduce them to acceptable levels. SVAs should be performed on information technology assets on a routine basis to identify significant exposures that could lead to negative consequences. SVAs should evaluate the potential business and financial impacts of loss of information integrity, disclosure of sensitive information, loss of processing capability, violation of regulations, and the impact on health, safety or the environment. Key outcomes of an SVA are the documentation of the owner's judgment of exposures and risks in the absence of controls, and the documentation of follow-up action plans or the justification for accepting residual risks.

7.2.6 Physical and Environmental Security

It is important to prevent unauthorized access, theft or damage to computing systems and information assets. Critical or sensitive information processing equipment should be housed in secure facilities, protected by a defined security perimeter. The nature of this perimeter should be commensurate with the identified risks and value of the business assets. 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 from hazards such as fire. Policies should be implemented when feasible that require desks to be left clear of sensitive documents and media, and computer screens to be locked when unattended.

7.2.7 Access Controls and Identity Management

The implementation of appropriate access controls and the management of user identities are essential for the preservation of confidentiality, integrity and availability. These processes are typically applied to network, host, application and physical assets. The resulting audit trails should be monitored to detect anomalies.

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 policies, procedures, training, background checks and supervision; logical or technical controls such as passwords, two-factor authentication mechanisms, encryption, system hardening and protected protocols; and physical controls such as locks, cables, security cameras, guards and fences.

Identity Management or User Management systems maintain system user identities for the purpose of authenticating individuals to multiple systems. Identity management processes create, remove or modify an individual's access to systems in compliance with company policy. When an Identity Management system is functioning properly, a change to an individual's status will automatically and appropriately modify the access permitted to that individual throughout the environment.

7.2.8 Network Security

Many controls are required to achieve and maintain the security of computer networks. Network controls should be implemented based on 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 intrusion detection that is required to ensure required security levels are maintained.

Access to networks by remote users, access to network management facilities, and access to remote diagnostic ports on network equipment should require an appropriate level of authentication, such as two-factor authentication. Additional controls within the network to segregate information systems or groups of users should be considered when different levels of trust or security requirements exist. Shared networks and those linked to third parties require particular access control policies, traffic filtering, and routing controls to ensure that computer connections and information flows do not breach the access control policy of business applications. Security patches should be maintained on all network devices.

7.2.9 Systems Development

Information security controls should be integrated into the initial phases of any application, data or system development process because it is much more effective to design information security requirements early in a development process rather than attempting to retrofit them after the system is operational. Security controls should be designed according to a risk mitigation strategy that attempts to reduce risk to levels acceptable to the business unit, based on the value of the asset and the likelihood of threats against it.

Periodic design reviews should be conducted during development and modification processes to assure that the design satisfies the specified security requirements. Production data should not be used to test application software until software integrity is assured. Application software should not be placed into production until the system tests have been successfully completed and the application has been properly certified and accredited. (See Change Control)

Infrastructure that supports applications that process or maintain sensitive data must be protected as well. Specific security controls such as intrusion detection/prevention and anti-virus should be implemented on hardware platforms and operating systems utilized during application development phases. Vulnerability assessment and patch management processes should be implemented to reduce or eliminate known or recently released vulnerabilities. Development and production environments

should be continuously monitored to verify controls such as identity management and access control are functioning as intended.

7.2.10 Change Control

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 submission and evaluation of change requests, recovery and back-out procedures, and a mechanism to monitor and protect the organization's capacity to ensure uninterrupted availability.

7.2.11 Viruses and other Malicious Code

Increasingly complex and sophisticated malicious code continues to be prevalent, making it essential to implement effective controls to mitigate this risk. Recent versions of malicious code combine different infection techniques, carry new payloads, and steal or expose information rather than just destroying it. To reasonably mitigate this risk, multiple solutions should be deployed. 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. To the extent possible, anti-virus software should be centrally administered to ensure desktops are updated quickly and uniformly.

Consideration should be given to the deployment of desktop (personal) firewalls and anti-spyware systems. Operating system and application security patches should be evaluated based on the risk they mitigate and installed as appropriate to reduce 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 distribution.

7.2.12 Intrusion Detection and Incident Management

Systems should be implemented and qualified personnel should be assigned to log and monitor inappropriate or unauthorized network activities. Electronic firewalls and other systems should be installed and configured to detect and prevent hostile activity at all external network access points, and between certain internal networks as appropriate. An incident response plan 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, including internal public relations staff and government or law enforcement agencies. 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. A computer security incident response plan was developed by the API IT Security Forum. For more information call 202-682-8590.

7.2.13 Business Continuity, Business Resumption and Disaster Recovery

Business Continuity, Business Resumption and Disaster Recovery are somewhat interchangeable terms. The intent of these plans is to enhance an organization's ability to counteract interruptions to normal operations. Business Impact Assessments should be performed by each department or function to determine the length of time they can operate without critical systems or processes before the business unit would incur a material loss. Appropriate business resumption plans, including well defined and tested data backup processes, should then be developed and implemented that would

have a reasonable probability of preventing such a material loss. These plans should be documented to form the Business Resumption Plan for the entire business unit. It is critical that Companies regularly test their Business Continuity Plans and revise the documentation as necessary to ensure the long-term effectiveness of their overall business continuity strategy.

7.2.14 Regulatory Compliance

Companies should establish a regulatory baseline to measure and provide corporate wide visibility to legal compliance requirements. To establish this baseline, all applications, systems and infrastructures should be identified and documented. Communication between corporate information security planners and other corporate functional sponsors or business owners should be established to ensure proper attention, visibility and guidance is obtained.

All relevant statutory, regulatory and contractual requirements should be identified, defined and documented for each information system. Major legislation has been passed in the following areas and should be addressed:

- Intellectual property (business information and copyrighted materials)
- Records retention (safeguard organizational records)
- Data protection and privacy of personal information
- Import/Export regulation (such as laws related to the use of encryption)
- Law enforcement (Rules of evidence)
- HIPPA, Sarbanes-Oxley, Graham-Leach-Bliley and others

7.2.15 Audit (Compliance and Assurance)

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

A company's executive management and Audit Committee have become increasingly interested in how well the company is protecting its critical information technology assets from unauthorized access and inappropriate use. One of the key assurance methods used by management is audit. Unsatisfactory audit reviews are discussed with management and/or the Audit Committee. These reviews typically require a clear definition of actions to be taken to prevent reoccurrence and a 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:

- Appropriate use of Internet and e-mail systems
- Intrusion Detection reporting
- Password strength
- User account administration (modifications, additions, deletions)
- Change Management compliance

Appendix A—Security Regulations Affecting the U.S. Petroleum Industry

Security Regulations Affecting the U. S. Petroleum Industry					
Operating Sector	**Federal Agency**	**Issue**	**Requirement**	**Deadline**	**Authority References**
Marine, Upstream, Downstream	USCG, DHS	Area Maritime Security Improvements – General Provision	Establishes framework for vessels and facilities located under, in, on or adjacent to U.S. waters to implement security plans developed under Parts 104, 105 and 106, to deter transportation security incidents; provides for civil and criminal penalties for noncompliance; provides for Coast Guard approval of Alternative Security Programs.		Final rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Subchapter H, Part 101. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Area Maritime Security	Integrates port security-related requirements in the Maritime Transportation Security Act of 2002 with International Ship and Port Security Code (ISPS) and amendments to International Convention for Safety of Life at Sea (SOLAS). Establishes Area Maritime Security (AMS) Committee, directs the Committee to develop a risk-based AMS Assessment and an AMS Plan to respond to maritime security threats. (See J and K.)		Final rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Subchapter H ,Part 103. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Vessel Security	Requires owners or operators of vessels calling on U.S. ports to designate security officers for vessels, develop a Vessel Security Assessment, develop and submit to the USGS for approval a Vessel Security Plan that addresses components outlined in the rule, implement security measures specific to the vessel's operation, and comply with Maritime Security Levels. (See G.)	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/30/04. Foreign vessels must have certificate of compliance with SOLAS and ISPS on or before 7/1/04.	Final rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Subchapter H, Part 104. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DHS	Port Facility Security	Requires owners or operators of certain facilities at U.S. ports to designate security officers for facilities, develop a Facility Security Assessment, develop and submit to the USCG for approval a Facility Security plan that addresses components outlined in the rule, implement security measures specific to the facilities' operations, and comply with Maritime Security Levels. (See H.) See also updated regulations for handling of Class I (explosives) or other dangerous cargoes within or contiguous to waterfront facilities.	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/30/04.	Final rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Subchapter H, Part 105. See also Interim Final Rule 7/1/03 [68 FedReg 39240] Final Rule – 9/26/03 [68 FedReg 55436]
	USCG, DOT	Port/Facility Access: Identification Credentials	Clarifies the identification credentials that are acceptable to allow access to waterfront facilities and to port and harbor areas, including the vessels in them.	Clarification effective 9/6/02.	Clarification of Regulation – 8/7/02 [67 FedReg 51082] See also 33 *CFR* 6.10-5, 125.09(f), 125.15 and 125.53

Security Regulations Affecting the U. S. Petroleum Industry					
Operating Sector	**Federal Agency**	**Issue**	**Requirement**	**Deadline**	**Authority References**
	USCG, DHS	Vessel Communication	Establishes technical and performance standards for an Automatic Identification System (AIS) and implements the AIS carriage requirements of the Maritime Transportation Security Act (MTSA) and the International Maritime Organization requirements adopted under International Convention for Safety of Life at Sea (SOLAS), 1974, as amended. Requires AIS on all vessels subject to SOLAS, Vessel Traffic Service Users and certain other commercial vessels. (See I and J.)	Varies by type of ship.	Final rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Parts 26, 161, 164, 165. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
	USCG, DOT	Vessels: Notification of Arrival (NOA) in US Ports	For vessels bound for or departing US ports: Specifies information required in a NOA including additional crew and passenger information, consolidates and centralizes NOA submissions, requires earlier NOA submission times, provides exemptions for certain vessels, and creates exceptions to submission times for cargo declaration.	Requirements effective 4/1/03.	Final Rule – 2/28/03 [68 FedReg 9537]
Upstream	USCG, DHS	Outer Continental Shelf Facility Security	Requires certain offshore mobile drilling units and fixed oil and gas platforms to develop Facility Security Plans and Facility Security Assessment reports (See A,B, and E), designate security officers for OCS facilities, implement security measures specific to the facility's operation, and comply with Maritime Security Levels. Criteria based on production or number of personnel. Smaller facilities are not required to have assessments and plans but are encouraged to use industry standards such as API RP 70 (See F.) Coast Guard will review need for further security requirements and then consider separate rule making that would require compliance with industry standards.	Plans to be submitted on or before 12/29/03. Compliance required on or before 6/25/04. Facilities built after 7/1/04 must file for approval 60 days prior to beginning operations.	Final Rule – 10/22/03 [68 FedReg 60448] 33 *CFR* Subchapter H, Part 106. See also Interim Final Rule 7/1/03 [68 FedReg 39240]
Transportation	RSPS, DOT	Hazmat transportation: Generally	Shippers and carriers of certain hazardous materials must develop and adhere to security plans. (See I.) Includes personnel security, unauthorized access information and en route security. Shippers and transporters of certain hazardous materials are required to comply with Federal security regulations that apply to motor carrier and vessel transportation.	Plans must be developed by 9/25/03. Compliance by 10/27/03.	Final rule – 3/25/03 [68 FedReg 14509] 49 *CFR* Part 172 Final rule – 9/26/03 [68 FedReg 55436] 33 *CFR* Part 126

Security Regulations Affecting the U. S. Petroleum Industry					
Operating Sector	**Federal Agency**	**Issue**	**Requirement**	**Deadline**	**Authority References**
	RSPS, DOT	Hazmat transportation: Employee Training	Shippers and carriers of certain hazardous materials must ensure that employee training includes a security awareness component. In-depth training required for shippers which have security plans. See 3.1	Compliance required no later than the date of the first scheduled recurrent training after March 25, 2003, and in no case later than March 24, 2006. New employees must receive training within 90 days of hire. Compliance by 12/22/03.	Final rule – 3/25/03 [68 FedReg 14509] Final rule – 3/25/03 [68 FedReg 14509]
	FMCSA, DOT	Hazmat transportation: Employee security	Applicants for a commercial driver's license (CDL) to transport hazardous materials must pass a security screening/background check by the Transportation Security Administration. States required to change procedures for issuing licenses, including collecting fingerprints and biographical and criminal history information of applicants for a hazmat endorsement for a CDL. Security threat assessment standards established to review applicants for hazmat endorsement to commercial driver licenses (CDL). Appeal and waiver procedures established. Certain individuals barred from shipping explosives. Exemption process provided.	State compliance on 4/1/04 (extended from 11/03/04). Limitations imposed beginning 9/2/03. After 4/01/04 (extended from 11/3/03), no renewals or issuances without TSA review Extension of licenses until 4/29/04 while TSA conducts reviews. Effective 3/11/04.	Delay of compliance date – 11/7/03 [68 FedReg 63030] Interim final rule – 5/5/03 [68 FedReg 23844] 49 *CFR* Parts 383, 384 Delay of compliance date – 11/7/03 [68 FedReg 63030] Interim final rule -- 5/5/03 [68 FedReg 23852] 49 *CFR* Parts 1570,1572 Final rule – 2/10/04 [69 FedReg 6195] Interim final rule -- 5/5/03 [68 FedReg. 23832] 49 *CFR* 107.105(c) 18 USC 842, 845
	USCG, DHS	Hazmat transportation: Facility security	Requires improved security and procedures related to the handling of dangerous cargoes and to and from vessels at such facilities, including fire extinguishing equipment, fire appliances, warning signs, outdoor lighting, international shore connection meeting for facilities involved with foreign-flag vessels, limited personnel access, certified material handling and other vehicles, and adequate equipment, materials and standards. Applicable also to waterfront facilities.	Compliance by 10/27/03.	Final rule – 9/26/03 [68 FedReg 55436] 33 *CFR* 126

Security Regulations Affecting the U. S. Petroleum Industry					
Operating Sector	**Federal Agency**	**Issue**	**Requirement**	**Deadline**	**Authority References**
	RSPS, FMCSA, DOT	Hazmat transportation: Security measures for motor carriers	Imposes specific security measures, e.g., escorts, vehicle tracing and monitoring systems, remote shutoffs, anti theft devices. Research and Special Programs Administration assumed the lead role from the Federal Motor Carrier Safety Administration for rulemaking addressing security of motor carrier shipments of hazardous materials.		ANPRM 7/16/02 [67 FedReg 46622] Notice – 3/19/03 [698 FedReg 13250]
Terminals	FERC, USCG, OPS, RSPA, DOT	LNG Terminal Siting	Applications for authorization to build LNG terminals to FERC (land based) or Coast Guard (offshore) must include security assessment and security plan. (See O.)	With application.	Title 49 *CFR* Part 193, Subpart J – Security 33 *CFR* Part 127
Pipelines	TSA, DHS	Security Assessment and Plan	OPS Pipeline Security Information Circular (non-public distribution) directs pipelines to identify critical facilities and develop, implement and annually review a security plan, utilizing industry association guidelines. OPS will audit to verify company response to circular. (See A, B, C, D and E.)	Written confirmation of compliance with the PSIC due 3/5/03.	Guidance with expectations and recommendations but not statutorily mandated. Pipeline Security Information Circular 9/5/02.
All Sectors	DHS	Procedures for handling Critical Infrastructure Information	Establishes procedures by which DHS will manage confidential data voluntarily submitted by companies. Implements Homeland Security Act of 2002 Sec. 214, also known as the Critical Infrastructure Act of 2002. Addresses how FOIA requests for physical and cyber vulnerability information will be handled.	Interim rule effective 2/20/04. Comments are due on 5/20/04	Interim rule – 2/20/04 [69 FedReg 8074] 6 *CFR* 29.1 et seq. Proposed rule -- 4/15/03 [68 FedReg 18523]

Statutory Authority:

- Homeland Security Act of 2002—Signed into law 11/25/02. Public Law 107-296.
- Pipeline Safety Improvement Act of 2003—Signed into law 12/17/02. Public Law 107-355
- Maritime Transportation Security Act of 2002—Signed into law 11/25/02. Public Law 107-295
- USA PATRIOT Act—Signed into law 10/26/01. Public Law 107-56
- Safe Explosives Act—Signed into law 11/25/02. Public Law 107-296

Appendix B—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 (Upstream), 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 C—Communication of Security Intelligence

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

Information Sharing and Analysis Centers (ISACs) were created to serve as information dissemination organizations 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 related 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 U.S. government agency, regulator, or law enforcement agency can access the ENERGY-ISAC. Other critical industries, such as finance and telecommunications, also 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 202-682-8286. Membership requests should be mailed to the ISAC administrator at:

ENERGY-ISAC
1220 L. Street N.W., Suite 900
Washington, D.C. 20005
USA

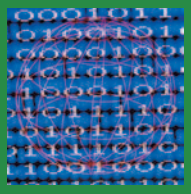
Appendix D—References

[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] 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.
[9] Ibid, AIChE.
[10] Ibid, AIChE.
[11] Ibid, AIChE.
[12] Ibid, AIChE.
[13] "National Infrastructure Protection Center, Homeland Security Information Update, Potential Al-Qa'ida Operational Planning," Information Bulletin 03-001, February 7, 2003.

API Creative Services: 25045 | 04.05





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.

API®
American Petroleum Institute

1220 L Street, NW
Washington, DC 20005-4070
USA
202-682-8000

Product No. OS0002