

First Edition

Confidential



Petroleum Refining

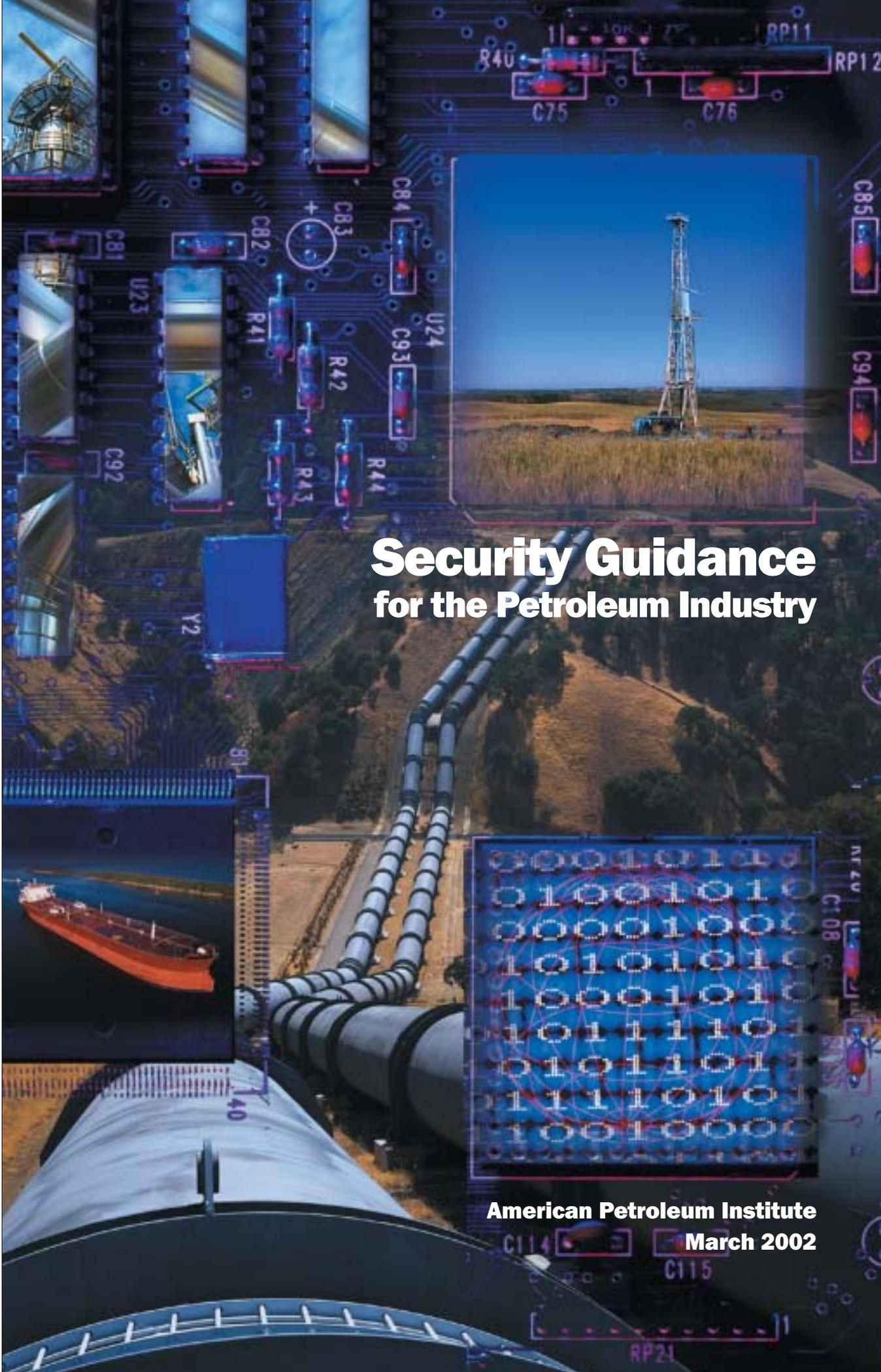
Pipeline Transportation (Liquids)

Petroleum Products Distribution and Marketing

Oil and Natural Gas Exploration and Production

Marine Transportation

Petroleum Cyber/Information Technology (IT) Infrastructure



Security Guidance for the Petroleum Industry

American Petroleum Institute
March 2002



Homeland Security Advisory System

SEVERE

Severe Risk of Terrorist Attacks

HIGH

High Risk of Terrorist Attacks

ELEVATED

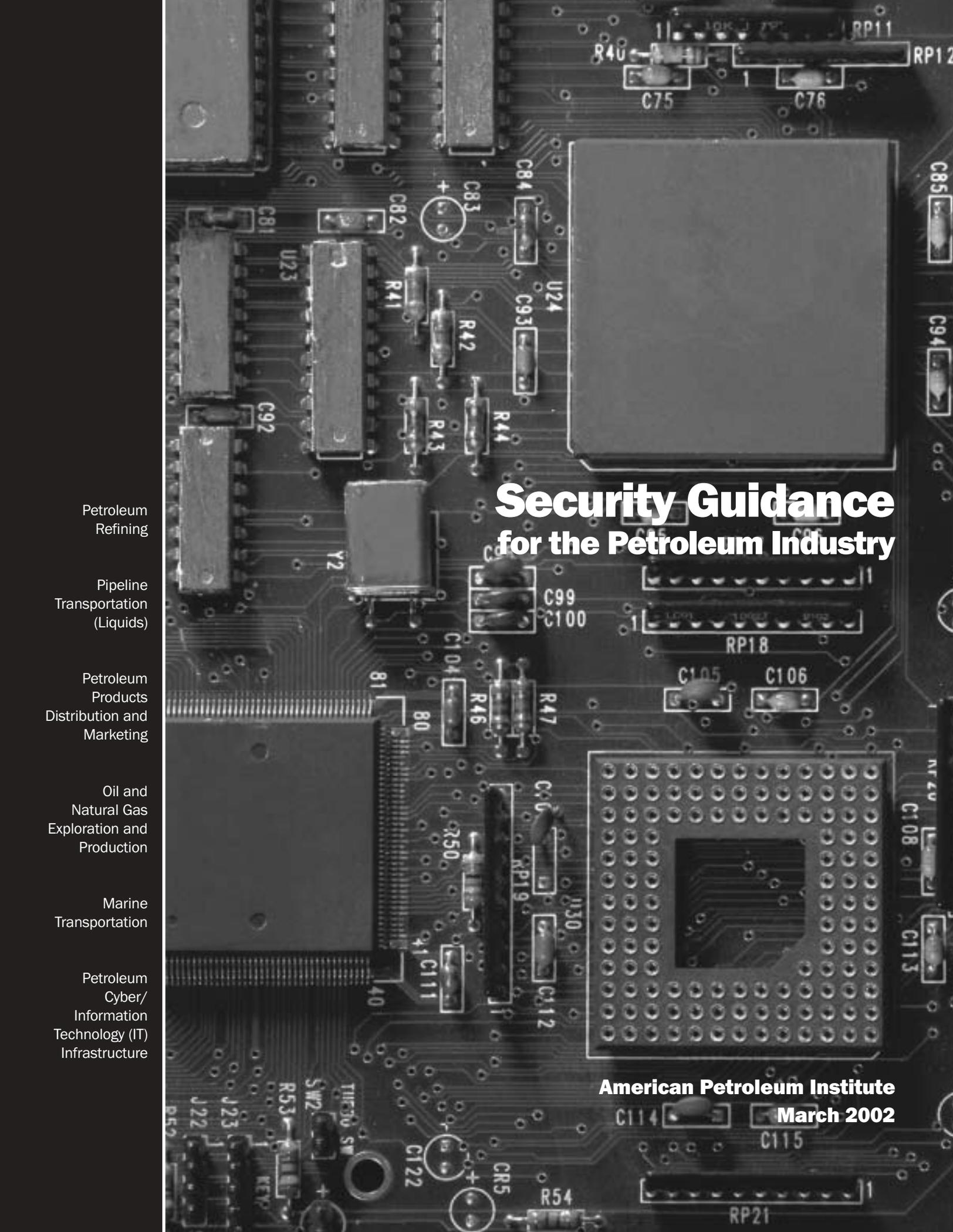
Significant Risk of Terrorist Attacks

GUARDED

General Risk of Terrorist Attacks

LOW

Low Risk of Terrorist Attacks



Security Guidance for the Petroleum Industry

Petroleum
Refining

Pipeline
Transportation
(Liquids)

Petroleum
Products
Distribution and
Marketing

Oil and
Natural Gas
Exploration and
Production

Marine
Transportation

Petroleum
Cyber/
Information
Technology (IT)
Infrastructure

American Petroleum Institute
March 2002

Contents

1.0 Introduction.....	1
2.0 Industry Overview.....	2
3.0 Definitions.....	3
4.0 Communication of Security Intelligence.....	4
5.0 Alert Levels.....	5
6.0 Elements of a Security Plan.....	7
7.0 Security Guidelines for Petroleum Refineries.....	10
8.0 Security Guidelines for Liquid Pipelines	24
9.0 Security Guidelines for Petroleum Products Distribution and Marketing.....	77
10.0 Security Guidelines for Oil and Natural Gas Production Operations.....	91
11.0 Security Guidelines for Marine Transportation.....	99
12.0 Cyber/Information Technology Security Guidelines for the Oil and Natural Gas Industry.....	102

This document is intended to offer security guidance to the oil and natural gas 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 operator efforts. With respect to particular circumstances, local, state and federal laws and regulations should be reviewed.

Please treat this information as sensitive, and for use by oil and natural gas companies and associations, and when needed to ensure national security, for use by Congress as well as appropriate federal agencies and state and local legislative and regulatory entities. This document is not intended for wider public or media distribution.

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

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

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

Executive Summary

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

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

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

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

1.0 Introduction

Recognizing the vital importance of safe, reliable energy supplies to our nation's prosperity, security has always been a top priority at oil and natural gas facilities. From designing safe and secure facilities to protecting plants and infrastructure to training with local emergency response teams, companies have long recognized and responded to the need to protect their workers, communities, and energy supplies through a variety of standards and procedures. These efforts, in addition to serving as a protection for the general public, can be effective against acts of vandalism, theft and other types of attacks.

Like other industries, since September 11, the oil and natural gas industry has taken steps to reevaluate potential threats to the industry and enhance the physical and operational security of its facilities, its workers and data. The oil and natural gas industry has also taken steps to improve channels of communication to quickly disseminate government intelligence concerning potential acts of terrorism. In doing so, each sector of the petroleum industry has needed to assess the risks it faces along with potential deterrence or response measures. The general risks to energy supply and vulnerability varies by segment of the petroleum industry, which we define broadly for these purposes as oil and natural gas exploration and production, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing. Electronic data, hardware and software, prevalent throughout the high tech oil and natural gas industry, are logically treated separately with respect to security.

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

- Assessed the general types of risks to supply interruptions that each sector may face;
- Identified existing standards, recommended practices, guidance and other operational practices, as well as ongoing initiatives that may mitigate those risks or vulnerabilities; and
- Worked with other industry associations and member companies to prepare appropriate guidance.

2.0 Industry Overview

The risks from terrorist attacks to U.S. energy supplies vary by segment of the petroleum industry. The industry's facilities and assets are widely distributed, consisting of over 300,000 producing sites, 4,000 offshore platforms, more than 600 natural gas processing plants, over 160,000 miles of pipelines (petroleum liquids), multiple oil offloading ports and facilities, 153 refineries, and more than 1,400 product terminals, 7,500 bulk stations and 170,000 gasoline retail stations. This wide distribution of domestic assets means that it is very difficult to interrupt, in any material way, the distribution of petroleum and petroleum products in the U.S. by targeting a single, or a few, facilities. Also, a large majority of these facilities are small, geographically remote, or difficult to use as an instrument for terrorist purposes.

3.0 Definitions

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 security measures may be implemented based on the level of threat to the facility.

Operator – A person or company who owns and/or operates oil and natural gas facilities.

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

Risk assessment – A process in which potential hazards from facility operation are identified, and the likelihood and consequences of potential adverse events are determined. Risk assessments can have varying scopes, and be performed at varying level of detail depending on the operator's objectives.

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.

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.

Segment – an aspect of the oil and natural gas industry that represent one of the steps needed to find, produce, process and transport oil and natural gas 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 oil and natural gas exploration and production, petroleum refining, pipeline transportation (liquids), marine transportation, and petroleum products distribution and marketing.

Threat – Information received by an operator which if carried out could impact the integrity of the pipeline system with consequences to the personnel, operations, and business interests of the operator.

Vulnerability – A measure or indication of a facility's susceptibility to a security threat.

4.0 Communication of Security Intelligence

One important key to prevent acts of terror and to protect facilities lies in good intelligence, and the quick dissemination of information to the large number of operators that may need the information. After September 11th, the oil and natural gas industry acted quickly to develop an effective information dissemination structure, with API taking the lead role in interfacing with key government agencies and disseminating government intelligence concerning potential acts of terrorism to the industry. API is providing this role until the Energy Information Sharing and Analysis Center (ISAC) can take over this critical function.

Although ISACs for other industries have been up and running for several years, particularly related to cyber threats, the Energy ISAC was just recently created based on a recommendation of the National Petroleum Council in its June 2001 report, *Securing Oil and Natural Gas Infrastructure in the New Economy*. The Energy ISAC, managed by Global Integrity, was created as a limited liability corporation and began official operation on November 1, 2001.

5.0 Alert Levels

5.1 Introduction

Alert levels describe a progressive qualitative measure of the likelihood of terrorist actions, from negligible to imminent risk of attack or action, based on government or company intelligence information. There are three relevant alert level systems that have been developed by the government or government/industry partnerships to warn of the potential for acts of terrorism:

- A 5 alert system based on the National Threat Advisory System developed by the Office of Homeland Security.
- A 5 alert system used by the petroleum pipeline segment and developed in conjunction with the Office of Pipeline Safety, based on the security alert system developed by the U.S. Department of Energy (DOE).
- A 3 alert system developed by the U.S. Coast Guard for use by marine vessels and ports.

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

5.2 Office of Homeland Security Alert Levels

A Homeland Security Advisory System was issued by the Office of Homeland Security on March 12, 2002. The alert levels are:

- **Low Condition - Green:** this condition is declared when there is a low risk of terrorist attacks.
- **Guarded Condition - Blue:** This condition is declared when there is a general risk of terrorist attacks.
- **Elevated Condition - Yellow:** An Elevated Condition is declared when there is a significant risk of terrorist attacks.
- **High Condition - Orange:** A High Condition is declared when there is a high risk of terrorist attacks.

- **Severe Condition - Red:** A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time.

5.3 Petroleum Pipelines Security Conditions

The petroleum pipelines segment, working in conjunction with the Office of Pipeline Safety, has adopted an alert system of 5 security conditions (SECON), which are based on a security alert system developed by the U.S. Department of Energy (DOE). The security condition alert levels are:

- **SECON-5:** Threat negligible - this condition exists when a general threat of possible terrorist activity or civil unrest exists but warrants only routine security measures associated with daily operations. **SECON-5** is for normal operating conditions.
- **SECON-4:** Threat low – this condition exists when there is an increased general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher SECON measures.
- **SECON-3:** Threat medium – this condition applies when an increased and more predictable threat of terrorist activity exists.
- **SECON-2:** Threat high – this condition applies when an incident occurs or information is received indicating that some form of terrorist action against personnel and facilities is imminent.
- **SECON-1:** Threat critical – this condition applies in the immediate area where a terrorist attack has occurred which may affect the facility or when an attack is initiated on the facility and its personnel. Normally, this SECON is declared as a localized condition at the affected facility.

5.4 Maritime Security Conditions

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

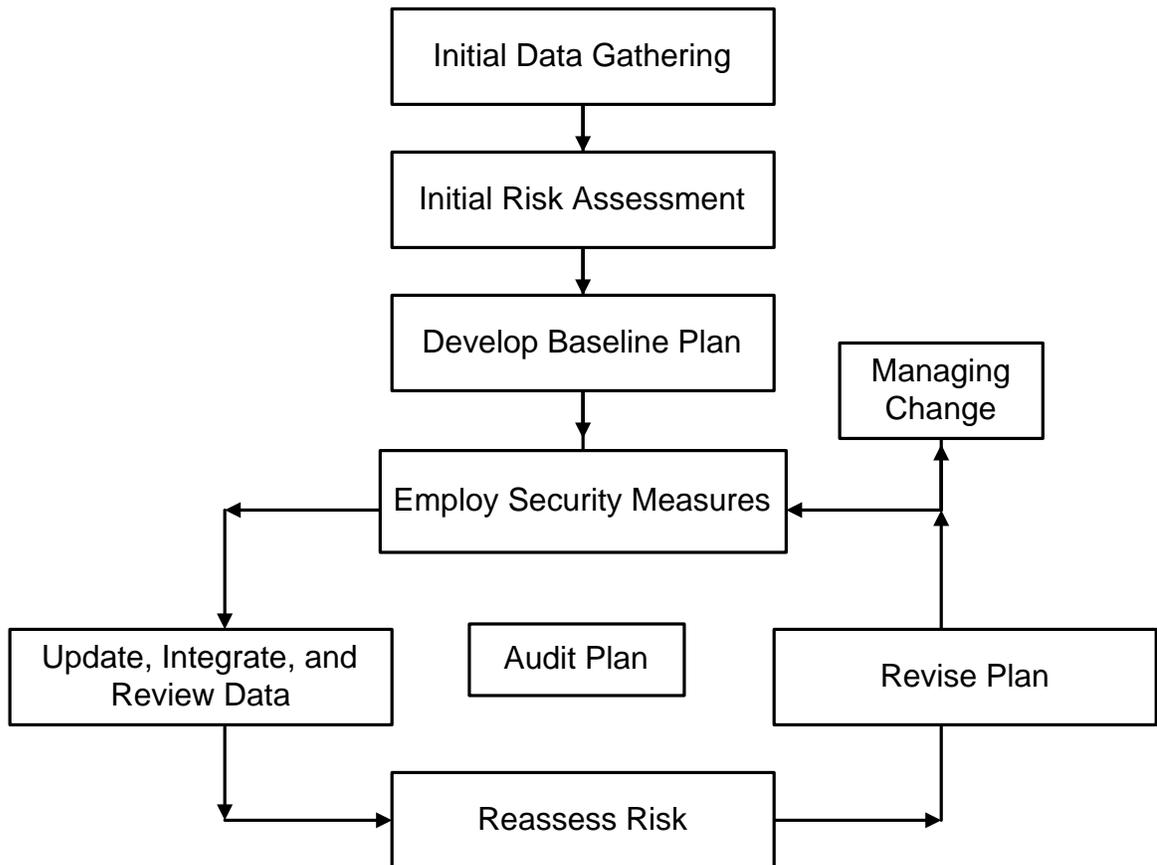
- **MARSEC I:** Low or Moderate Threat – this alert is defined as the “new normalcy”.
- **MARSEC II:** Heightened Alert – this alert is issued when there is credible intelligence suggesting a high threat, but no specific target or delivery method is known.
- **MARSEC III:** Maximum Alert – this alert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

6.0 Elements of a Security Plan

All oil and natural gas facilities have unique design features and operating characteristics, necessitating individualized facility security plans. An effective security plan should have a solid base of several essential elements. Figure 6.1 illustrates a typical security plan framework.

The framework shown in Figure 6.1 provides a common structure upon which to develop an operator specific security plan. In developing a security plan, operators should consider their unique security risks, and then assess the risks to assure the plan addresses key risks. There are many different approaches to implementing the different elements identified in Figure 6.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no “best” approach that is applicable to all oil and natural gas facilities for all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

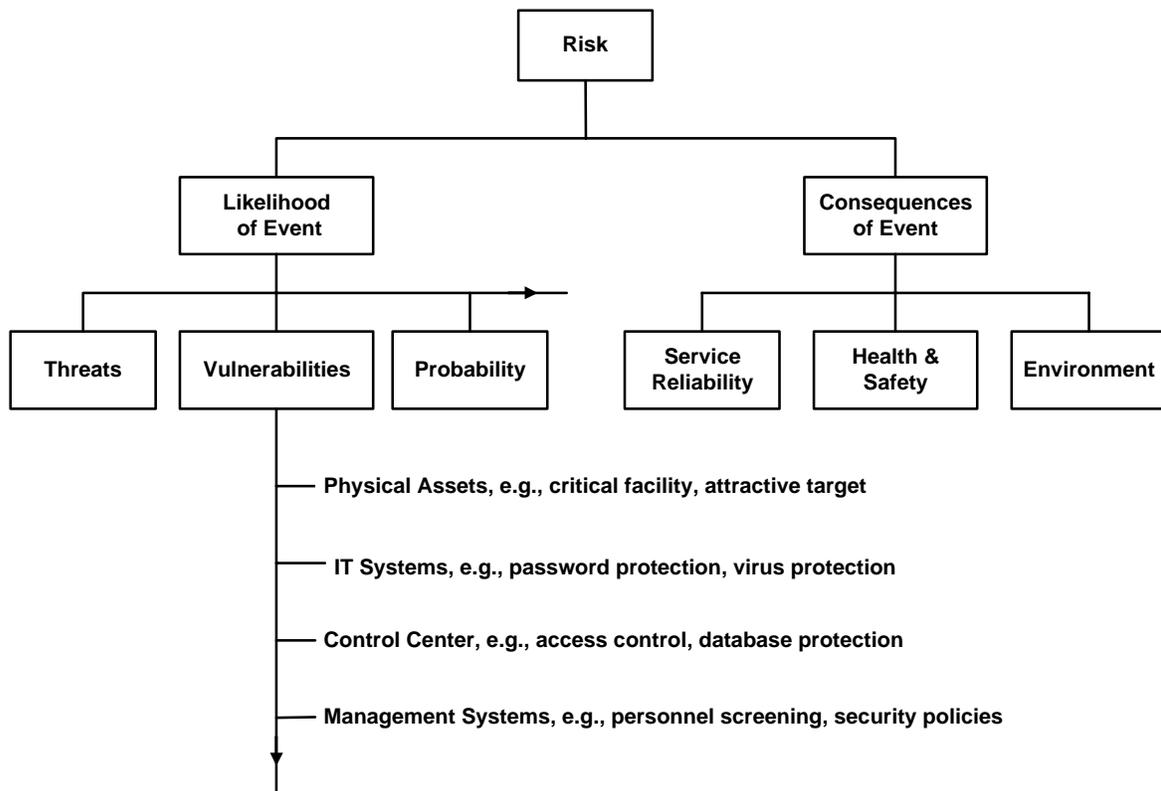
Figure 6.1
Framework for a Security Plan



It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 6.1 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 risk assessment approach depends in part on what risk related data and information are available. Conversely and while performing a risk assessment, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and risk assessment elements could be highly integrated and iterative.

The overall risk to a facility or operation is a function of the likelihood of a security related event or condition to lead to an interruption of services, and the consequence in the event of an interruption of services. Both components of threat and vulnerability which lead to risk must be considered when conducting a risk assessment and in making prudent risk-based decisions. Figure 6.2 provides a simple depiction of risk.

Figure 6.2
Risk Assessment Structure



There are many risk assessment techniques and methods available but they all have these common elements. Ultimately, it is the responsibility of the operator to choose the risk assessment method that best meets the requirements of the risk assessment task.

Independent of the risk assessment method used, all techniques incorporate the same basic components:

1. Identify potential security related events or conditions that threaten the system's service or integrity.
2. Determine risk represented by these events or conditions by determining the likelihood of an interruption in services and the consequences of an interruption in services.
3. Rank risk assessment results.
4. Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses)
5. Integrate security plan and evaluations, e.g., drills and audits
6. Re-assess risk

An overview of the individual security plan framework elements as they pertain to the individual industry segments is provided the segment sections that follow.

7.0 Security Guidelines for Petroleum Refineries

7.1 Purpose & Objective

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

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

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

This guideline outlines a process that a refinery security manager or team can use to assess risks and make decisions about risks in operating a refinery, and to make progress towards the goal of reducing the risks associated with refinery operations. Section 7.7 describes the framework for creating a refinery security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 7.1.

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

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

7.2 Overview of Segment Operations

There are 153 refineries in the U.S., which have a combined operating capacity of about 16.5 million barrels per day. The average refining capacity of these refineries is about

110,000 barrels per day. Many of these refineries are located on the West and Gulf coasts, primarily because of access to major sea shipping routes. These refineries process crude oil into a variety of petroleum products such as gasoline, heating oil, jet fuel and asphalt.

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

For refineries, some specific examples of enhanced security measures include:

- Increased identification checks of all persons entering facilities
- Conducting new and revising existing security/threat scenario assessments
- Initiated detailed checks of all vehicles entering facilities
- Established heightened security procedures for handling packages entering facilities
- Enhanced perimeter protection against vehicular intrusion
- Bolstered security procedures for ship personnel disembarking the ship onto facility docks
- Increased perimeter security by additional security guards and surveillance equipment
- Restricted vehicle access to and from facilities
- Background checks of employees and contractors
- API co-sponsored a joint conference with NPRA, ACC and SOCMA on plant security for refiners and chemical manufacturers in February. The conference emphasized best practices and benchmarking. The event attendees shared experiences on security issues, such as what to do about contractors and other people inside the refinery, information collection and sharing, perimeter protection, and transportation at and near the facility. Senior officials from the U.S. Department of Energy, the FBI, the National Infrastructure Protection Center (NIPC), and the Energy Information Sharing and Analysis Center (ISAC) also attended the conference.

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

7.4 Security Guidelines

The following provide general security guidance for petroleum refinery operations relative to potential acts of terrorism:

- Each operator should assess the risk and impact of a terrorist attack. The assessment may include a determination of the likelihood of an act or attack, the

- type of terrorist action and the size and location of the refinery. The assessment may include: 1) the potential risk to workers, 2) the potential risk to the surrounding community; 3) the potential impact to the local and national energy supply; and 4) the potential risk to adjacent facilities and infrastructure.
- After conducting the assessment, the operator should develop a security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, or event, and; 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets and terrorist tactics and periodically tested, as appropriate.
 - Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout its organization. Operators should respond appropriately to this information to safeguard potential targets. Operators should also, as appropriate, report suspicious activities and behaviors, attempted incursions, terrorists' threats, or actual events to the appropriate agencies. The Energy Information Sharing and Analysis Center (Energy ISAC) is an avenue to stay informed of intelligence and threat information.
 - Each operator should establish clear communication channels and responsibilities for assessing, preparing for, responding to and recovering from potential or actual threats.
 - Operators should be aware of existing regulations, standards and operating practices as they relate to refinery security.

7.5 Elements of a Refinery Security Management Plan

In developing a refinery security management plan, several basic elements should be considered. The refinery security management plan framework shown in Figure 7.1 provides a general structure upon which a security management plan can be developed. When developing a refinery security management plan, one should consider, to the extent possible, the refinery's unique security risks, and then, if possible, assess the risks to ensure the plan addresses them. There are many different approaches to implementing the different elements identified in Figure 7.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all facilities. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a refinery security management plan could be a highly integrated and iterative process. Although the elements depicted in Figure 7.1 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 risk assessment approach depends in part on what risk related data and information are available. Conversely and while performing a risk assessment, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and risk assessment elements could be highly integrated and iterative.

A refinery security management plan could include elements such as:

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

7.6 Security Management Plan Framework

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

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

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

- Vehicles
- Process units
- Control rooms and associated control systems
- Electrical power lines (including back-up power systems)
- Natural gas lines
- Storage tanks
- Boilers, turbines and process heaters
- Water supply
- Sewer systems

- Wastewater treatment units
- Railroad lines
- Pipelines entering and leaving plants
- Ships, dock area and associated equipment

Initial Risk Assessment. In this element, the data assembled from the previous step is used to conduct a risk assessment. The risk assessment 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 risk assessment process identifies the location-specific security-related events or conditions, or combinations of events and conditions, that could lead to loss of security, and provides an understanding of the likelihood and consequences of these events. If possible, the output of a risk assessment should include the nature and location of the most significant risks.

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

Examples of security risks or threats for refineries can include:

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

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

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

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

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

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that might lead to system failures are controlled. As noted previously, a risk assessment may identify other risks that should be addressed.

Examples of physical security elements for refineries could include:

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

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

Reassess Risk. Risk assessments 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 risk assessment, 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 risk assessments to ensure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The baseline security management plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of

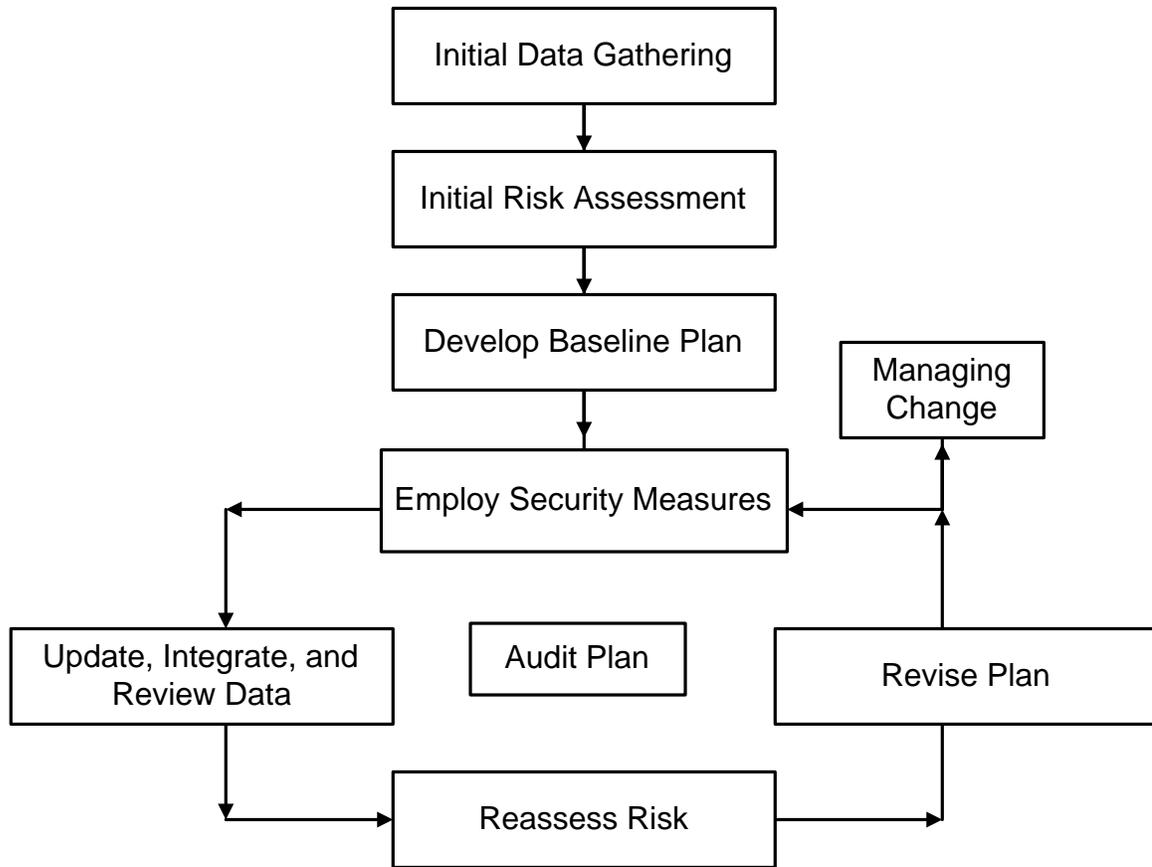
previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated risk assessment results should also be used to support scheduling of future security assessments.

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

Managing Change. A systematic process should be used to ensure that changes to a facility or its operations are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future risk assessments to be sure the risk assessment 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 7.1, a security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. Risk assessments must be periodically updated and revised to reflect current vehicle or facility conditions so operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

Figure 7.1
Framework for a Security Plan



7.7 Security Conditions and Potential Response Measures

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

Each operator should develop a means to advise and communicate to operator personnel and others as warranted the security condition at the refinery and otherwise as applicable.

The potential measures associated with each alert level are not prioritized but those implemented should be initiated concurrently where practical and as applicable. Refinery management should maintain a record of specific actions taken for each alert level. Following is a detailed explanation for each alert level and the potential response measures associated with each level:

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

Access Control/Perimeter Protection

- Having all contractors and visitors check or sign in and out of the refinery at designated location(s).
- Ensuring existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting. Identifying those additional security measures and resources that could enhance the security at the higher alert levels, e.g. increased surveillance or lighting.

Communications

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

Training/Policies/Procedures/Plans

- Developing terrorist and security awareness information and providing education to employees on security standards and procedures. Cautioning employees not to talk with outsiders concerning their facility or related issues.
- Advising all refinery personnel to report the presence of unknown personnel, unidentified vehicles, aircraft or watercraft, vehicles, watercraft or aircraft operated out of the ordinary, abandoned parcels or packages, and other suspicious activities.
- Developing procedures for shutting down and evacuation of the refinery, if considered necessary, in case of imminent attack.
- Incorporating security awareness and information into public education programs and notifications to emergency response organizations as appropriate.
- Surveying surrounding areas to determine those activities that might increase the security risks that could affect the refinery, e.g., airports, government buildings, industrial facilities, and other facilities.

CONFIDENTIAL

- Ensuring contingency and business continuity plans are current and include a response to terrorist threats.
- Reviewing existing emergency response plans and modifying them, if required, in light of potential threats.

Cyber Security

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

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

Perimeter Protection/Access Control

- Securing all facilities, buildings and storage areas not in regular use, if possible. Increasing frequency of inspections and patrols within the refinery, including the interior of buildings and along the refinery perimeter.
- Inspecting perimeter fencing and repairing all fence breakdowns. In addition, reviewing all outstanding maintenance and capital project work that could affect the security of the refinery.
- Reducing the number of access points, if possible, for vehicles, aircraft, watercraft and personnel to minimum levels and periodically spot checking the contents of vehicles, watercraft, or aircraft at the access points. Being alert to vehicles or watercraft parked or moored for an unusual length of time in or near a refinery.
- Checking designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increasing surveillance in designated areas.
- Requiring visitors to check in at a refinery office and verifying their identification - being especially alert to repeat visitors or outsiders who have no apparent business at the refinery and are asking questions about the refinery or related issues including the refinery's personnel. Familiarizing refinery personnel with vendors who service the refinery and investigating unusual changes in vendor personnel.

CONFIDENTIAL

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

Communications

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

Training/Policies/Procedures/Plans

- Reviewing all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.
- Ensuring that an operator response can be mobilized appropriate for the increased security level. Reviewing communications procedures and back-up plans with all concerned.

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

Perimeter Protection/Access Control

- Closing and locking gates and barriers except those needed for immediate entry and egress. Inspecting perimeter and perimeter fences on a regular basis. Ensuring that other security systems are functioning and are available.
- Inspecting on a more frequent basis the interior and exterior of all buildings and around all storage tanks and other designated critical areas.
- Dedicating personnel to assist with security duties with duties to monitor personnel entering the refinery and to inspecting the area on a regular basis, reporting to refinery management as issues surface.
- Limiting visitors and confirming that the visitor has a need to be and is expected at the refinery. Escorting visitors while at the refinery.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements

that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.

- Advising appropriate agencies that the refinery is at a **Yellow** level and advising the measures being employed - requesting agencies to increase the frequency of their routine patrol of the refinery if possible.
- Checking to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirming availability of security resources that can assist with extended coverage, if needed.
- Identifying areas where explosive devices could potentially be hidden.
- Instructing employees working alone to check-in on a periodic basis.
- Directing that all personal, operator, and contractor vehicles at the refinery are secured.

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

Perimeter Protection/Access Control

- Reducing refinery access points to the absolute minimum necessary for continued operation.
- Securing a trained and knowledgeable security workforce at the refinery - ensuring that all security personnel have been briefed concerning policies governing the use of force and pursuit.
- Increasing security patrol activity to the maximum level sustainable. Increasing perimeter patrols and inspections.
- Checking all security systems such as lighting and intruder alarms to ensure they are functioning. Installing additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.
- Prohibiting unauthorized or unidentified vehicles/personnel entrance to the refinery.

CONFIDENTIAL

- Inspecting all vehicles entering the refinery, if possible, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed. Inspecting all packages and cargo being delivered by aircraft or watercraft.
- Limiting access to the refinery to those personnel who have a legitimate and verifiable need to enter. Implementing positive identification of all personnel. Evacuating all non-essential personnel.
- Implementing frequent inspection of the refinery including the exterior and roof of all buildings and parking areas. Increasing patrolling or inspections at night and ensuring all vulnerable critical points are fully illuminated and secure.
- Protecting the refinery from an attack by a parked or moving vehicle - operator vehicles may be used for this purpose. Implementing centralized parking and shuttle service where feasible.
- Canceling or delaying all non-vital refinery work conducted by contractors, or continuously monitor their work with operator personnel.

Communications

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

Training/Policies/Procedures/Plans

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

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

Perimeter Protection/Access Control

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

Training/Policies/Procedures/Plans

- Continuing **Orange** and **Yellow** measures or introducing those that have not already been implemented.
- Consider shutting down the refinery and operations in accordance with contingency plans unless there is a compelling reason not to and evaluating security prior to resuming operations if they are temporarily shut down.
- Implementing business contingency and continuity plans as appropriate.

8.0 Security Guidelines for Liquid Pipelines

8.1 Introduction

8.1.1 Purpose and Objectives

The goal of all operators of liquid pipelines is to operate and maintain the pipelines in such a way that there are no adverse effects on employees, the environment, the public, or the customers as a result of the pipeline company's actions or actions from other parties. This is done to satisfy the needs of the customer while earning a reasonable return on the investment.

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

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

This guideline outlines a process that an operator of a pipeline system can use to assess risks and make decisions about risks in operating a hazardous liquid pipeline, and to make progress towards the goal of reducing the risks associated with operating a pipeline system. Section 8.7 describes the framework for creating a pipeline security plan that forms the basis of this guideline. This framework is illustrated schematically in Figure 8.1.

This guideline is intended for use by individuals and teams charged with creating, implementing, and improving a pipeline security program. Typically a team would include risk managers, security personnel, engineers, operating personnel, and technicians or specialists with specific experience or expertise, e.g., risk assessment, threat identification, and risk mitigation. Users of this guideline should be familiar with the pipeline safety regulations (Title 49 CFR Part 195).

8.1.2 Guiding Principles

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

- A pipeline security program must be flexible.

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

- The integration of information is a key component to managing a pipeline security program.

A key element of the security management framework is the integration of all available information in the decision making process. Information that can impact an operator's understanding of the important risks to a pipeline system comes from a variety of sources. The operator is in the best position to gather and analyze this information. By integrating all of the available information, the operator can determine where the risk of an incident are the greatest, and make prudent decisions to reduce the risk. Operators have multiple options available to address risks. Components of the facility or system can be changed; additional training can be provided to the people that operate the system; processes or procedures can be modified; or a combination of actions can be used that will have the greatest impact on reducing risk.

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

Risk assessment is an analytical process through which an operator determines the types of adverse events or conditions which might impact pipeline security, the likelihood that those events or conditions will lead to a security related event, and the nature and severity of the consequences that might occur following an event. This analytical process involves the integration and analysis of the pipeline system and its facilities, the environment in which the pipeline operates, and risk reduction methods available to the pipeline operator. Risk assessments can have varying scopes, varying levels of detail, and use different methods. However, the ultimate goal of assessing

risks is to identify and prioritize the most significant risks so that an operator can make informed decisions about these issues.

- Assessing risks to pipeline security is a continuous process.

Analyzing for risks in a pipeline system is an iterative process. The operator will periodically gather additional security related information and system operating experience. This information should be factored into the understanding of system risks. As the significance and relevance of this additional information to risk is understood, the operator may need to adjust its security plan accordingly. This may result in changes to risk assessment methods or frequency, or additional modifications to the pipeline security plan in response to the data. As changes are made, different pipelines within a single operating company and different operators will be at different places with regard to the goal of risk reduction.

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

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

- All pipeline operators should use a standardized set of security alert conditions and response measures.

Section 8.15 of this guideline provides a standardized set of security alert conditions and response measures for use by operators in the liquid pipeline industry. The security alert conditions describe a progressive level of protective measures that should be implemented in response to the possibility of a terrorist threat or to a terrorist threat directed at liquid pipeline facilities, assets, and personnel. The purpose of such a system is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and company personnel prior to and during a threat crisis.

8.2 Scope

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

This guideline is specifically designed to provide the operator with a description of industry practices in pipeline security management. The guidance is specific to pipeline

segments and facilities, and the process and approach can and should be applied to all pipeline facilities including pipeline stations, terminals, pipe segments, valve sites, delivery and receipt locations, and control centers associated with pipeline systems.

8.3 Terms, Definitions, and Acronyms

Operator – A person who owns or operates pipeline facilities. Definition based on 49 CFR Part 195.

Pipeline 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.

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

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

Risk assessment – A systematic, analytical process in which potential hazards from facility operation are identified, and the likelihood and consequences of potential adverse events are determined. Risk assessments can have varying scopes, and be performed at varying level of detail depending on the operator's objectives (See Section 6).

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 on a pipeline system to reduce the security risk to the pipeline system.

Shall – The term “shall” is used in this standard to indicate those practices that are mandatory.

Should – The term “should” is used in this standard to indicate those practices which are preferred, but for which operators may determine that alternative practices are equally or more effective or those practices for which engineering judgement is required.

Threat – Information received by an operator which if carried out could impact the integrity of the pipeline system with consequences to the personnel, operations, and business interests of the operator.

Vulnerability – A measure or indication of a pipeline system’s susceptibility to a security threat.

8.4 Overview of Segment Operations

Oil pipelines, both crude oil and refined petroleum products, are the most significant mode of petroleum transportation in the U.S. Pipelines carry 68% of oil transported (in barrel-miles), while water transportation accounts for 27%, trucks 3% and rail 2%. Nationwide there are some 160,000 miles of oil pipelines, excluding intra-state systems and gathering lines associated with crude oil production (see E&P segment operations). The vast majority of oil pipeline assets are buried, providing limited access to the cross-country lines themselves.

The concentrations of pipeline assets vary across the United States based on whether regions of the country are net producing regions or net consuming regions. For example, the Gulf Coast region is the largest supply area of the U.S, while the East Coast has virtually no indigenous crude oil production and the highest regional refined product demand. Pipelines play a key role in moving oil from producing areas and coastal ports to refineries and from refineries and large redistribution centers to smaller regional supply centers. Logistics hubs provide for the interconnections of major pipeline systems.

Pipeline systems vary from large diameter, large throughput major systems to small diameter, small throughput pipelines and run the gamut in between. Each pipeline operator maintains relationships with the shippers on its systems. Shippers also vary widely, including major integrated oil companies, power plants, airports, municipalities, defense facilities, and many others.

Pipeline operators have long recognized the importance of system reliability, both to themselves as operators, to the shippers that transport on their systems and to the consuming public. As such all operators have effective emergency response plans and the capability to rapidly restore service disruptions, regardless of the initiating event. Operators also have mutual aid agreements in place to augment emergency response capability in areas where multiple operators' systems converge, such as logistics hubs. The capability of operators to recover has been proven by responses to accidents in the past.

8.5 Relevant Operations Standards and Industry Practices

The federal government through the U.S. Department of Transportation Office of Pipeline Safety regulates the oil pipeline industry. The federal regulations address design, construction, operations, maintenance, testing, emergency response planning, and overall pipeline system integrity. Many aspects of the federal regulations address safety and security issues. The oil pipeline industry, along with its natural gas counterparts, works in cooperation with the Office of Pipeline Safety.

The oil pipeline industry has used a risk management approach to ensuring pipeline system reliability and integrity. One key industry standard is API 1160, Managing

System Integrity for Hazardous Liquid Pipelines. This standard lays out a framework for conducting risk assessments for pipeline systems.

8.6 Ongoing Initiatives/Additional Measures Implemented

Since September 11, several efforts have been undertaken by the oil pipeline industry to enhance security:

- The oil pipeline industry has developed a set of standardized security condition alert levels based on the U.S. Department of Energy (DOE) security conditions.
- The oil pipeline industry has drafted a set of countermeasures that operators can implement as threat conditions change. Operators would build on these standard measures for those critical company assets that require additional protections. These protective measures are company specific and necessarily confidential.
- The oil pipeline industry is drafting a guidance document based on the principles of risk management and risk assessment specific to security preparedness.
- The oil pipeline industry is recommending to operators that company personnel apply for and maintain appropriate security clearances and develop appropriate networks related to security information, including contacts with the FBI, the National Infrastructure Protection Center, and federal, state and local law enforcement, as appropriate.

Individual pipeline operators have been evaluating their own security preparedness and the relative vulnerability of systems or system components. Both the likelihood and potential consequences of potential terrorist acts vary widely for individual operators dependent on the size, complexity, location, product moved, and associated facilities for particular assets.

Many operators have instituted additional security measures. Such enhanced security measures include:

- Enhanced verification and identification procedures for persons entering pipeline facilities, including control centers, manned facilities, and tank farms.
- Review of company emergency response capability considering the potential for terrorist activities.
- Review of company physical security preparedness (gates, fences, lighting, surveillance).
- Increased employee awareness of security, including bomb threat procedures, mail handling procedures, package inspection, and vehicle security.

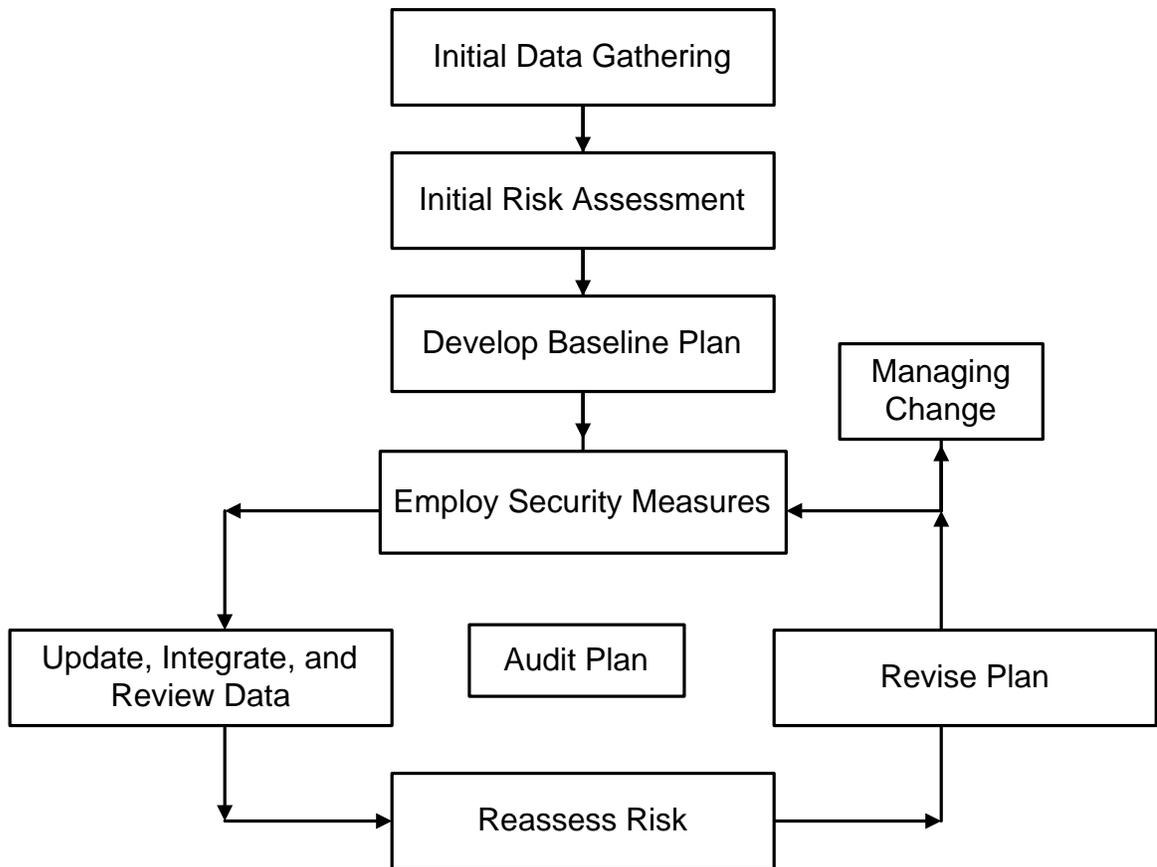
8.7 Pipeline Security Plan

8.7.1 Essential Elements:

All pipeline systems have design features and operating characteristics that are unique to each system. An effective *pipeline security plan* should have a solid base of several essential elements. This section describes a program that includes the essential elements and is the basis for this guideline. Figure 8.1 illustrates a pipeline security plan framework.

The framework shown in Figure 8.1 provides a common structure upon which to develop an operator specific pipeline security plan. In developing a pipeline security plan, operators should consider their unique security risks, and then assess the risks to assure the plan addresses all of the known risks. There are many different approaches to implementing the different elements identified in Figure 8.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no “best” approach that is applicable to all pipeline systems for all situations. This guideline recognizes the importance of flexibility in designing pipeline security plans and provides guidance commensurate with this need.

Figure 8.1
FRAMEWORK FOR A PIPELINE SECURITY PLAN



It is important to recognize that a pipeline security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 8.1 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 risk assessment approach depends in part on what risk related data and information are available. Conversely and while performing a risk assessment, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and risk assessment elements could be highly integrated and iterative.

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

8.7.2 Framework Elements

Initial Data Gathering. The first step in understanding the potential risks along the pipeline system is to assemble information about potential risks. In this element, the operator performs the initial collection, review, and integration of data that is needed to understand location-specific risks to the pipeline security. The types of data to support a

risk assessment include information on the operation, surveillance practices, security measures, and the specific security issues and concerns that are unique for each system. Section 8.8 provides a summary of useful data sources, common data elements that are typically used in risk assessment, and approaches to data review and integration. For operators that are just formalizing an approach to a pipeline security plan, the initial data gathering may be focused on a limited number of facilities or assets so that a screening for the most significant security risks can be readily identified.

Initial Risk Assessment. In this element, the data assembled from the previous step is used to conduct a risk assessment of the pipeline system. The risk assessment begins with a systematic and comprehensive search to identify possible security risks to the pipeline system. The identification of potential risks should not be limited to a review of known risk categories, but should also include steps to look for new or unique manifestations of risks. Through the integrated evaluation of the information and data collected in the previous step, the risk assessment process identifies the location-specific security related events or conditions, or combinations of events and conditions, that could lead to loss of pipeline security, and provides an understanding of the likelihood and consequences of these events. The output of a risk assessment should include the nature and location of the most significant risks on the pipeline system. There is a significant variation in the detail and complexity associated with different risk assessment methods. Some operators without formal risk assessment processes have found that an initial screening level risk assessment can be beneficial in terms of focusing resources on the most important areas. During a screening risk assessment, an operator may limit the scope of the system to those portions of the system where a failure could have the most severe consequences, e.g., interruption of a strategic or high volume supply or an HCA event. Similarly, risk assessment and data collection may be focused to support identification of the most likely security targets at those facilities or pipeline segments, without going into extensive detail. Some operators may find a screening approach as the most practical approach to prioritize facilities or pipeline segments for risk assessment. After identifying the most significant risks on the system, the next step is to determine what mitigation actions or security measures might be desirable to reduce risk, and where assessment techniques such as facility or pipeline security inspections would be of the most value in identifying potential risk-threatening issues. The risk control and mitigation process involves:

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

Risk assessment also helps to identify and prioritize likely targets and avoid expending resources where the likelihood of attack is remote. A tiered, risk-based approach is the most effective way to evaluate, identify, and prioritize potential targets. There are a number of methods that can be employed to conduct a risk assessment and identify risk control activities. Section 8.9 provides guidance for developing and implementing a useful risk assessment approach.

Develop Baseline Security Plan. Using the output of the risk assessment, a plan is developed to address the most significant risks and assess the security of the pipeline system. This plan should include the mitigation risk control actions, as well as security assessment activities, e.g., inspections and traffic and personnel control. Section 8.10 provides a description of the various risk control options available, guidance to assist operators in selecting a security assessment method, establishing a schedule for periodic security inspections, and employment of security measures.

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that might lead to pipeline system failures are controlled. As noted previously, a risk assessment may identify other risks that should be addressed. For example, if pipeline exposure was identified as a significant security risk in a particular area, the operator may elect to conduct additional patrolling, increase public communication, and/or actively engage local police agencies to reduce the likelihood of the security threat to their pipeline. A menu of risk control activities and mitigation options to address common security risks is provided in Section 8.11.

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

Reassess Risk. Risk assessments should be performed periodically to factor in recent operating data, consider changes to the pipeline system design, e.g., new IT systems and new pipeline segments or facilities, and to analyze the impact of any external changes that may have occurred since the last risk assessment, 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 risk assessments to assure the analytical process reflects the latest understanding of the security issues.

Revise Plan. The baseline security plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation actions to address these risks should be performed, as appropriate. Furthermore, the updated risk assessment results should also be used to support scheduling of future security assessments. Section 8.12 discusses updating the security plan.

Audit Plan. The operator should collect information and periodically evaluate the success of its security assessment techniques and other mitigation risk control activities. The operator should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions. Section 8.13 provides

guidance for developing performance measures to evaluate plan effectiveness, and guidance for conducting audits of security management plans.

Managing Change. Pipeline systems and the environment in which they operate are never static. A systematic process should be used to ensure that changes to the pipeline system are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the pipeline operates are evaluated. Furthermore and after these changes have been made, they should be incorporated, as appropriate, into future risk assessments to be sure the risk assessment process addresses the system as it is currently configured. Section 8.14 discusses the important aspects of managing changes as they relate to security management.

As this final element indicates, managing pipeline security is not a one-time process. As implied by the loop in the lower portion of Figure 8.1, a security management program involves a continuous cycle of monitoring pipeline conditions, identifying and assessing risks, and taking action to minimize the most significant risks. Risk assessments must be periodically updated and revised to reflect current pipeline conditions so operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

8.8 Data Gathering, Review, and Integration

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

The types of data required depend on the types of risks and failure modes that are anticipated. The operator should consider not only the risks and failure modes currently suspected in the system, but also consider whether the potential exists for other risks and failure modes not previously experienced in the system, e.g., bomb blast damage. This section includes lists of many types of data elements. These lists have been organized using risks and failure mode as organizational tools that can be helpful in defining and utilizing the information. As different types of data are listed, common types of related risks and failure modes are indicated. The purpose of indicating risks and failure modes is to help the user understand the need and importance for the related type of data. All possible risks and failure modes are not necessarily listed, so the operator is responsible for evaluating its system to identify those that may be of concern.

Section 8.8 covers the gathering, review, and integration of data for pipeline security management. The discussion is separated into six subsections that address sources of data, identification and location of data, establishment of a common reference system, data collection and review, and data integration.

8.8.1 Data Sources

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

Facility and Right of Way Records. Facility and right of way records are used to identify the location of the facilities and the pipelines. This information is essential for determining areas and other facilities that either may impact the pipeline system or may be affected by the system and for developing the plans in protecting the pipeline system from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various areas along the pipeline system, e.g., HCA's, populations centers, industrial and government facilities.

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

Operation Records. Operating data is used to identify the products transported and the operations as they may pertain to security issues or facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, e.g., type of product, facility type and location, and volumes transported.

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

8.8.2 Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual pipeline system, the risk assessment methodology selected, and the decisions that are to be made. The data collection approach will follow the risk assessment path determined by the initial expert team assembled to identify the data needed for the first pass at risk assessment. The size of the pipeline system to be evaluated and the resources available may prompt the risk assessment team to begin their work with an overview or screening

assessment of the most critical issues that impact the pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this risk assessment. As the risk assessment process evolves, the scope of the data collection will be expanded to support a more detailed assessment, and improved results. Thus, as the operator reviews this section, a sampling of potential data types are presented to help readers in formulating their plans when embarking on the identification of pipeline data sources.

8.8.3 Locating Required Data

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

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

8.8.4 Data Collection and Review

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

Resolution of the input data should also be taken into account. Data resolution addresses the specific length over which data impacts the pipeline system and is recorded. Every effort should be made to utilize data as it actually exists along the pipeline system. Widespread data assumptions should be minimized, as they will not increase the overall accuracy of the assessment. The resolution will be handled during the risk assessment (see Section 8.9).

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

8.8.5 Data Integration

The quality of an ongoing risk assessment, as well as data maintenance programs relies strongly on the use of available information and on monitoring conditions over a period of time.

A substantial amount of inspection and monitoring data is collected over the life of a pipeline system. Examples of such data are changes in the system; security related issues; security inspections; external changes; different risks; etc. These data may reside within various departments and agencies and considerable effort can be involved to collect, collate, and arrange these data in a format that allows ready comparison.

The number of data points may become large, especially with the application of a risk-based assessment system and the pipeline identification, inspection and monitoring data. Security data can be stored in an electronic database. This greatly simplifies the comparison of data over time and provides for follow up pipeline security assessments.

The strength of a threat assessment is in its ability to compare the existing data for the coincident occurrence of suspected conditions or security related events. The user will be collecting data that indicates threat increasing conditions, as well as activities that will confirm or deny the impact of suspect threat conditions. Integration of data is an integral part of this approach. Shown below is an example of how integration of data is used to answer the question, "What is the likelihood of terrorist damage at a location on the pipeline system?"

Integration Example: Potential for Terrorist Damage	
Risk Increasing Indicators	Confirmation Activities (confirm or deny)
Pipeline Patrol	Frequency
Exposed Sections	Identify locations
Outside Party Knowledge	Assistance in warding off risks
Existing Security Measures	Identify and quantify
Accessibility	Easy or difficult
Visibility	Exposed or isolated
Police agencies	Availability
Question: What is the likelihood of terrorist damage at a specific location along the pipeline?	

Additional advantages of using a data management system for data integration include:

- Vast amounts of information can be stored;
- Keeping track of changes and updating reference points is easier.

- Data from different sources can be cross-referenced, e.g., a pipeline location in relation to a public thoroughfare.
- Information can be combined more readily between inspections or other evaluations, e.g., security plan and drill.
- Information and data can be sorted, filtered, or searched, e.g., list all pipelines in a particular location.
- Discovering and identifying data needed for a threat assessment process is made easier;
- The capability to import documents, photographs, videos, drawings, etc., allows user-friendly visualization of locations displays of aerial pictures of terrain with superimposed maps and drawn in pipeline with depicted selected areas.
- Integration of security assessment modules allows sorting and prioritizing areas based on the security assessment;
- Areas can be prioritized based on combined information, e.g., location, size, exposure.
- Security data can be compatible with other data management systems.

Building the databases in accordance with a company-wide or industry-wide data standard offers numerous advantages in allowing operators to compare their own performance with comparable companies or across the pipeline industry.

8.9 Risk Assessment

8.9.1 Developing a Risk Assessment Approach

When establishing a risk assessment program, a pipeline operator should consider many features that are unique to its systems and operations to determine which approach is most appropriate. The ultimate goal of risk assessment is to identify and prioritize significant security risks in the system so the pipeline operator can determine how, where, and when to allocate risk mitigation resources to improve pipeline system security and integrity. 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 risk assessment.

A risk management program is a continuous process that requires complete integration into a company's daily operation. The benefits of effective data integration will greatly enhance an operator's ability to plan effective security activities as well as identify circumstances that could result in security risks. In selecting the types of data that the operator will use for the risk assessment, the operator should consider the following:

The completeness of the data. For a set of data to be useful for an assessment, the data set should be as complete and consistent as possible across the portion of the pipeline system within the scope of the assessment. Using incomplete data will introduce uncertainty into the assessment, possibly resulting in poor and misleading results.

However, it is likely that some preliminary risk assessments may be performed with little or incomplete information to quickly screen a large collection of assets. This initial risk assessment, or risk screening, step may be used, for example, to develop a baseline security plan and/or to prioritize pipeline systems or portions of systems for more complete risk assessments. The scope, purpose and objectives of such an assessment should be clearly communicated so that decision makers do not interpret the results of a screening risk assessment to have a higher degree of accuracy than is possible given the information considered in the assessment.

The quality of the data. Data that has not been consistently and regularly prepared, updated and maintained may also introduce error into the assessment that may be detrimental to achieving the objective. Operators should strive to use data that best reflects the known, actual location-specific security risks to the pipeline system. Where possible, operators should avoid the use of global data assumptions. This will support a risk assessment that discriminates potential problematic areas in the system and will allow risk results to be based on the changing “actual” conditions along the pipeline length.

The importance of specific pipeline data. Not all information about a pipeline system is considered of equal value in a risk assessment. The pipeline operator must decide what level of importance will be placed on specific pipeline data. Risk assessment methods should consider the historical and the potential security risks of the specific system, tempered with broader industry and other proven practices and expert guidance.

Risk assessment is a very important analytical process in a security management program. Although there are a number of different methods for performing risk assessments, all approaches should answer the following basic questions:

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

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

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

8.9.2 Definition of Pipeline Risk

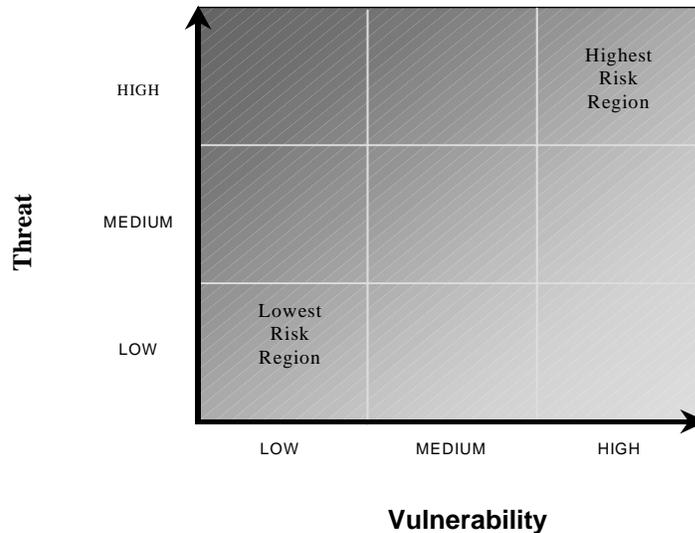
The overall risk to a pipeline system is a function of the likelihood of a security related event or condition to lead to an interruption of services, and the consequence in the event of an interruption of services. Both components of threat and vulnerability which lead to risk must be considered when conducting a risk assessment and in making prudent risk-based decisions. Figure 8.9.1 provides a simple depiction of risk.

8.9.3 Estimating Risk Using Risk Assessment Methods

Many pipeline risk and pipeline security plans use risk assessment methods that collect and logically process data to arrive at a risk estimation result. Risk assessment methods are tools that define a relationship between the threats and vulnerabilities that can reduce the level of service or system integrity and the consequences in such through a variety of data and assumptions about how the system is designed, and operated, as well as the external factors that can affect risk. Risk assessment methods "predict" the value of the output variable, e.g., level of risk, based on the input values of measured or evaluated variables. The quality of the prediction is dependent on the quality of the inputs and the soundness of the logical relationships inherent in the risk assessment method used to evaluate the input and output conditions.

It is important to distinguish between a risk management process and a risk assessment method. Risk assessment is the estimation of risk for the purposes of decision making. Risk management is the overall process that includes the risk assessment, development and implementation of a security plan, and reintegration of data into subsequent risk assessments. Risk assessment methods can be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks along a pipeline system. However, risk assessment methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. Risk assessment methods should be used as part of a process that involves knowledgeable, experienced personnel that critically review the input, assumptions, and results. This review should integrate the risk assessment 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.

Figure 8.9.1
Schematic Illustration of Risk



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

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

Independent of the risk assessment method used, all techniques incorporate the same basic components:

1. Identify potential security related events or conditions that threaten the system’s service or integrity.
2. Determine risk represented by these events or conditions by determining the likelihood of an interruption in services and the consequences of an interruption in services.
3. Rank risk assessment results.
4. Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses)
5. Integrate security plan and evaluations, e.g., drills and audits
6. Re-assess risk

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

8.9.4 Characteristics of a Sound Risk Assessment Approach

A risk assessment should be:

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

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

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

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

Use appropriate data. Some risk assessment decisions are judgment calls. However, relevant data and particularly data about the system under review should affect the confidence level placed in the decisions.

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

8.9.5 First Step in the Risk Assessment Process

A common step in all risk assessment approaches is to collect a representative group of company experts plus outside experts if needed to identify potential security related events or conditions that could lead to a pipeline interruption of service or pipeline failure, the consequences of these events, and risk reduction activities for the operator's system. These experts draw on the years of experience, practical knowledge, and observations from experienced field operations and maintenance personnel in understanding where the security risks may reside and what can be done about them. Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance and right-of-way departments. This group of experts will focus on the potential problems and risk control activities that would be effective in a pipeline security plan and not become

encumbered by the presence or absence of data on hand. During a later step in the risk assessment method development process, the availability of data, and the incremental value of collecting specific data will be handled. The primary goal of this group is to capture and build into the risk assessment method, the experience of this diverse group of individual experts so that the risk assessment 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 panels that have proven useful in assuring a systematic and thorough review. These include:

- Free-form brainstorming of issues and potential risks;
- Conducting a segment-by-segment review along the line using pipeline alignment sheets or maps and operations data;
- Using checklists or structured question sets designed to elicit 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.

8.9.6 Risk Assessment

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

- Does the scope of the risk assessment method encompass and identify significant security related events and risks along the pipeline system? If not, how can the risks that are not included in the risk assessment method be assessed and integrated in the future?
- Will all data be assessed as it really exists along the pipeline system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, i.e. station by station, mile by mile, dependent on the evaluation needs?
- What is the logical structure of variables that are evaluated to provide the qualitative and quantitative results of the risk assessment? Does this provide for straightforward data assimilation and assessment?
- Does the risk assessment 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 risk assessment method require data that are available to the operator? Do operator data systems and industry data updating procedures provide sufficient support to apply the risk assessment method effectively? What is the process for updating the risk assessment data to reflect changes in the pipeline system, the pipeline infrastructure, and other new security data? How are the input data validated to ensure that the most accurate, up-to-date

depiction of the pipeline system is reflected in the risk assessment?

- Does the risk assessment output provide adequate support for the justification of risk-based decisions? Are the risk assessment results and output documented adequately to support justification of the decisions made using this output?
- Does the risk assessment method allow analysis of the effects of uncertainties in the data, structure, and parameter values on the method output and decisions being supported? What sensitivity or uncertainty analyses is supported by the risk assessment method?

8.9.7 Core Risk Assessment Methodology Components

This section describes the common characteristics of the various risk assessment methods that can be used to assess pipeline system risk. There are many techniques and methods available but they all have common elements.

A risk assessment technique is typically based on a logically structured process that collects and analyzes data for the common causes of pipeline system interruptions of service and integrity due to security related events as well as the consequences to the pipeline system.

The risk assessment methods typically include a number of different operation and security related variables that can be important in affecting the likelihood of pipeline security related events, as well as variables that reflect conditions in the surrounding area, e.g., population density, sensitive environmental resources, and government facilities. Variable scores or values are assigned based on the presence or absence of these variables for each pipeline segment. These variables are assessed according to their importance and combined to determine the degree of risk represented by that segment. Risk estimation is the process of combining risk potential and severity estimates into a risk value. The risk potential and consequence estimated for each of the various identified security related events, or sequences of events, are combined into a risk value for that event sequence. The risk values for all identified event sequences can be combined into an overall risk value for the pipeline system or segment. The risk values may be qualitative, quantitative, or a combination of both, depending upon the processes used for frequency and consequence assessment, and the goals of the operator's risk management program.

The sensitivity of risk assessment methods is a function of the number of variables and the ability to estimate the changing risk along the length of the pipeline. Some techniques require the user to evaluate long sections of pipeline using a uniform set of characteristics, while others integrate the localized effect of changing data. In many risk assessment methods, the likelihood is estimated using a combination of variables in categories such as the following:

- Third party involvement
- System operations
- Visibility

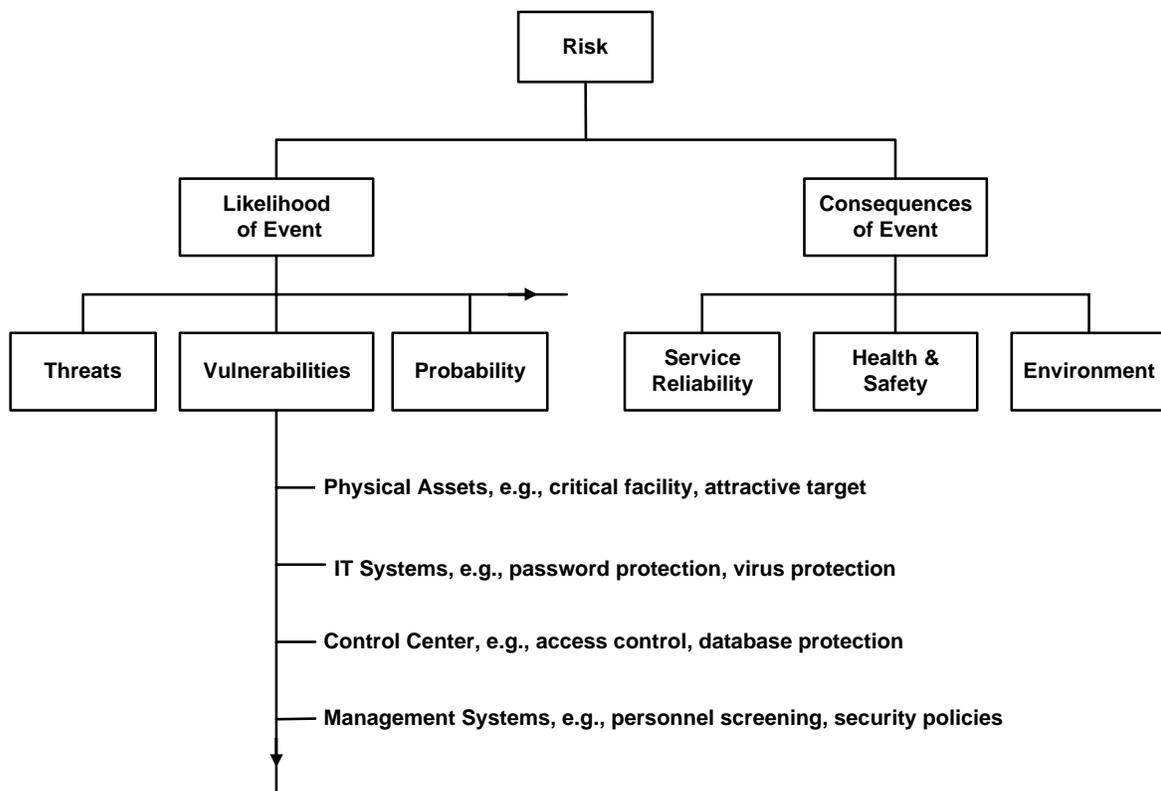
- Security features
- Event probability

The consequence is estimated as a combination of variables in categories such as:

- Population impacts
- Business impacts
- System reliability
- Environmental danger

Figure 8.9.2 provides a simplified example of the logical structure of risk assessment methods.

Figure 8.9.2
Simplified Risk Assessment Structure



The values used in a risk assessment method are determined based on the pipeline operator's knowledge and experience with the systems with the risk increasing or decreasing being a variable output. For example, an operator may consider a remote, unattended facility a higher risk than an attended facility or a large diameter pipeline a higher risk than a small diameter pipeline. For relative risk estimation, the numerical value assigned to a condition is not critical, only that the higher risk condition contributes more to the final risk level than a lower risk condition. The risk assessment method is looking for the coincident occurrence of multiple risk increasing features. Risk assessment methods may consider very few or many variables in the analysis depending on the available data, the purpose of the risk assessment and resource availability for the risk assessment. The risk levels can be qualitative if only a limited number of variables are used. The risk levels can become more quantitative as the number of variables used in the assessment increase. The quantitative accuracy can be further enhanced by overriding the effect of assumptions, e.g., existing security measures and location of facilities, when performance data are collected that suggests a specific security threat is not active, i.e., low probability.

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

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

- Scope of the risk assessment; that is which assets are included/excluded from the assessment.
- Equipment boundaries such as pump stations or block valves.
- Geographical boundaries such as state lines or rivers.

- Desired minimum/maximum length of any one segment, i.e., foot-by-foot, mile-by-mile.
- How system databases are set up and organized; this is important since data will be transferred from one or several databases into the risk assessment method.
- Operation changes, e.g., region, product, and volumes.
- Population density changes.
- The presence of environmentally sensitive or population sensitive areas, e.g., schools, waterways, third party facilities, and government installations.

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

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

Some additional criteria to evaluate the results of a risk assessment are:

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

8.9.8 Identify and Gather Data Required for Risk Assessment

For each potential pipeline security threat or risk factor, the characteristics or variables that potentially could impact risk (both beneficially and adversely) are identified. During the risk assessment process, specific risk increasing characteristics of the pipeline system are generally either external variables, e.g., outside influences acting on the pipeline system, or operation variables, e.g., characteristics associated with the physical properties. In either case, these variables are features of the in-service pipeline 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 risk assessment.

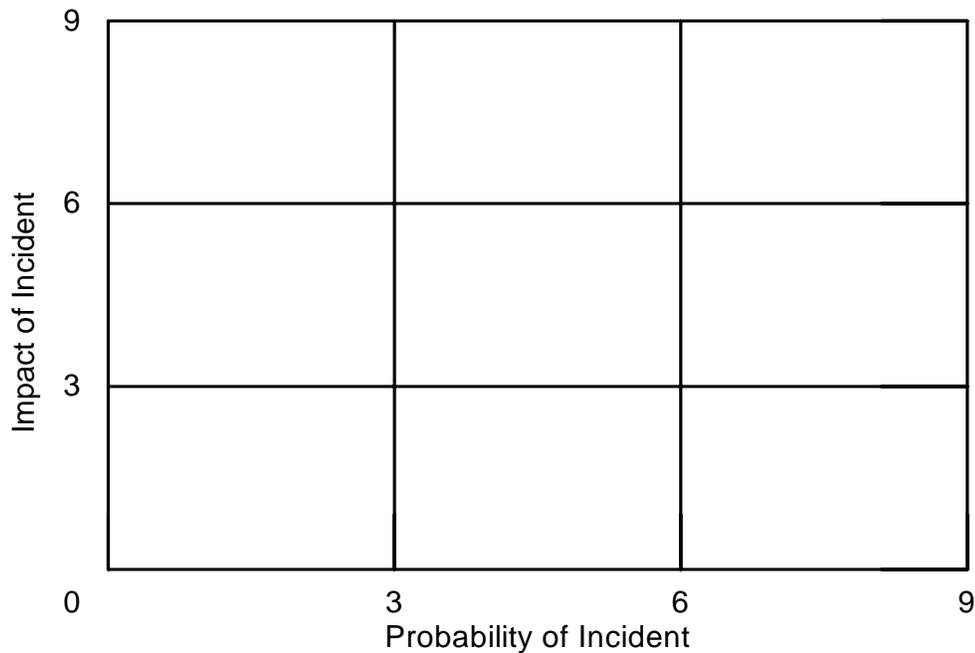
Once the likelihood of risk increasing features are evaluated, the next step is to incorporate security related countermeasures, e.g., fencing, lighting, patrols, and traffic flow, into the likelihood of event (LOE) estimation. Direct security variables have the ability to either increase the LOE, e.g., lack of fencing or lighting, or decrease the LOE in the event that no adverse security measures are identified. The impacts on risk should be based on sound security assessment.

Total risk is determined by combining the factors that affect the LOE with the impact associated with the consequence of a security event. The overall process of *proactively* evaluating and identifying the potential of risk increasing conditions *prior* to the onset of a security event is the science of risk assessment.

8.9.9 Risk Assessment Example

Several companies use the matrix approach in performing a risk assessment of facilities. One such matrix employed is where the Probability of Incident is plotted against the Impact of Incident with both factors being given numerical values. In such an example, the higher the Probability and/or the Impact, the higher the risk assessment value which leads to increased security measures being employed at the facility. Figure 8.93 shows such a matrix:

**Figure 8.93
Risk Assessment Matrix**



CONFIDENTIAL

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

<u>Item</u>	<u>Detail</u>	<u>Value</u>
Location	Rural	1
	Small Town/Village	2
	Urban Location	3
Environmental Exposure	Heavy Oils/Asphalt	0
	Distillate	1
	Gasoline	2
	HVL	3
	Highly Toxic	4
Size	Less than 10 barrels	1
	10 to 100 barrels	2
	More than 100 barrels	3

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

<u>Item</u>	<u>Detail</u>	<u>Value</u>
Personnel Exposure	None	0
	Minimal Exposure	2
	Large Exposure	4
Environmental Exposure	None	0
	Land and/or Air	1
	Minor Waterway	2
	Major Waterway	3
Business Interruption	None	0
	Less than \$10M	1
	\$10M to \$100M	2
	More than \$100M	3

Likewise, each item would be evaluated and the values would be totaled with the total value plotted on the matrix as the Impact of Incident. Where the two values cross on the matrix is the overall numerical risk assessment value for a particular facility. In conducting such an assessment for a number of facilities, they could be ranked in comparison to each other in using such a system.

A second example of conducting a risk assessment is in using a standardized form together with a risk assessment matrix with both documents being completed for each facility assessed.

8.9.10 Validation and Prioritization of Risks

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

Once the risk assessment method and process has been validated, the operator has the necessary information to prioritize risks. To do this, the operator sorts the pipeline segments in order of overall risk level of each segment. The higher risk level pipeline segments should be given higher priority when deciding where to implement security measures. To determine what risk mitigation actions to take, the operator considers which pipeline systems (or segments of systems) have the highest risk and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

For example, when considering a pipeline segment that has the highest overall risk, the operator found that two risk factors had a much greater influence on the risk determination than any of the other risk factors. For this segment, the factors that drove the risk to a higher level than the rest of the segments considered were critical facility and visibility. The risk assessment identified a higher likelihood of a security related event due to target visibility. Also, the risk assessment identified a higher potential consequence of a security related event due to the facility being critical to maintain supply. These risk drivers were combined in the risk assessment method to result in the highest overall risk level for the assets considered. This information about risk drivers can then be used to plan what risk mitigation activities would be effective in reducing risk for this specific pipeline segment. This process is discussed in the following section.

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

8.9.11 Risk Control and Mitigation

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

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

- Identification of risk control options that lower the likelihood of a pipeline system security related event, reduce the consequences, or both, i.e., mitigation activities;
- A systematic evaluation and comparison of those options to quantify the risk reduction impact of the proposed project; 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, inspection practices, personnel training, pipeline control and monitoring methods, emergency response, and interface with the public and other external organizations. Section 8.11 of this guideline provides a discussion of risk control options that are frequently used to reduce pipeline integrity risks. In order to find the optimum approach to risk control, it is important that a variety of options, and perhaps combinations of activities, be considered, rather than just taking the first idea that is proposed or doing what has always been standard practice. This allows management to consider innovative solutions and perhaps new technologies that may be more effective in addressing risk. Many operators have found that a structured process for identifying risk control options and encouraging innovative solutions has produced unique insights and contributed to more effective risk management.

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

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

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

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

The integrity inspection and risk mitigation decisions that are produced by this process are used to prepare the baseline security plan, or modify the existing plan, as described in Section 8.10.

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

8.9.12 Periodic Risk Assessment

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

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

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

8.10 Initial Baseline Plan Development and Implementation

8.10.1 Initial Baseline Plan

The baseline plan is developed as a result of the initial data gathering and risk assessment (see Sections 8.8 and 8.9) and consists of an initial security inspection plan and the employment of security mitigation activities including a schedule for these activities to be implemented. To develop the baseline plan, the most appropriate inspection requirements must be identified for each asset, and the work must be prioritized and scheduled dependent on the ranking of the asset. Inspection of each asset or pipeline segment could be accomplished by experts visiting the facilities, review of an existing data base, meetings with operations and maintenance personnel, or a combination of these techniques. The initial risk assessment will provide guidance to determine what factors to consider (see Section 8.9). This section provides information about inspection techniques and security mitigations. The baseline plan, once developed, tells the operator what to inspect, how to inspect, and when to inspect as well as the security measures to consider in mitigating risks.

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

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

1. Pipeline security risks that can adversely affect pipeline security.
2. Various security inspection techniques typically used for pipeline systems.
3. Methodology for evaluation of inspection data.
4. Pipeline security measures, and other mitigation activities that can improve pipeline security.

8.10.2 Pipeline Security Risks

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

8.10.3 Pipeline System Inspections

This is an overview of the elements that should be considered in a security related pipeline system inspection that can be applied to pipeline segments and facilities as defined in Section 8.9.7. The listed items should not be considered as all inclusive as there could be other items which are unique to the pipeline segment or facility. In general, a security related inspection should include as applicable the following elements:

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

8.10.4 Determination of Inspection Interval/Frequency

8.10.4.1 *Initial Inspections*

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

8.10.4.2 *Setting Inspection Intervals*

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

8.10.5 Inspection Methods

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

8.10.6 Methodology for Evaluation of Inspection Data

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

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

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

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

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

An operator should take into consideration the inspector's recommendations in determining an effective security program. Once all the security related issues are addressed, the operator should document all the security issues and integrate the information into the risk assessment model.

8.10.7 Response Strategies

Inspections conducted per an operator's security management plan could result in security related issues that must be evaluated. A number of these issues will require changes and modifications to the status quo and some could require company expenditures to implement. The operator should develop a strategy to evaluate each of the identified security issues and then develop a program to implement those actions that are needed for improved security.

8.11 Mitigation Options

An operator's pipeline security plan will include applicable mitigation activities to prevent, detect, and minimize the consequences of security related events. Mitigation activities do not necessarily require justification through additional inspection data. Mitigation actions can also be identified during normal pipeline operation, during the initial risk assessment, during implementation of the baseline plan, or during subsequent inspections.

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

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

8.11.1 Management Issues

Company security management should be assigned to one senior level position within the company. In most companies, this responsibility can be included with the responsibilities of another position such as risk management, operations, or health, environmental, and safety. Security management should also be assigned to one person at each company facility and/or pipeline segment. The persons assuming the security roles can perform a number of important management functions such as promulgating policy, establishing relationships with law enforcement agencies and surrounding communities to address security concerns, developing and managing incident reporting systems, boosting employees' security awareness, referring securing breaches for investigation, coordinating emergency response, and periodically directing the reassessment of the security plan.

8.11.2 Security Policy

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

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

8.11.3 Collaboration With Others

The company as well as each of its facilities should establish partnerships with local, state, and federal law enforcement and other public safety agencies. Through such a network, information can be gained regarding risks, dangerous trends, and successful and unsuccessful security measures. It may also be possible to obtain threat and other information from regulatory agencies, LEPC's, community advisory panels, industry associations, mutual aid groups, state chemical associations, and ISAC's. Internal collaboration can also be important. By clarifying relationships and procedures with

other management functions, e.g., employee safety and health, legal, and human resources, information channels can open within the company and provide a more coordinated response to security related incidents.

8.11.4 Incident Reporting and Analysis

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

8.11.5 Employee and Contractor Training and Security Awareness

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

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

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

8.11.6 Investigations

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

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

8.11.7 Emergency Response and Crisis Management

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

8.11.8 Periodic Reassessment

The conditions surrounding a security effort change constantly. Even such mundane changes as vegetation growth or new buildings around a facility's exterior may impact the security plan. Therefore, company and facility security measures must be reviewed periodically as well as whenever conditions that could impact security change significantly. At appropriate intervals, it is necessary to:

- Update risk assessments and site surveys
- Review the level of employees and contractors compliance with security procedures
- Consider the need to modify or update the security plan

8.11.9 Physical Security

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

8.11.9.1 *Access Control*

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

- Post “No Trespassing” and “Authorized Access Only” signs along with signs stating vehicles and visitors are subject to search
- To the extent feasible, employ natural surveillance by arranging space so unescorted visitors and non-company vehicles can be noticed easily
- Install appropriate and secure locks on all asset features which should be secured and control access to the keys or combinations when such locks are used
- Require visitor sign-in logs, verify visitors are expected, and provide escorts
- Institute and maintain vehicle traffic control entering the facility and while in the facility – establish minimum spacing between vehicles and buildings and other assets pending verification of the necessity and intent of the vehicles presence
- Require visitor parking off-site or at some minimum distance from the facility
- Install appropriate penetration resistant openings to the facility, e.g., doors, windows, hinges, gates
- Institute a system of employee and contractor photo ID badges – train employees to question persons who not wearing badges
- Install an electronic access control system that requires the use of key cards or number pads at main entrances and on appropriate doors and provides an audit trail of ingress and egress – consider electronic access control to motor control centers, switchgear rooms, server rooms, telecommunication rooms, and control centers
- Install a closed-circuit television system to monitor key areas of the facility – where appropriate, install motion sensors

- Institute a system of parcel inspection or consider routing of parcels and mail through off-site facilities
- Require the use of property passes to bring or remove property from the facility

8.11.9.2 *Perimeter Protection*

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

- Fences and exterior walls that make it difficult for intruders to enter the facility
- Bollards and trenches that prevent vehicles from driving into the facility at points other than intended entrances
- Vehicle gates with retractable barriers
- Personnel gates and turnstiles
- Setbacks and clear zones which make it difficult for visitors to approach the facility unnoticed
- Lighting that makes it possible for employees and others to observe and identify visitors before they are in the facility
- Intruder detection systems along the perimeter such as infrared detection and light or sonic beam technology
- Video cameras and audio systems at the entrances to identify visitors before they are in the facility

8.11.9.3 *Security Officers*

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

8.11.10 *Cyber Security*

As organizations increasingly rely on networked computer systems, they lose the control of information processing that was present in the traditional data center. As the control of computing information moves to the desk top and remote sites via networking, it is essential that companies understand the risks to this and create security plans that will

meet this challenge. Computer systems have unique security issues that must be understood for effective implementation of security measures. These issues include:

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

- Disaster Recovery
- Policy

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

8.11.10.1 *Hardware Accessibility*

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

8.11.10.2 *Software*

Most security intrusions to a computer system's software are either by introducing a virus to the system or by a security breach of the computer system allowing an outsider into the system to modify or interrupt the commands of the system or to gain information. Software viruses have left a number of companies sadder but the wiser. A virus can change data within a file, erase a disc, or direct a computer to perform system slowing calculations. Viruses may be spread by downloading programs off a bulletin board, sharing floppy diskettes, or communicating with an infected computer through a network. Anti-virus products are a necessity for the detection, eradication, and prevention of viruses. The company's computer security policy should define permissible software sources, bulletin board use, and the types of applications that can be run on company computers. This policy should also provide standards for testing unknown applications and limit diskette sharing. Network security including intrusion prevention is discussed in section 8.11.10.5.

8.11.10.3 *Data Communications*

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

8.11.10.4 *SCADA Systems*

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

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

8.11.10.5 *Networking*

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

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

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

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

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

- A log of all attempts to gain access to the system
- A chronological log of all network activity
- Flags to identify unusual activity and variations from established procedures

8.11.10.6 *Disaster Recovery*

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

situations where locally stored backup copies would be lost with originals, special consideration should be given to storing periodic archival copies at some location unlikely to be affected by common emergencies and security related events. Many companies maintain three copies of all computer information referred to as grandfather, father, and son. The son is the working copy, the father is kept close at hand, i.e., it is the backup needed most frequently, and the grandfather is kept off-site in a location that the company can easily access. Such backups are also done on a routine and regular basis, e.g., once per calendar day.

8.11.10.7 *Policy*

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

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

8.12 Updating the Security Plan

Inspections and other security assessments conducted under an operator's pipeline security plan will result in data that must be analyzed and integrated with previously collected data. This is in addition to the other types of security related data that is constantly being gathered, updated, reviewed and integrated into the operator's database (see Section 8.8). The result of this ongoing data integration, and periodic risk assessment will result in revision of the plan in the form of new or modified mitigation plans and subsequent security assessments.

Analysis of inspection and other security assessment data will most likely result in a series of additional mitigation activities. Some of these mitigation activities may require immediate action while others may be scheduled in a long-term plan. The criticality of

mitigation actions and how they are scheduled will depend on the results of integrating this information into an operator's risk assessment.

8.13 Plan Evaluation

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

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

8.13.1 Performance Measures

The operator should collect performance information and periodically evaluate the effectiveness of its security assessment methods, and its mitigation risk control activities, including response. The operator should also evaluate the effectiveness of its management systems and processes in supporting security management decisions. A combination of performance measures, and internal and external system audits is necessary to evaluate the overall effectiveness of a pipeline security plan.

Each operator should have performance measures. These performance measures should include a distribution of leading, lagging, and deterioration measures (see 8.13.2 for a discussion of the types of performance measures). These performance measures should be part of the operator's security management program, and should be based on an understanding of the risks to the security for each pipeline system operated.

The following performance measures should be considered:

1. A performance measurement goal to document the percentage of security management activities completed during the calendar year.
2. A performance measurement goal to track and evaluate the effectiveness of the operator's collaboration efforts with outside agencies.
3. A performance measure based upon audits and drills of the operator's security plan.
4. A performance measure based on operational events, e.g., security breaches, cyber attacks, alerts, and countermeasures employed, that have the potential to adversely affect pipeline security.
5. A performance measure to demonstrate that the operator's security management program reduces risk over time with a focus on high risk items.

6. A performance measure to demonstrate that the operator's security management program for pipeline segments and facilities reduces risk over time with a focus on high risk items.

8.13.2 Performance Measurement Methodology

All of the risk assessment and mitigation methods discussed earlier in this guideline are put forth with the intent of reducing the likelihood and consequences of a security event. Ultimately the performance measurement of an operator's security management program is the degree to which security risks are eliminated. However, a typical security management program will contain many elements, and the program will operate over long time horizons. Thus a security management program cannot be evaluated based on any one measure. This section describes an approach to monitoring performance of the components of a security management program with the expectation that component progress will correlate with overall program success. Performance measures actually form a continuum from leading indicators (before security events) to lagging (after security events), and include process measures and measures of actual security events. The distinction between many of these measures will not always be clear.

Selected process measures. Metrics employed to monitor the surveillance and other mitigation activities undertaken by the operator. These measures indicate how well an operator is implementing the various elements of the security management program. These measures answer the questions: "Once the program has been defined, how well are the details being executed?" Drills are an effective way to demonstrate awareness and understanding of security management programs. Activity measures must be thoughtfully selected since not all activity measures will effectively measure performance.

Security event measures. Operational and maintenance trends employed to indicate when the security of the system is reduced despite mitigation measures. Some performance measures of this type may indicate that the system condition is deteriorating despite well executed mitigation activities. Other performance measures may indicate that predicted security events are within expected parameters or they are not within expected parameters. Security event measures should be evaluated over time to understand trends.

8.13.3 Measuring Performance Using Internal Comparisons

Every operator should evaluate its current performance against past performance and set specific goals. Internal comparisons over time are suitable for analyzing trends. For example, security audits and drills during the last 12 months can be plotted on a rolling basis once per quarter. An increasing trend would indicate that the average age of security data is improving.

Internal comparisons of one portion of a pipeline system against another portion of the same pipeline system (for example, portions of the system within designated high

consequence areas versus other portions outside designated high consequence areas) may be used to evaluate the effectiveness of specific mitigation actions.

Internal comparisons from one geographic region to another geographic region within the same operating company, or from one business unit to another business unit may be helpful ways to identify areas with deficiencies.

8.13.4 Measuring Performance Using External Comparisons

External comparisons may be more difficult to obtain. This is particularly true for the metrics related to mitigation actions. Benchmarking among operators may prove practical when those operators are not in direct competition. Care needs to be taken to ensure that benchmarking is conducted such that information is comparable among the benchmarking operators or systems.

Operators should also conduct periodic evaluations of their own performance in comparison with industry-wide data sources. In order to ensure that operators have access to external databases, operators need to participate in data initiatives, both operator benchmarking and industry wide databases. Individual operators should collect internal incident information using standard incident data fields even if they do not choose to contribute operator information to external databases. Only by using standard data fields can comparisons be made external to individual operators.

In order to conduct trend analysis of incidents, system characteristics also need to be captured using a standard format (facility location, pipeline miles, miles by diameter, and volumes moved). Operators should collect infrastructure data for trend analysis using standard data fields even if they do not choose to contribute system infrastructure information to external databases.

8.13.5 Audits

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

- Is there a written policy/program for Security Management?
- Are there written procedures for tasks relating to security management?
- Are activities being performed as outlined in the operator's program documentation?
- Is someone assigned responsibility for each subject area?
- Are appropriate references available to those who need them?
- Are the people who do the work trained in the subject area?

- Are qualified people used when required?
- Are activities being performed using an appropriate integrity management framework as outlined in this guideline?
- Are all required activities documented by the operator?
- Are action items followed-up?
- Is there a formal review of the rationale used for developing the risk criteria used by pipeline operator?
- Are there established criteria for responding to security events? Are criteria established for these activities stated above for terminals, pump stations, associated piping, and pipeline segments?

8.13.6 Drills

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

- a scripted event indicative of a security related event
- emergency management and reporting procedures
- availability of essential resources and response actions
- review of lessons learned, i.e., critique of drill
- modifications to plan

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

8.13.7 Performance Improvement

Program evaluation should be conducted on an ongoing basis. Information should be accumulated and documented over time. Since the details of operator security management programs will vary, so too will the appropriate set of performance measures. Section 8.13.1 identifies performance measures that can be used by operators. Some operators may elect to have additional performance measures.

Audits should be used as additional information sources for understanding the effectiveness of pipeline security programs. Recommendations for security management program improvement shall be developed based on the results of performance evaluation, including performance measures and audits. The performance measurement and audit results shall also be factored into future risk assessments.

The results of performance measurement and audits, including all follow-up recommendations, should be reported to those individuals within an operating company who are responsible for pipeline security. Performance should be reviewed at least annually and issues should be addressed.

8.14 Managing Change in a Security Program

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

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

Operators with an existing management of change (MOC) program should verify that the types of changes mentioned in this section are included in their MOC program. For other operators, a system should be established to recognize and manage changes relevant to their pipeline security program.

8.14.1 Recognizing Changes That Affect the Security Program

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

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

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

8.14.2 Updating the Pipeline Security Program

A change may impact any or all of the pipeline security program. Sections 8.8 through 8.13 of this document address elements of the program that may be impacted by a change. As part of managing a change, the operator should evaluate security program issues such as:

- Have the potential impacts or affected impact zones been altered? (Section 8.8)
- Should data be added, deleted, or modified? (Section 8.9)

- Does this change impact data that was input or assumptions that were made during the risk assessment? (Section 8.9)
- Does this change affect mitigation plans? (Sections 8.11)
- Does this change impact the security program for pipeline segments or facilities? (Section 8.11)
- Should this change lead to a revision of the security management plan? (Section 8.12)
- Does this change impact any performance indication or auditing criteria? (Section 8.13)

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

8.15 Guidelines and Recommendations- Liquid Pipeline Security Conditions and Response Measures

The Security Conditions (SECON's) describe a progressive level of protective measures that should be implemented in response to the possibility of a terrorist threat or to a terrorist threat directed at liquid pipeline facilities, assets, and personnel. The purpose of the SECON system is to establish standardized alert and response measures for a broad range of threats and to help disseminate appropriate and timely information for the coordination and implementation of the response measures by management and company personnel prior to and during a threat crisis. The associated response measures should be implemented for each SECON level at each designated facility and as applicable to the other parts of the system and system facilities. A designated facility is:

- a pipeline, pipeline segment, or pipeline facility mutually agreed as such between the federal government and the company, or
- a pipeline, pipeline segment, or pipeline facility designated as such by the company.

A designated facility will typically be maintained at a higher level of preparedness as warranted by the security risk at the facility. Each company should develop a means to advise and communicate to company personnel and others as warranted the security condition at a designated facility and otherwise as applicable. The measures associated with each SECON level are not prioritized but should be initiated concurrently where practical and as applicable. Local facility management should maintain a record of specific actions taken for each SECON level. Following is a detailed explanation for each SECON level and the response measures associated with each level:

SECON-5: Threat negligible - this condition exists when a general threat of possible terrorist activity or civil unrest exists but warrants only routine security measures associated with daily operations. SECON-5 is for normal operating conditions. All measures under SECON-5 must be maintained indefinitely.

Measure 1. All contractors and visitors must check or sign in and out of designated facilities at the designated location(s) within the facility.

- Measure 2.** Ensure existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting. Identify those additional security measures and resources that can enhance the security at the higher SECON levels, e.g., increased surveillance.
- Measure 3.** Establish emergency communications and contact information with local police agencies including the region FBI office. Emergency communications should have redundancy in both the hardware and the means for contacting police agencies.
- Measure 4.** Develop terrorist and security awareness and provide information and educate employees on security standards and procedures. Caution employees to not talk with outsiders concerning their facility or related issues.
- Measure 5.** Advise all personnel at each facility to report the presence of unknown personnel, unidentified vehicles, vehicles operated out of the ordinary, abandoned parcels or packages, and other suspicious activities.
- Measure 6.** Develop procedures for shutting down and evacuation of the facility. Facilities located near critical community assets should be especially vigilant of security measures.
- Measure 7.** Incorporate security awareness and information into public education programs and notifications to emergency response organizations, e.g., land owner contacts, mail-outs, and LEPC advisories.
- Measure 8.** Survey surrounding areas to determine those activities that might increase the security risks that could affect the facility, e.g., airports, government buildings, industrial facilities, and other pipelines.
- Measure 9.** Ensure contingency and business continuity plans are current and include a response to terrorist threats.
- Measure 10.** Develop and implement hardware, software, and communications security for computer based operational systems.

SECON-4: Threat low – this condition exists when there is an increased general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher SECON measures. It may be necessary to implement certain selected measures from higher SECON levels to address information received or to act as a deterrent. All measures under SECON-4 must be maintained as long as the increased general threat exists. In addition to the measures required by SECON-5, the following measures should be implemented:

- Measure 11.** Ensure that a company response can be mobilized and review facility security plans and procedures. Test security and emergency communications procedures and protocols.
- Measure 12.** Secure all buildings and storage areas not in regular use. Increase frequency of inspections and patrols within the facility including the interior of buildings and along the facility perimeter.
- Measure 13.** Inspect perimeter fencing and repair all fence breakdowns. In addition, review all outstanding maintenance and capital project work that could affect the security of facilities.
- Measure 14.** Reduce the number of access points for vehicles and personnel to minimum levels and periodically spot check the contents of vehicles at the access points. Be alert to vehicles parked for an unusual length of time in or near a facility.
- Measure 15.** Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher SECON levels.
- Measure 16.** Check designated unmanned sites and remote valve sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increase ROW surveillance in designated areas.
- Measure 17.** Require each visitor to check in at the designated facility office and verify 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 related issues including the facility’s personnel. Be familiar with vendors who service the facility and investigate changes in vendor personnel.
- Measure 18.** Inspect all mail and packages coming into a facility. Do not open suspicious packages. Review the USPS “Suspicious Mail Alert” and the “Bombs by Mail” publications with all personnel involved in receiving mail and packages.

SECON-3: Threat medium – this condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this SECON must be capable of being maintained for several weeks without causing undue hardship, affecting operational capability, or aggravating relations with the local community. In addition to the measures required by SECON-4, the following measures should be implemented:

- Measure 19.** Increase the frequency of warnings required by Measure 5 and inform personnel of additional threat information as available. Implement procedures to provide periodic updates on security measures being implemented.

- Measure 20.** Ensure that a company response can be mobilized appropriate for the increased security level. Review communications procedures and back-up plans with all concerned.
- Measure 21.** Review with all facility employees the operations plans, personnel safety, security details, and logistics requirements that pertain to implementing increased security levels.
- Measure 22.** Confirm availability of security resources that can assist with 24/7 coverage.
- Measure 23.** Move automobiles and other non-stationary items at least 30 yards from designated facilities, particularly buildings and sensitive areas. Identify areas where explosive devices could be hidden.
- Measure 24.** Close and lock gates and barriers except those needed for immediate entry and egress. Inspect perimeter fences on a regular basis. Ensure that other security systems are functioning and are available.
- Measure 25.** Inspect on a more frequent basis the interior and exterior of all buildings and around all storage tanks and other designated critical areas.
- Measure 26.** Dedicate personnel to assist with security duties at designated facilities with duties to monitor personnel entering the facility, checking vehicles entering the facility, and to patrol the area on a regular basis reporting to facility management as issues surface.
- Measure 27.** Limit visitors and confirm that the visitor has a need to be and is expected at the facility. All unknown visitors should be escorted while in the facility.
- Measure 28.** Advise local police agencies that the facility is at a SECON-3 alert level and advise the measures being employed – request the police agencies to increase the frequency of their routine patrol of the facility.
- Measure 29.** Resurvey the surrounding area to determine if activities near the facility could create emergencies and other incidents that could affect the facility, e.g., airports, government buildings, industrial facilities, railroads, other pipelines, etc.
- Measure 30.** Instruct employees working alone at remote locations or on the ROW to check-in on a periodic basis.
- Measure 31.** Check to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Measure 32. Direct that all personal, company, and contractor vehicles at designated facility sites are secured by locking the vehicles.

SECON-2: Threat high – this condition applies when an incident occurs or information is received indicating that some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this SECON 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 required by SECON-3, the following measures should be implemented:

Measure 33. Continue all SECON-3 and SECON-4 measures or introduce those that have not already been implemented.

Measure 34. Activate emergency response plans for the designated facilities.

Measure 35. Reduce facility access points to the absolute minimum necessary for continued operation.

Measure 36. Secure a 24/7 trained and knowledgeable security workforce to man the impacted facilities – ensure that all security personnel have been briefed concerning policies governing the use of force and pursuit.

Measure 37. Increase security patrol activity to the maximum level sustainable. Increase perimeter patrols and inspections of facility.

Measure 38. Advise local police agencies that the facility is at a SECON-2 alert level and advise the measures being employed – request the police agencies to increase the frequency of their patrol of the facility.

Measure 39. Consult with local authorities about control of public roads and accesses that might make the facility more vulnerable to terrorist attack if they were to remain open.

Measure 40. Erect barriers to control direction of traffic flow and protect the impacted facility from an attack by a parked or moving vehicle – company vehicles may be used for this purpose. Implement centralized parking and shuttle bus service where feasible.

Measure 41. Schedule more frequent visits to remote valve sites and other locations that are potentially impacted.

Measure 42. Increase the frequency of call-ins from remote locations. Employees should not work alone in remote areas.

Measure 43. Cancel or delay all non-vital facility work conducted by contractors, or continuously monitor their work with company personnel.

- Measure 44.** Check all 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 decrease lighting to detract from the area.
- Measure 45.** Identify the owner of all vehicles at designated facilities and have all vehicles removed which are not identified.
- Measure 46.** Inspect all vehicles entering designated facilities including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed.
- Measure 47.** Limit access to designated facilities to those personnel who have a legitimate and verifiable need to enter the facility. Implement positive identification of all personnel – no exceptions. Evacuate all non-essential personnel.
- Measure 48.** Implement frequent inspection of designated facilities including the exterior and roof of all buildings and parking areas. Increase patrolling at night and ensure all vulnerable critical points are fully illuminated and secure.

SECON-1: Threat critical – this condition applies in the immediate area where a terrorist attack has occurred which may affect the facility or when an attack is initiated on the facility and its personnel. Normally, this SECON is declared as a localized condition at the affected facility. In addition to the measures required by SECON-2, the following measures should be implemented:

- Measure 49.** Continue all SECON-2, -3, and -4 measures or introduce those that have not already been implemented.
- Measure 50.** Augment security forces to ensure absolute control of the facility and access to the facility and other potential target areas. Establish surveillance points and reporting criteria and procedures. Solicit assistance from the local police agencies in securing the facility and access. Cooperate with local police or other authorities if they take control of security measures.
- Measure 51.** Shut down impacted facilities and operations in accordance with contingency plans unless there is a compelling reason not to and evaluate prior to resuming operations.
- Measure 52.** Implement business contingency and continuity plans as appropriate.

9.0 Security Guidelines for Petroleum Products Distribution and Marketing

9.1 Purpose & Objective

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

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

9.2 Overview of Segment Operations

The petroleum distribution and marketing sector includes over 1,400 terminals, 7,500 bulk stations, more than 45,000 trucks and 170,000 gasoline stations. Each day the petroleum industry transports and purchasers consume over 350 million gallons of gasoline and more than 150 million gallons of diesel and home heating oil. The loss of any one terminal, bulk station, truck or gasoline station would not significantly affect U.S. energy supplies. Further, in the unlikely event of attack, these marketing and distribution facilities have been designed with extensive safety precautions that provide considerable mitigation to criminal or terrorist attack.

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

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

For example, some have stationed guards to further protect the facility. These decisions have been based on the risk to the community or to sensitive environmental areas from a potential attack.

Once a truck is loaded with product at a terminal, the driver delivers the product to a retail gasoline station (wholesale and aviation accounts also). The driver, in accordance with Department of Transportation (DOT) rules, must follow designated hazardous material routes where possible. There has been an increase in security training and awareness by transportation personnel, truck and rail. Transportation personnel have implemented additional security procedures throughout the transportation process. The American Petroleum Institute has also met with the DOT Direct Action Group on hazardous material transportation and participated in a meeting where DOT discussed the development of security training procedures for transportation of hazardous materials.

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

9.3 Relevant Operational Standards and Industry Practices

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

In addition to the regulatory framework governing transportation of hazardous materials, API maintains a number of design and operational standards and recommended practices that address aspects of safety and security in the distribution and marketing segment. While none of these were developed specifically for security reasons, aspects of them are directly applicable. In many cases, prudent safety procedures would also serve to address appropriate security precautions. These recommended practices provide a starting point for developing guidance on security at distribution and marketing facilities.

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

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

- Recommended Practice 1621 Bulk Liquid Stock Control at Retail Outlets (Primarily applied to underground storage of motor fuels and used oil at retail and commercial facilities).
- Recommended Practice 1004, Bottom Loading and Vapor Recovery for MC-306 Tank Motor Vehicles (Provides an industry practice for bottom loading and vapor recovery of proprietary and hired carrier DOT MC-306 tank vehicles at terminals operated by more than one supplier. Guides the manufacturer and operator of a tank vehicle as to the uniform features that should be provided to permit loading of a tank vehicle with a standard 4-inch adapter).
- Recommended Practice 1007, Loading and unloading of MC306/DOT 406 Cargo tank Motor Vehicles (This document provides details on how tank trucks can be safely loaded when all equipment is used properly and when the person responsible for the loading follows prescribed safety procedures. It provides a short list of the equipment that should be available in case of an emergency).

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

- Recommended Practice 1112, Developing a Highway Emergency Response Plan for Incidents Involving Hazardous Materials (Provides minimum guidelines for developing and emergency response plan for incidents involving hazardous liquid hydrocarbons such as gasoline or crude oil).
- Recommended Practice 1626, Storage and Handling Ethanol and Gasoline-Ethanol Blends at Distribution Terminals and Service Stations (Provides safety and fire protection guidelines for emergency response personnel and the facility).
- Recommended Practice 1627, Storage and Handling of Gasoline-Methanol/CoSolvent Blends at Distribution Terminal and Service Stations (Provides safety and fire protection guidelines for emergency response personnel and the facility).

Ongoing Initiatives/Additional Measures Implemented

Since September 11, several efforts focused on enhanced security have been initiated. For example:

- Many companies are now tracking security information and alert levels and have appropriate security procedures in place to respond to the alert levels.
- Many companies have developed and implemented security procedures.

Added security measures already implemented may include:

- Companies have modified their assessment of their physical security, from the threat of a theft (protection of product) to that of a hostile threat
- Terminal gates are now locked around the clock with card-in procedures in effect
- Facilities are instructing drivers not to leave their truck running unattended or to leave keys in their trucks (trucks are kept locked while driving and unloading)
- Companies are meeting with local police and fire personnel to discuss emergency procedures and issues
- Electronic locks have been added on pumps at loading facilities to prevent theft
- Companies are assessing the need for 24/7 attendants for additional security
- Companies are considering biomarker identification technology for terminals
- Companies are reassessing hiring procedures (includes criminal background checks for new hires and existing employees)
- Heightened awareness at all facilities and asking all employees to be vigilant for suspicious behavior or activities
- Use of video/cctv to monitor remote areas like docks and gates.

9.4 Security Guidelines

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

- Each operator should assess the potential risk of a terrorist attack. The assessment may include a determination of the likelihood of an act or attack, the type of terrorist action likely, and the consequences of an attack. The assessment should take into account the hazards of the material carried, volume of the shipment for tank trucks and rail cars or the type, size, the routes taken and location of the facility for terminals or gas stations. The assessment may include: 1) the potential risk to workers, 2) the potential risk to the surrounding community, 3) the potential impact to the local and national energy supply, and 4) the potential risk to adjacent facilities and infrastructure.
- If, after conducting the assessment, the operator determines that a security plan is needed, the operator should develop a security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, theft, or event, and 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets and terrorist tactics and periodically tested, as appropriate.

- Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout its organization. Operators should respond appropriately to this information to safeguard potential targets. Operators should also, as appropriate, report suspicious activities and behaviors, attempted incursions, terrorists' threats, or actual events to the appropriate agencies.
- Operators should be aware of the DOT unsatisfactory carrier reports and on the licensing status of their drivers.
- Each operator should establish clear communication channels and responsibilities for assessing, preparing for, responding to and recovering from potential or actual threats.
- Operators should be aware of existing regulations, standards and operating practices as they relate to transportation and facility security.

9.5 Elements of a Security Plan

In developing a security plan, the operator should consider several basic elements. The security plan framework shown in Figure 9.1 provides a common structure upon which an operator may develop a security plan. In developing a security plan, an operator, to the extent possible, should consider its unique security risks, and then, if possible, assess the risks to ensure the plan addresses these risks. There are many different approaches to implementing the different elements identified in Figure 9.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all situations. This guidance recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 9.1 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 risk assessment approach depends in part on what risk related data and information are available. Conversely and while performing a risk assessment, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and risk assessment elements could be highly integrated and iterative.

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

9.6 Security Plan Framework

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

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

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

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

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

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that might lead to system failures are controlled. As noted previously, a risk assessment may identify other risks that should be addressed.

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

Reassess Risk. Risk assessments should be performed periodically to factor in recent operating data, consider changes to the facility design, change in transportation routes, carrier changes and to analyze the impact of any external changes that may have occurred since the last risk assessment, 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 risk assessments to ensure the analytical process reflects the latest understanding of the security issues.

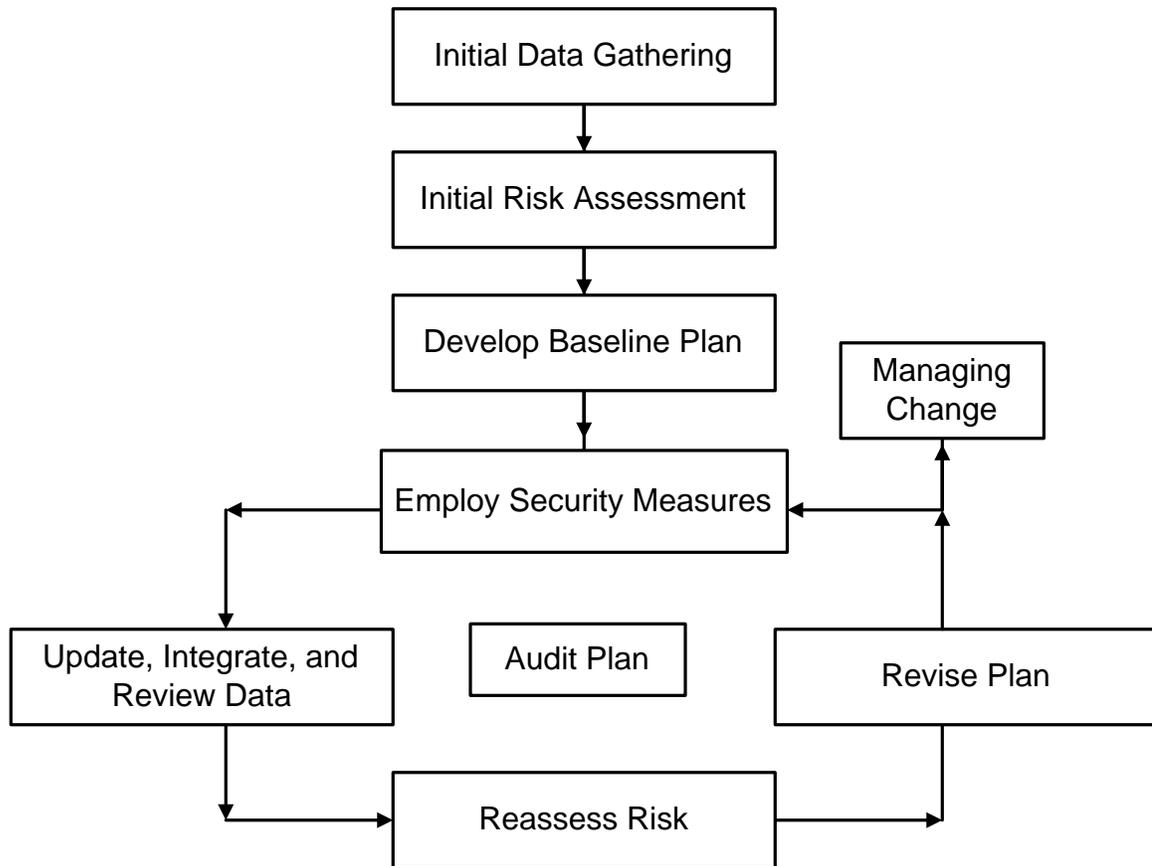
Revise Plan. The baseline security plan should be transformed into an on-going security assessment plan that is periodically updated to reflect new information and the current understanding of security risks. As new risks or new manifestations of previously known risks are identified, additional mitigation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

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

Managing Change. A systematic process should be used to ensure that changes to a facility (or transportation vehicle) are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future risk assessments to be sure the risk assessment 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 9.1, a security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. Risk assessments must be periodically updated and revised to reflect current vehicle or facility conditions so operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

Figure 9.1
Framework for a Security Plan



9.7 Security Conditions and Potential Response Measures

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

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

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

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

Access Control/Perimeter Protection

- Having all contractors and visitors check or sign in and out of designated facilities at the designated location(s) within the facility.
- Ensuring existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting. Ensuring that transportation vehicles implement security measures to prevent tampering and theft while parked, in transit or while loading or unloading. Identifying those additional security measures and resources that could enhance the security at the higher alert levels, e.g. increased surveillance or lighting.

Communications

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

Training/Policies/Procedures/Plans

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

- Advising all personnel to report to the appropriate agencies the presence of unidentified individuals and transportation vehicles including those being operated out of the ordinary, abandoned parcels or packages, and other suspicious activities.
- Developing procedures for shutting down and evacuating the facility, if considered necessary, in case of imminent attack. Developing procedures for returning vehicles to secure locations.
- Incorporating security awareness and information into public education programs at onshore facilities and notifications to emergency response organizations as appropriate.
- Surveying surrounding areas and along transportation routes to determine if activities exist that may pose security risks to the facility, e.g., airports, government buildings, industrial facilities, railroads and other facilities.
- Ensuring contingency and business continuity plans are current and include a response to terrorist threats.
- Reviewing existing emergency response plans and modifying them, if required, in light of potential threats.

Cyber Security

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

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

Perimeter Protection/Access Control

- Securing all facilities, buildings and storage areas not in regular use, if possible. Increasing frequency of inspections and patrols within the facility including the interior of buildings and along the facility perimeter.
- Inspecting perimeter fencing and repairing all fence breakdowns. Routinely inspect vehicles for suspicious items. In addition, reviewing all outstanding maintenance and capital project work that could affect the security of facilities.

CONFIDENTIAL

- Reducing the number of access points, if possible, for transportation vehicles and personnel to minimum levels and periodically spot checking the contents of vehicles at the access points. Being alert to vehicles or watercraft parked or moored for an unusual length of time in or near a facility.
- Checking designated unmanned sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increasing surveillance in designated areas.
- Requiring visitors to check in at the designated facility office or to designated personnel and verifying their identification - being especially alert to repeat visitors or outsiders who have no apparent business at the facility and are asking questions about the facility or transportation operations or related issues including personnel. Familiarizing facility personnel with vendors who service the facility or transportation vehicles and investigating unusual changes in vendor personnel.
- Inspecting all packages/equipment coming into a facility. Not opening suspicious packages. Reviewing the USPS "Suspicious Mail Alert" and the "Bombs by Mail" publications with all personnel involved in receiving packages.

Communications

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

Training/Policies/Procedures/Plans

- Reviewing all operations plans, personnel details, and logistics requirements that pertain to implementing higher alert levels.
- Ensuring that an operator response can be mobilized appropriate for the increased security level. Reviewing communications procedures and back-up plans with all concerned.

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

Perimeter Protection/Access Control

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

CONFIDENTIAL

- Inspecting on a more frequent basis the interior and exterior of all buildings and around all storage tanks and other designated critical areas.
- Dedicating personnel to assist with security duties for transportation vehicles and at designated facilities with duties to monitor personnel entering the facility and to inspecting the area on a regular basis, reporting to facility management as issues surface.
- Limiting visitors and confirming that the visitor has a need to be and is expected at the facility. Escorting visitors while at the facility.

Communications

- Informing personnel of the change in alert status. Reviewing with employees the operations plans, personnel safety, and security details and logistic requirements that pertain to the increased security level. Implementing procedures to provide periodic updates to employees on security measures being implemented.
- Advising appropriate agencies that the facility is at an **Yellow** level and advising the measures being employed - requesting appropriate agencies to increase the frequency of their routine patrol of the facility if possible.
- Checking to ensure all emergency telephone, radio, and satellite communication devices are in place and they are operational.

Training/Policies/Procedures/Plans

- Confirming availability of security resources that can assist with extended coverage, if needed.
- Identifying locations where explosive devices could potentially be hidden near sensitive or vital areas.
- Instructing employees working alone or in transit to check-in on a periodic basis.
- Directing that all personal, operator, and contractor vehicles at designated facility sites are secured.

High Condition - Orange (MARSEC III): This condition applies when there is a high risk of terrorist attacks or an incident occurs or information is received indicating that some form of terrorist action against personnel and facilities is imminent. 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

- Reducing facility access points to the absolute minimum necessary for continued operation.
- Securing a trained and knowledgeable security workforce to man the impacted facilities or transportation vehicles - ensuring that all security personnel have been briefed concerning policies governing the use of force and pursuit.
- Increasing security patrol activity to the maximum level sustainable. Increasing perimeter patrols and inspections.
- Checking all security systems such as lighting and intruder alarms to ensure they are functioning. Installing additional, temporary lighting if necessary to adequately light all suspect areas or decreasing lighting to detract from the area.
- Prohibiting unauthorized or unidentified vehicles/personnel entrance to designated facilities.
- Inspecting all vehicles entering facilities, if possible, including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed.
- Limiting access to designated facilities to those personnel who have a legitimate and verifiable need to enter the facility. Implementing positive identification of all personnel. Evacuating all non-essential personnel.
- Implementing frequent inspection of designated facilities. Increasing patrolling or inspections at night and ensuring all vulnerable critical points are fully illuminated and secure.
- Protecting the impacted facility from an attack by a parked or moving vehicle - operator vehicles may be used for this purpose. Implementing centralized parking and shuttle service where feasible.
- Canceling or delaying all non-vital facility work conducted by contractors, or continuously monitor their work with operator personnel.

Communications

- Advising appropriate agencies that the facility is at a **Orange** alert level and advise the measures being employed - requesting an increase in the frequency of their patrol of the facility.
- Consulting with local authorities about control of public roads and accesses that might make the facility more vulnerable to terrorist attack if they were to remain open. Inform them of the location of the hazardous material transportation vehicles.

Training/Policies/Procedures/Plans

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

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

Perimeter Protection/Access Control

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

Training/Policies/Procedures/Plans

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

10.0 Security Guidelines for Oil and Natural Gas Production Operations

10.1 Purpose and Objective

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

10.2 Overview of Upstream Operations

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

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

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

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

These larger platforms mean a greater concentration of personnel, often 100 to 150 people.

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

10.3 Relevant Operational Standards and Industry Practices

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

The following list of recommended practices address operational measures:

- Recommended Practice 2A, Planning, Designing, Constructing Fixed Offshore Platforms (Contains engineering design principles and practices for fixed offshore platforms including assessment of existing platforms, and fire, blast, and accidental overloading).
- Recommended Practice 2FPS, Planning, Designing, Constructing Floating Production Systems (FPSOs) (This recommended practice provides guidelines for design, fabrication, installation, inspection and operation of floating production systems).
- Recommended Practice 2T, Planning, Designing, and Constructing Tension Leg Platforms (TLPs) (Summarizes available information and guidance for the design, fabrication and installation of a tension leg platform).
- Recommended Practice 14B, Design, Installation, Repair and Operation of Subsurface Safety Valve Systems (Provides guidelines for safe operating practices of equipment used to prevent accidental release of hydrocarbons to the environment in the event of unforeseen circumstances).
- Recommended Practice 14C, Analysis, Design, Installation and Testing of Basic Surface Safety Systems on Offshore Production Platforms (Describes processes and systems for emergency well shut-ins on offshore platforms).

- Recommended Practice 14H, Installation, Maintenance and Repair of Surface Safety Valves and Underwater Safety Valves Offshore (Provides guidelines for safe operating practices of equipment used to prevent accidental release of hydrocarbons to the environment in the event of unforeseen circumstances).
- Recommended Practice 14J, Design and Hazardous Analysis for Offshore Production Platforms (Provides procedures and guidelines for planning, designing, and arranging offshore production facilities and for performing a hazardous operations analysis).
- Recommended Practice 75, Development of a Safety and Environmental Management Program for Outer Continental Shelf Operations and Facilities (Provide guidance in preparing safety and environmental management programs for offshore facilities).
- Recommended Practice 750, Management of Process Hazards (Provides assistance in helping to prevent the occurrence of, or minimize the consequences of catastrophic releases of toxic or explosive materials).
- An Overview of Petroleum Industry Operations and An Assessment of Current Security Practices & Standards

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

- Recommended Practice 49, Drilling and Well Servicing Operations involving Hydrogen Sulfide (Describes response plans for wells involving hydrogen sulfide).
- Recommended Practice 54, Occupational Safety for Oil and Gas Well Drilling and Servicing Operations (Describes emergency response plans for oil and natural gas well drilling and servicing).
- Recommended Practice 74, Occupational Safety for Onshore Oil and Gas Production Operations (Describes general occupational safety and emergency response plans).
- Publication 761, Model Risk Management Plan for E&P Facilities (Provides a guideline on how affected facilities develop a risk management plan including hazard assessment, prevention and emergency response).

10.4 Security Guidelines

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

- Each operator should assess the potential security risk at its facilities. This informal assessment may include a determination of the likelihood of an act or attack, the type of action likely, and the consequences of an attack. The assessment should take into account the type, size, and location of the facility. The assessment may consider: 1) the potential risk to workers, 2) the potential risk to the surrounding community; 3) the potential impact to the local and national energy supply; and 4) the potential risk to adjacent facilities and infrastructure.
- If, after conducting the informal assessment, the operator determines that additional security planning is needed, the operator should develop a security plan that may include the following elements: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that may be considered at various security alert conditions, including the response to an actual attack, intrusion, or event, and; 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically based on evolving government intelligence on potential targets and terrorist tactics and periodically tested, as appropriate.
- Operators should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout the organization. Operators should respond appropriately to this information to safeguard potential targets. Operators should also report, as appropriate, suspicious activities and behaviors, attempted incursions, terrorist threats, or actual events to the appropriate agencies.
- Each operator should establish clear communication channels and responsibilities for assessing, preparing for, responding to and recovering from potential or actual threats.
- Each operator should establish and maintain effective liaison with local emergency response agencies and organizations, as appropriate.
- Operators should be aware of existing regulations, standards and operating practices as they relate to facility security.

10.5 Elements of a Security Plan

In developing a security plan, the operator should consider several basic elements. The security plan framework shown in Figure 10.1 provides a common structure upon which an operator may develop a security plan. In developing a security plan, an operator, to the extent possible, should consider its unique security risks, and then, if possible, assess the risks to ensure the plan addresses these risks. There are many different approaches to implementing the different elements identified in Figure 10.1 ranging along a continuum from relatively simple to highly sophisticated and complex.

There is no “best” approach that is applicable to all situations. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a security plan could be a highly integrated and iterative process. Although the elements depicted in Figure 10.1 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 risk assessment approach depends in part on what risk related data and information are available. While performing a risk assessment, additional data needs may be identified that can be used to better address potential vulnerability issues. These data gathering and risk assessment elements should be highly integrated and iterative, as appropriate.

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

10.6 Security Plan Framework

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

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

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

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

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

Employ Security Measures. In this element, the baseline security plan activities are implemented, the results are evaluated, and the necessary changes are made to assure risks that might lead to system failures are controlled. As noted previously, a risk assessment may identify other risks that should be addressed.

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

Reassess Risk. Risk assessments 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 risk assessment, 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 risk assessments to ensure the analytical process reflects the latest understanding of the security issues.

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

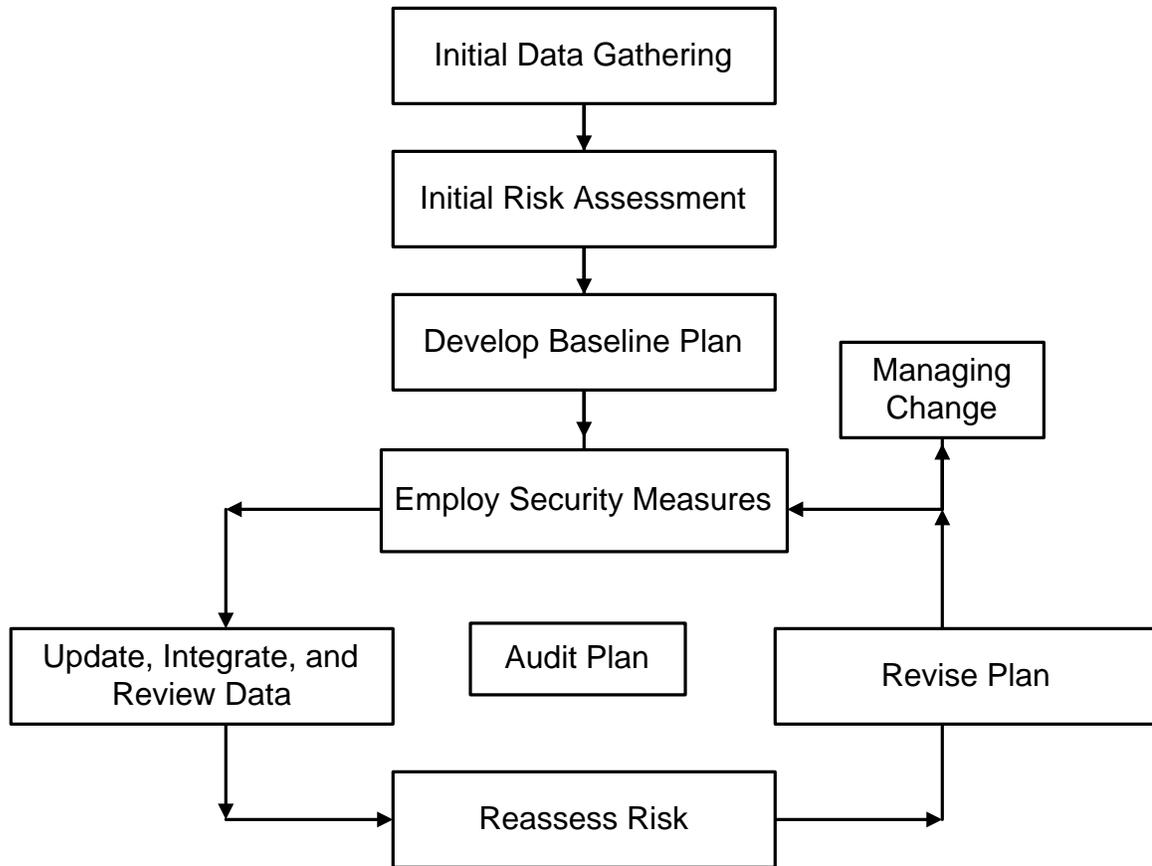
Audit Plan. The operator should collect information and periodically evaluate the success of its security assessment techniques and other mitigation risk control activities.

The operator should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions.

Managing Change. Production facilities and the environment in which they operate are never static. A systematic process should be used to ensure that changes to the facility are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future risk assessments to be sure the risk assessment 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 10.1, a security management program involves a continuous cycle of monitoring facility conditions, identifying and assessing risks, and taking action to minimize the most significant risks. Risk assessments must be periodically updated and revised to reflect current facility conditions so operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

Figure 10.1
Framework for a Security Plan



11.0 Security Guidelines for Marine Transportation

11.1 Overview of Segment Operations

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

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

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

11.2 Relevant Operational Standards and Industry Practices

11.2.1 U.S. Regulations

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

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

- 59 FR 34070 Facility Response Plans
- 62 FR 13991 Response Plans for Facilities Located Seaward of the Coast Line
- 61 FR 30533 Facility Response Plans for Pipelines (Interim Final Rule)
- 57 FR 7640 Coastwise Oil spill Response Cooperatives
- 60 FR 65478 Criminal Record Reviews in Renewals

CONFIDENTIAL

- 60 FR 45006 Designation of Lightering Zones
- 59 FR 42962 Escorts for Certain Tankers
- 60 FR 13318 Establishment of Double Hull Requirements for Tank Vessels
- 59 FR 40186 Existing Tank Vessel Requirements – Lightering requirements and Advanced Notification
- 62 FR 1622 Existing Tank Vessel Requirements – Structural Requirements
- 61 FR 39770 Existing Tank Vessel Requirements – Training, Survey and Maneuverability Measures
- 61 FR 7890 Facility Response Plans for Marine and Non-Marine Transportation Facilities
- 58 FR 48434 Lightering Requirements
- 59 FR 47384 National Contingency Plan Revisions
- 58 FR 13360 Pilotage in Prince William Sound
- 58 Fr 27628 Second Person Required (on bridge)
- 61 FR 1052 Tank Vessel Response Plans
- 59 Fr 49294 Term of Licenses, Certificates of Registry and Merchant Mariners Documents
- 57 FR 14483 Vessel Communication Equipment Regulations
- 59 FR 36316 Vessel Traffic Service

11.2.2 International Conventions and Treaties

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

11.3 Ongoing Initiatives/Additional Measures Implemented Since September 11

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

- Identified high interest vessels and prioritized critical infrastructure so that its limited resources could be applied in an efficient manner.
- As part of the Homeland Security Plan, the U.S. Coast Guard established Maritime Security (MARSEC) levels (MARSEC I - III) for assessing security response capabilities, activities, and equipment inventories.
- Increased the Advanced Notice of Arrival Information (NOA) time for commercial vessels arriving from foreign ports from 24 to 96 hours, to provide more analysis of crew and passenger lists, etc.
- Instituted a Sea Marshal program for high-risk ports on the west coast (San Francisco, San Diego, and Los Angeles).
- Held a three-day public workshop (January 28-30, 2002) to discuss/assess security procedures, programs, and capabilities within marine transportation systems, in an effort to ascertain whether improvements (i.e., new regulations, the development of industry standards) are necessary.

12.0 Cyber/Information Technology Security Guidelines for the Oil and Natural Gas Industry

12.1 Purpose & Objective

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

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

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

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

The guidance provided herein and in ISO/IEC International Standard 17799 does not attempt to provide an all-inclusive list of cyber security considerations, but does provide a basis for measures that could be implemented when evaluating and implementing cyber security measures.

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

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

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

Oil and natural gas industry cyber initiatives that are currently underway include:

- Companies recognize that effective security is a combination of layered security processes, policies, procedures, education, awareness and assessments to ensure compliance. Companies currently use a combination of firewalls, intrusion detection, antivirus and risk assessment programs, host intrusion detection systems and other audit programs to safeguard their computer systems. Each company analyzes and assesses its needs based on individual vulnerability and probability assessments.
- Companies are clued into individual efforts at the local and/ or national level such as InfraGard, National Infrastructure Protection Center (NIPC), and EPRI security committee to receive security threat and monitoring information.
- In November 2000 the API Information Technology Security Forum (ITSF) was formed to address the cyber security of the oil and natural gas industry. Committee members maintain a high level of cyber security and have been focusing on activities and initiatives in increasing security awareness within the industry; privacy; policies; risk management and mitigation; and emerging technologies. The ITSF developed and delivered a *Framework for a Computer Security Incident Response Plan (November 2001)* to provide guidance on reporting cyber-related security incidents. This document is provided in Appendix A.
- Companies have individually taken steps to reduce computer incidents such as: confidential information being given out by employees, use of weak passwords, unauthorized access to facilities and networks, telephone fraud, spread of computer viruses, software piracy, and unauthorized email or Internet usage.

Oil and natural gas companies, have taken additional precautions to enhance cyber security in response to the catastrophic events of September 11, 2001. These enhanced measures include:

- Increased electronic access control to facilities and networks, by use of badges, authentication services and proximity controls.
- Reexamined and tested disaster recovery plans in mainframe, PC and Unix environments.
- Applied knowledge acquired through international operations in countries more accustomed to civil unrest and possible acts of terrorism.

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

Since every company's cyber/information technology infrastructure, systems, and information are different, companies have been individually evaluating their own security preparedness and the relative vulnerability of cyber-related systems and information. A risk-based approach would take into account both the likelihood and possible consequences of potential terrorist acts. These will vary widely for individual companies depending on the size, complexity, location, associated products, and facilities for particular assets.

12.3 Security Guidelines

The following provide general security guidance to oil and natural gas companies relative to potential acts of terrorism:

- Each company should assess the potential risk of a cyber terrorism attack on its operations and assets. The assessment should include a determination of the likelihood of an act or attack, the type of terrorist action likely to occur, and the consequences of an attack. The assessment should take into account the type, size, and location of the facility. The consequence analysis should include: 1) the potential impact to local and national energy supply; 2) the potential risk to workers and the surrounding community; 3) the potential risk to company's financial stability; 4) the potential impact on customers; and 5) the potential risk to adjacent companies and infrastructure.
- Each company should develop a security plan to safeguard those facilities and infrastructure deemed by the company, or the company in conjunction with government officials to be targets with potential risk. The plan should describe: 1) an assessment of the potential risks, terrorist actions and consequences; 2) the detection and deterrent measures being taken to mitigate potential risks; 3) the responses that will be taken at various security alert conditions, which describe progressive, low to high, levels of potent risk of a terrorist action), including the response to an actual attack, intrusion, or event, and; 4) the recovery from an event or events. The plan should be kept confidential for security reasons. The plan should be reevaluated and

updated periodically based on evolving government intelligence on potential targets and terrorist tactics and periodically tested, as appropriate.

- Companies should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout its organization. Companies should respond appropriately to this information to safeguard potential targets. Companies should also appropriately report suspicious activities and behaviors, attempted incursions, terrorists' threats, or actual events to the responsible law enforcement agencies.
- Each company should establish clear communication channels and responsibilities for assessing, preparing for, responding to and recovering from potential or actual threats.
- At a minimum, companies and their facilities should comply with existing regulations, standards and operating practices.

12.4 Elements of a Cyber Security Management Plan

In developing a cyber security management plan, several basic elements should be considered. The cyber security management plan framework shown in Figure 12.1 provides a general structure upon which a cyber security management plan can be developed. When developing a cyber security management plan, one should consider, to the extent possible, the company's unique security risks, and then, if possible, assess the risks to ensure the plan addresses them. There are many different approaches to implementing the different elements identified in Figure 12.1 ranging along a continuum from relatively simple to highly sophisticated and complex. There is no "best" approach that is applicable to all companies. This guideline recognizes the importance of flexibility in designing security plans and provides guidance commensurate with this need.

It is important to recognize that a cyber security management plan could be a highly integrated and iterative process. Although the elements depicted in Figure 12.1 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 risk assessment approach depends in part on what risk related data and information are available. Conversely and while performing a risk assessment, additional data needs are usually identified to better address potential vulnerability issues. Thus the data gathering and risk assessment elements could be highly integrated and iterative.

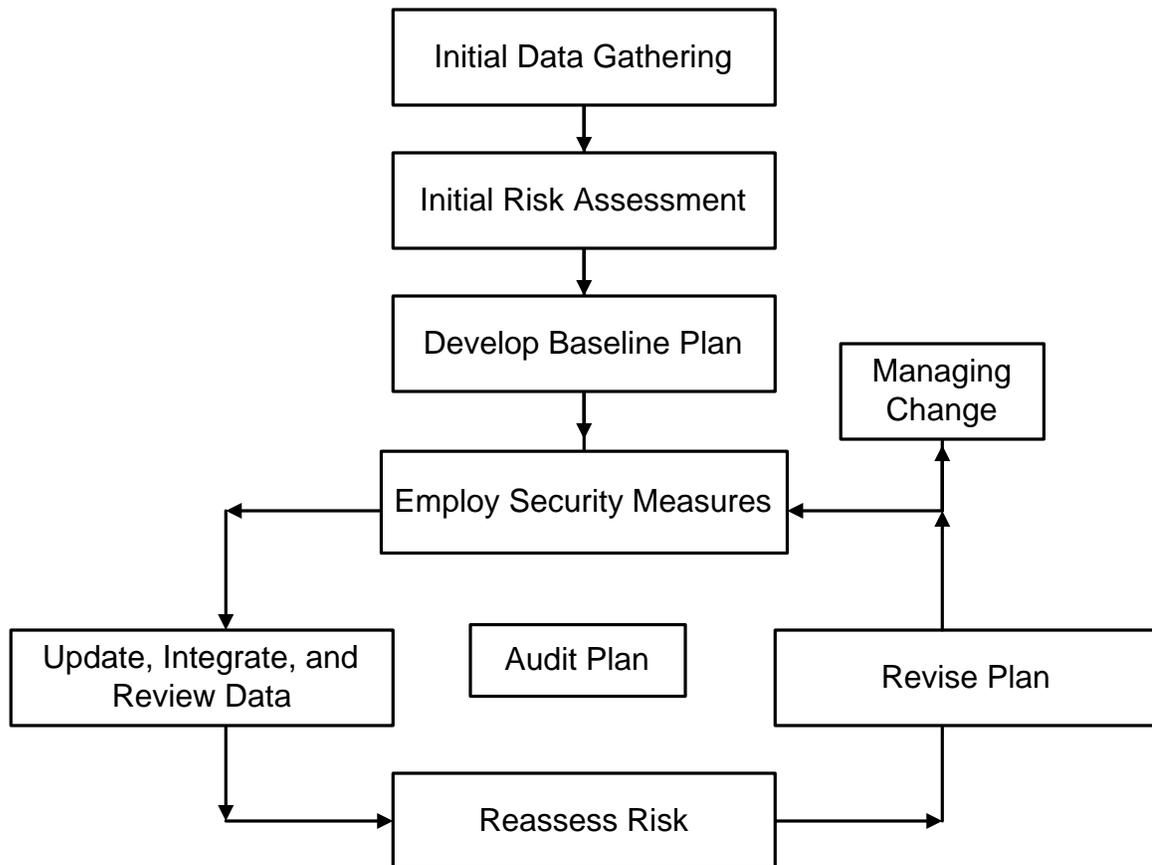
A cyber security management plan could include elements such as:

- Risk assessment and prevention strategies
- Incident reporting mechanism
- Communications plan with appropriate local, state and federal agencies
- Incident investigation procedures
- Emergency response and crisis management programs

- Reassessment of risk assessments
- Reassessment of security management plan

A cyber security management plan should be an integral part of the company's overall security management program.

Figure 12.1
Framework for a Cyber Security Plan



12.5 Security Management Plan Framework

ISO/IEC International Standard 17799, *Information technology – Code of practice for information security management*, describes a framework for creating a cyber security program. This framework has been endorsed by API's Information Technology Security Forum as voluntary guidance to protect the oil and natural gas industry against acts of cyber terrorism. Information on how to obtain this standard is provided at <http://webstore.ansi.org/ansidocstore/iso.asp>. The standard attempts to ensure preservation of confidentiality, integrity, and availability of user access, hardware and software, and data. The standard involves eight steps in the security process: create an information security policy, select and implement appropriate controls, obtain upper management support, perform security risk assessment, create statement of applicability for all employees, create information security management system, educate and train staff, audit.

Additionally, in November 2001 the API Information Technology Security Forum developed and delivered a *Framework for a Computer Security Incident Response Plan (November 2001)* to provide guidance on reporting cyber-related security incidents. This document is provided in Appendix A.

CONFIDENTIAL

APPENDIX A

FRAMEWORK FOR A COMPUTER SECURITY INCIDENT RESPONSE PLAN

CONFIDENTIAL



American
Petroleum
Institute

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

prepared by:

API IT Security Forum
Security Operations and Best Practices Sub-Team

November 2001

Table of Contents

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

Acronyms, Definitions and Terms

APPENDICES

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

1.0 Background

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

2.0 Mission Statement

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

3.0 Scope

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

4.0 Incident Types

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

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

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

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

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

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

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

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

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

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

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

5.0 Incident Escalation Criteria and Security Level

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

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

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

6.0 Priorities in Incident Handling

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

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

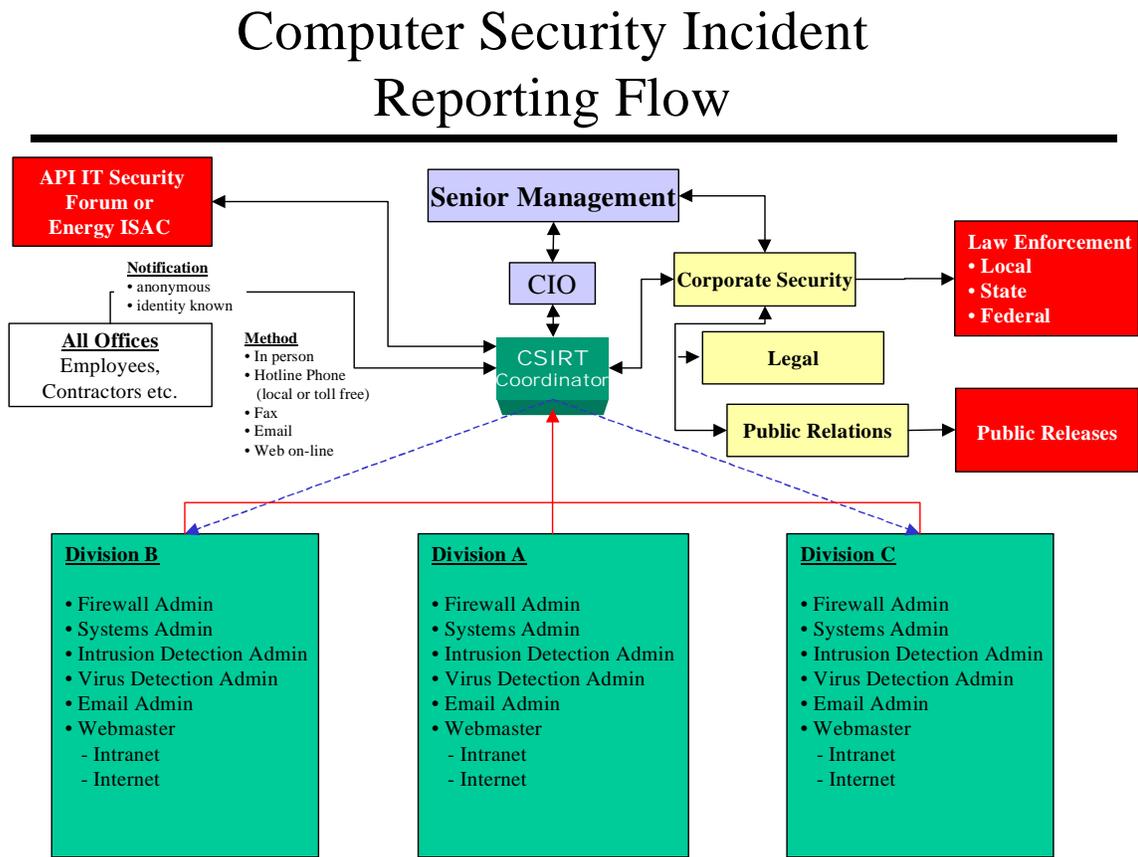
Priority two – protect company confidential and/or sensitive data; national safety and security is second only to protecting human life.

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

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

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

7.0 Computer Security Incident Reporting Flow



- 7.1 Information Security is the responsibility of every employee and contractor that uses <Company Name> information technology resources.
- 7.2 When an incident or infraction is noted, whether known or suspect, it must be immediately reported to the CSIRT Coordinator and the employee's supervisor (incident may also be reported to Help Desk, who in turn reports incident to CSIRT Coordinator).
- 7.3 Ideally, the identity of the individual reporting the incident is provided when the report is filed with the CSIRT. However, incidents may also be reported anonymously.
Note: Confidentiality will be strictly maintained.
- 7.4 The preferred communication methods for reporting an incident to the CSIRT are: in person, hotline phone number (local or toll free), Fax, Email and Web-based. In the event of a system compromise, electronic-based (email, web) communications is not recommended unless it is encrypted since such methods of communication are easily intercepted.
- 7.5 Incidents detected by system administration personnel will be immediately reported direct to the CSIRT.

- 7.6 The CSIRT Coordinator will assess the severity of a reported incident and notify the CIO, other division IT Security Advisors and IT Management, as necessary.
- 7.7 The CIO will report incident summary information to senior management.
- 7.8 The CSIRT Coordinator will notify Corporate Security of the incident.
- 7.9 Senior Management, Corporate Security, Legal and Public Relations will determine whether to contact law enforcement agencies, issue official press releases, or contact members of the API IT Security Forum. *Note: Any incident determined to be a violation of local, state, or federal law must be reported to the appropriate law enforcement agency.*

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

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

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.2 **CSIRT On-Site Technical Team Members.** The On-Site Team members are the subject matter experts that are deployed to the location(s) of the incident. They are responsible for securing the area, surveying the situation and initiating the containment, eradication, recovery and resumption of normal business operations. Team members should have special skills and experience in handling incidents of varying types (e.g. Unix, Microsoft NT/Win2K, Virus eradication etc.)

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.3 **Management Decision Team Members.** This CSIRT Coordinator translates the technically oriented assessments of the On-Site CSIRT Team into recovery steps for the Management Decision team to determine business decisions affected by the incident and direct actions to be taken by the team. The Management Decision Team works with the organization's public affairs, corporate security and legal departments to coordinate information statements that would be provided to stock holders, outside organizations or public media. They are also responsible for communicating the status of the incident with corporate executives.

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.4 **Public Relations Team Members.** The Public Relations team is responsible for answering questions from the public regarding corporate activities. When a security-related incident occurs, it is this team's responsibility to disseminate appropriate information to the public.

	1	2	3	4	5
Name					
Department					
Roles and Responsibilities					
Work phone #					
Cell phone #					
Home phone #					
E-mail					

8.5 **Law Enforcement Agency Contacts** (local, state and federal).

Agency/Name	<u>Agency Functions and Responsibilities</u>	Phone #	Phone #	E-mail

9.0 Incident Investigation and Response Steps

9.1 **Incident handling** starts with *preparation, training and testing*. Preparation involves establishing a program to identify critical resources and information that if disrupted, damaged or lost would impact the organizations ability to conduct business. Once the critical resources and information have been identified, the organization must determine the necessary protection controls and implement them. Additional steps include preparing incident handling guidelines or contingency response plans to minimize the impact of an incident when one occurs, training staff to respond to various incidents and testing the response capability. Paragraphs 9.2 – 9.8 are the generic life-cycle steps of Incident Investigation and Response. Each organization should develop appropriate processes to handle security breaches (perimeter and firewall intrusions, operating system attacks, Distributed Denial of Service (DDoS) attacks, malicious code attacks etc. These processes should be considered living entities that require continual updates and improvement.

9.2 **Event documentation** is a critical aspect of incident investigation and handling. Documentation directs the investigation life cycle. Without an accurate and verifiable account of events, the investigation will be rendered useless. This

process begins with the Computer Security Incident Report and the assignment of a relevant Incident Tracking Number.

- 9.3 **Incident identification** involves a quick-response triage assessment of the situation to determine exactly what the problem is and the severity of it.
 - 9.3.1 Systems should be checked for the following symptoms:
 - 9.3.1.1 System crashes
 - 9.3.1.2 New user accounts
 - 9.3.1.3 System access points
 - 9.3.1.4 New files
 - 9.3.1.5 Accounting discrepancies
 - 9.3.1.6 Changes in file lengths or dates
 - 9.3.1.7 Attempts to write to system files
 - 9.3.1.8 Modified or deleted data
 - 9.3.1.9 Unexplained poor system performance
 - 9.3.1.10 Other anomalies
 - 9.3.2 Identify and document all evidence.
 - 9.3.3 Study and review the system and network logs.
- 9.4 **Containment** should occur only if the indications observed during the Identification stage conclusively show that an incident has or is occurring. The primary goal is to minimize the breadth of the incident and isolate it from causing wide-spread damage.
 - 9.4.1 Do not alter the system until an image backup is performed.
 - 9.4.2 Do not try to contact the attacker with ping, telnet or other tools.
 - 9.4.3 Backup the system to new media and safely store it before proceeding.
 - 9.4.4 Determine the necessity of disconnecting and isolating a system component(s) from other system components.
- 9.5 **Eradication** is the time in the process when infected files are fully deleted or the system(s) is restored to its normal operational state.
- 9.6 **Recovery** involves returning the system back to normal.
 - 9.6.1 Change passwords on compromised system.
 - 9.6.2 Consider changing system's IP address or name.
 - 9.6.3 Restore the system from the most recent clean backup.
- 9.7 **Follow-up** involves performing a post-incident analysis. Document exactly what happened and when.
 - 9.7.1 After recovering, evaluate the system again to verify normal operational functions.
 - 9.7.2 Perform system and network vulnerability assessments using special tools.
 - 9.7.3 Study the attack and try to learn how it was executed.
 - 9.7.4 If vulnerability is determined, check if it exists on other similar systems within the enterprise.
 - 9.7.5 Evaluate the incident response process and document lessons learned. Follow-up activities may include asking some of the following questions:
 - Was there sufficient preparation for the incident?
 - Did detection occur promptly? If not, why not?

Could additional tools have helped the detection and eradication process (how to avoid further exploitation)?

Was the incident sufficiently contained?

Was communication adequate or could it have been better?

What practical difficulties were encountered?

How much is the associated monetary cost? (personnel time, time to restore systems, etc.)

How much did the incident disrupt ongoing operations?

Were any data irrecoverably lost, and, if so, what was the value of the data?

Was any hardware damaged?

9.7.6 Determine the retention period for the documentation.

9.7.7 Review external communication flow and risk assessment process.

- 9.8 **Archive** the incident file and all supporting evidence related to the investigation in an access-controlled environment in the event it is needed to support legal or other action. Strict “Chain of Custody” must be maintained.

10.0 Resources

Energy Information Sharing and Analysis Center (Energy ISAC) <http://energyisac.com/>

National Security Agency (NSA) Glossary of Terms,
<http://www.sans.org/newlook/resources/glossary.htm>

National Infrastructure Protection Center “Incident Reporting Form (Print Version – pdf file) <http://www.nipc.gov/incident/incident.htm>

National Institute of Standards and Technology “Establishing a Computer Security Incident Response Capability” NIST Pub 800-3, November 1991
<http://csrc.nist.gov/topics/incidentNIST/index.htm>

The SANS Institute “Incident Handling Step By Step” version 1.5, May 1998
<http://www.sans.org>

University of California, Lawrence Livermore National Laboratory “Responding To Computer Security Incidents: Guidelines for Incident Handling”. Schultz, Eugene Jr.; Brown, David S; Longstaff, Thomas A., July 23, 1990.

Acronyms Definitions and Terms

ACRONYM – A Contrived Reduction Of Nomenclature Yielding Mnemonics

API – American Petroleum Institute

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

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

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

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

APPENDICES

APPENDIX I

Emergency Action Quick Reference Guide

<p>Step #1: <u>Remain calm.</u> Even a fairly mild incident tends to raise everyone's stress level. Communication and coordination become difficult. Your calm can help others avoid making critical errors.</p>
<p>Step #2: <u>Take good notes.</u> Keep in mind that your notes may become evidence in court. Make sure you answer the four Ws - Who, What, When, and Where- and, for extra credit, Why and How. You may find a small hand-held tape recorder to be a valuable tool.</p>
<p>Step #3: <u>Notify the right people and get help.</u> Begin by notifying your security coordinator and your manager and asking that a coworker be assigned to help coordinate the incident handling process. Get a copy of the corporate phonebook and keep it with you. Ask your helper to keep careful notes on each person with whom he or she speaks and what was said. Make sure you do the same.</p>
<p>Step #4: <u>Enforce a "need to know" policy.</u> Tell the details of the incident to the minimum number of people possible. Remind them, where appropriate, that they are trusted individuals and that your organization is counting in their discretion. Avoid speculation except when it is required to decide what to do. Too often the initial information in an incident is misinterpreted and the "working theory" has to be scrapped.</p>
<p>Step #5: <u>Use out of band communications.</u> If the computers may have been compromised, avoid using them for incident handling discussions. Use telephones and faxes instead. Do not send information about the incident by electronic mail, talk, chat, or news; the information may be intercepted by the attacker and used to worsen the situation. When computers are being used, encrypt all incident handling e-mail.</p>
<p>Step #6: <u>Contain the problem.</u> Take the necessary steps to keep the problem from getting worse. Usually that means removing the system from the network, though management may decide to keep the connections open in an effort to catch an intruder.</p>
<p>Step #7: <u>Make a backup of the affected system(s) as soon as practicable.</u> Use new, unused media. If possible make a binary, or bit-by-bit backup.</p>
<p>Step #8: <u>Get rid of the problem.</u> Identify what went wrong if you can. Take steps to correct the deficiencies that allowed the problem to occur.</p>
<p>Step #9: <u>Get back in business.</u> After checking your backups to ensure they are not compromised, restore your system from backups and monitor the system closely to determine whether it can resume its tasks.</p>
<p>Step #10: <u>Learn from this experience,</u> so you won't be caught unprepared the next time an incident occurs.</p>

APPENDIX II

CSIRT Incident Response Worksheet Sample

The incident response worksheet is designed for use by the response team to ensure uniformity of the documented information gathered by each team member. This will make the review of information by the CSIRT Coordinator easier. Also keep in mind that an incident should be investigated as though it were going to be presented as evidence for legal action.

Date MM/DD/YY		
Incident Tracking Number 000X – YYYY/MM/DD/HH:MM		
Time	Observation	Action Taken

NAME (print)	SIGNATURE
1)	
2)	
3)	

APPENDIX III

User Incident Report Form Sample

The user incident report form should be used by the general user population to report all suspected incidents. At a minimum, the following information must be obtained, whether the user submits the report or the report is filled out by a third party.

Date:	
Name:	
Department:	
Phone Number:	
Nature of Incident:	<Describe briefly what you observed, where the incident occurred and name(s) of persons involved (if applicable)>

APPENDIX IV

Incident Investigation Report Form Sample

The incident investigation report form is a detailed report that provides details of the incident and investigative information. The form is initiated by the CSIRT Coordinator and periodically updated throughout the duration of the incident investigation until closure. Depending on the nature and severity of the incident, this report may remain open for as little as an hour or as long as several days or weeks.

<u>Report Date</u>	<u>Incident Tracking Number</u>
August 1, 2001	000X - YYYY/MM/DD/HH:MM

Reported By:

<u>Name</u>		<u>Date /</u>	
<u>Title</u>		<u>Time Reported</u>	
<u>Organization</u>		<u>Phone Number</u>	
<u>Description</u>			
<u>Details</u>	<u>August 1, 2001:</u>		
<u>Open Actions</u>			
August 1, 2001:			
<u>The following items remain open</u>		<u>Actionee</u>	
<u>Closure</u>			

Submitted By:

<u>Name</u>		<u>Phone Number</u>	
<u>Title</u>			
<u>Organization</u>			

APPENDIX V

Incident Tracking Form Sample

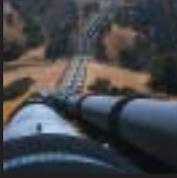
The incident tracking form is a spreadsheet or database for the purpose of maintaining a log of incidents reported during the year. Each organization should decide what the severity or frequency guidelines are for documenting this information. For instance you may not want to track every virus detected and eradicated.

Incident Tracking Number	Date Opened	Date Closed	Description	Loc.	Type of Incident							
					Access	e-mail	Unauthorized Use	Loss or Theft	Intrusion	Denial of Service	Other	
000X – YYYY/ MM/ DD/ HH:MM												

APPENDIX VI

NIPC Incident Reporting Form

The National Infrastructure Protection Center (NIPC) incident reporting form may be found at <http://www.nipc.gov/incident/incident.htm>. The NIPC was established to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response to threats or attacks against the critical infrastructures of the United States. These infrastructures include telecommunications, energy, banking and finance, water systems, government operations, and emergency services.



Petroleum Refining

Pipeline Transportation (Liquids)

Petroleum Products Distribution and Marketing

Oil and Natural Gas Exploration and Production

Marine Transportation

Petroleum Cyber/Information Technology (IT) Infrastructure