

Third
Edition



Petroleum
Refineries

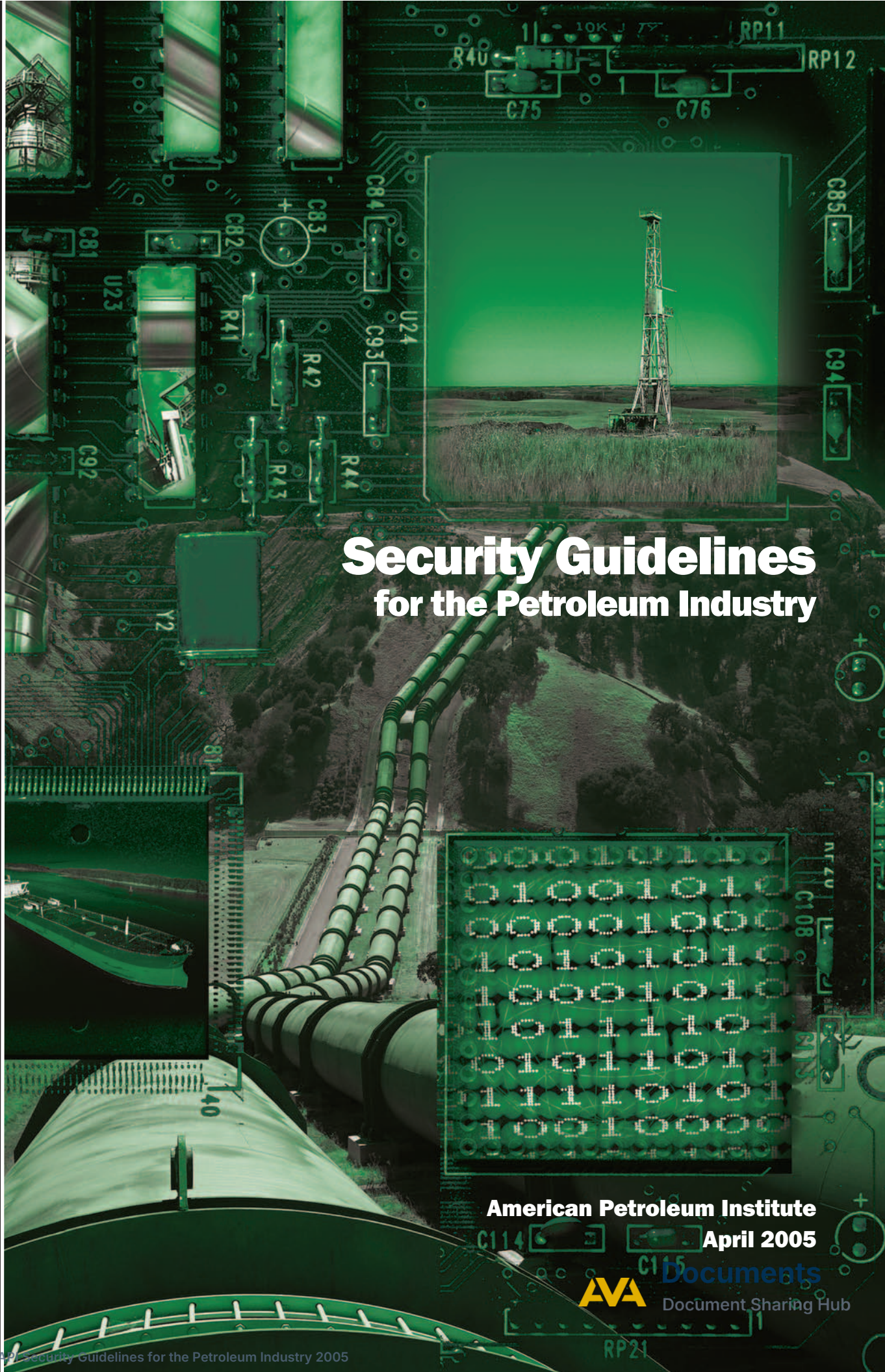
Liquid
Petroleum
Pipelines

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

AVA Documents
Document Sharing Hub

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



Documents

Document Sharing Hub

Third Edition



Petroleum
Refineries

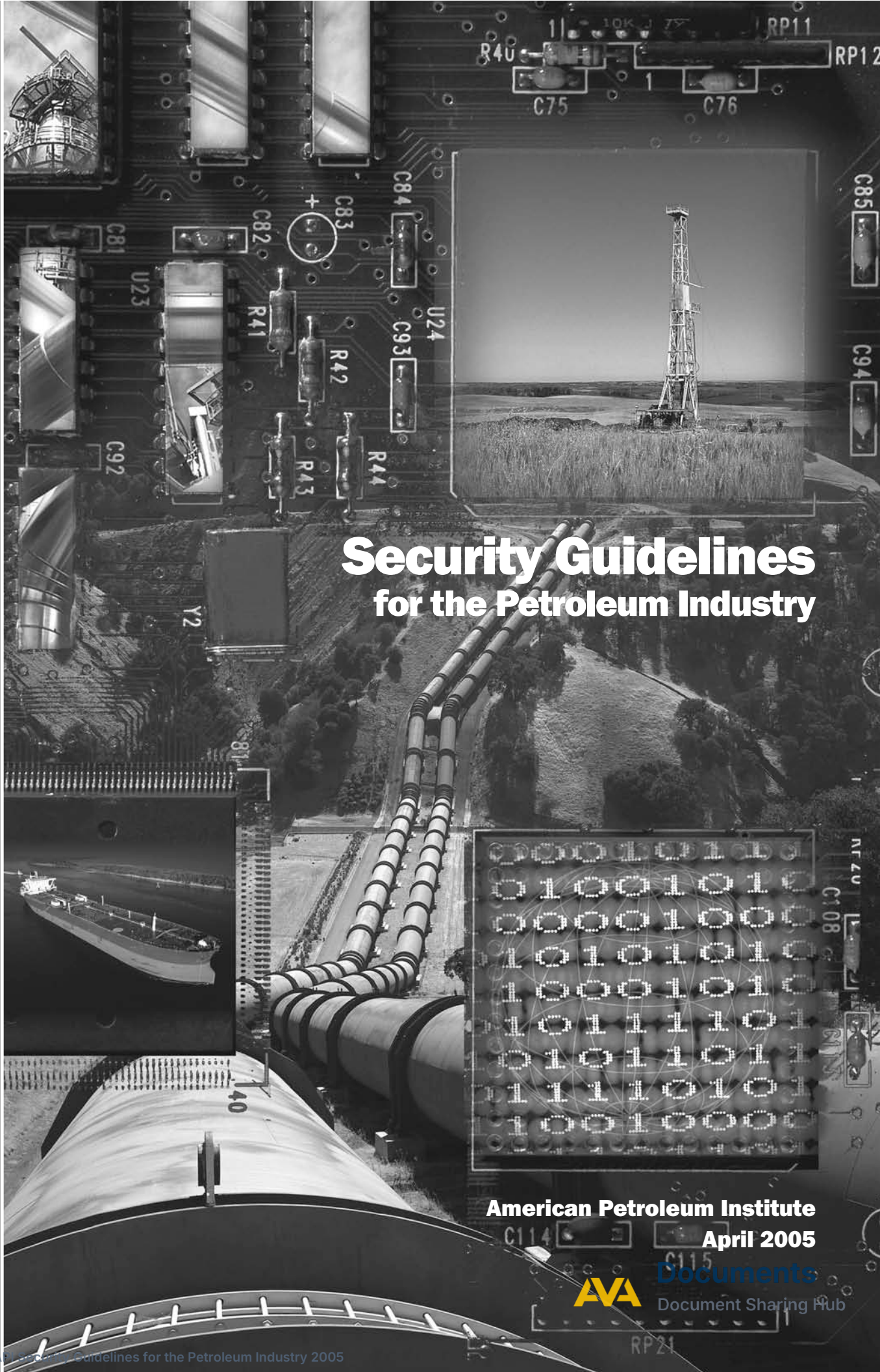
Liquid
Petroleum
Pipelines

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

Documents

Document Sharing Hub



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Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years.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.

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

Copyright © 2005 American Petroleum Institute

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

	Page
Executive Summary.....	vii
1.0 Introduction.....	1
1.1 Scope and Objective.....	1
1.2 Organization of the Document.....	1
1.3 Underlying Basis of this Guidance.....	2
1.4 Other Guidelines and Security References	2
2.0 Overview of Terrorism and the Petroleum Industry	3
2.1 Background on Terrorism and Security	3
2.2 Threat to the Petroleum Industry	3
3.0 Threat Assessment.....	4
3.1 The Value of Threat Assessment.....	4
3.2 Threat Assessment Process	4
3.3 Security Alert Level Systems.....	6
3.3.1 Introduction	6
3.3.2 Department of Homeland Security Alert System (HSAS).....	6
3.3.3 U.S. Coast Guard Maritime Security Levels	7
3.3.4 International Ship and Port Facility Security (ISPS) Alert Levels	8
4.0 The Security Management System Process	8
4.1 Initial Screening	9
4.2 Data Gathering	10
4.3 Initial SVA.....	10
4.4 Example Elements of a Security Plan	12
4.4.1 Security Administration & Organization of the Facility	13
4.4.2 Personnel Training	13
4.4.3 Drills and Exercises.....	14
4.4.4 Record and Documentation	14
4.4.5 Response to Change in Alert Level.....	14
4.4.6 Communications	15
4.4.7 Security Systems and Equipment Maintenance.....	15
4.4.8 Security Measures for Access Control, Including Designated Public Access Areas.....	15
4.4.9 Protected/Controlled/Restricted Areas	16
4.4.10 Security Measures for Monitoring	16
4.4.11 Security Incident Procedures	16
4.4.12 Audits and Security Plan Amendments	16
4.4.13 Security Vulnerability Analysis (SVA) Report	16
5.0 Security Vulnerability Assessment (SVA) Concepts	17
5.1 Security Vulnerability Assessment Overview	17
5.2 Steps in the SVA Process	18
5.3 Estimating Risk Using SVA Methods.....	19
5.4 Definition of SVA Terms	19
5.4.1 Risk Definition for SVA.....	19
5.4.2 Consequences (C).....	21
5.4.3 Threat (T)	22
5.4.4 Vulnerability (V).....	22
5.4.5 Target Attractiveness (A _T).....	22
5.5 Characteristics of a Sound SVA Approach	23
5.6 First Step in the SVA Process	23

5.7	SVA Strength and Limitations.....	24
5.8	Recommended Times for Conducting and Reviewing the SVA	25
5.9	Risk Control and Mitigation	25
5.10	Risk Screening	26
6.0	Security Conditions and Potential Response Measures.....	27
6.1	Low Condition—Green	27
6.2	Guarded Condition—Blue	28
6.3	Elevated Condition—Yellow	29
6.4	High Condition—Orange	29
6.5	Severe Condition—Red	30
7.0	Information (Cyber) Security	30
7.1	Introduction.....	30
7.2	Specific Security Guidelines.....	31
7.2.1	Security Policies, Standards and Procedures	31
7.2.2	Security Awareness and Education.....	32
7.2.3	Accountability and Ownership	32
7.2.4	Data/Information Classification.....	33
7.2.5	Security Vulnerability Assessments	33
7.2.6	Physical and Environmental Security	33
7.2.7	Access Controls and Identity Management	33
7.2.8	Network Security	34
7.2.9	Systems Development.....	34
7.2.10	Change Control.....	35
7.2.11	Viruses and other Malicious Code.....	35
7.2.12	Intrusion Detection and Incident Management.....	35
7.2.13	Business Continuity, Business Resumption and Disaster Recovery.....	35
7.2.14	Regulatory Compliance	36
7.2.15	Audit (Compliance and Assurance).....	36
Figures		
4.1	Security Management System Process.....	9
4.2	Example Elements of a Security Plan.....	13
5.1	Security Events Evaluated during the API SVA Process	18
5.2	API/NPRA Security Vulnerability Assessment Methodology.....	19
5.3	Example Risk Matrix.....	20
5.4	SVA Risk Definition	20
5.5	SVA Risk Variables	21
5.6	Target Attractiveness Factors.....	23
5.7	Times for Conducting and Reviewing the SVA	25
Tables		
3.1	Homeland Security Alert System.....	7
4.1	Examples of Petroleum Facility Assets Subject to Potential Security Risk.....	10
4.2	Examples of Security Risks or Threats in the Petroleum Industry.....	11
5.1	Questions to Determine SVA Approach Needed.....	24
Appendix A	Security Regulations Affecting the U.S. Petroleum Industry	37
Appendix B	Glossary and Terms	41
Appendix C	Communication of Security Intelligence	45
Appendix D	References	46

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 in 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 increased². 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 State³, 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 public 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 levels⁶.

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 1 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.