Security for Worldwide Offshore Oil and Natural Gas Operations

API RECOMMENDED PRACTICE 70I
FIRST EDITION, MAY 2004

REAFFIRMED, JANUARY 2012

AMERICAN PETROLEUM INSTITUTE

Security for Worldwide Offshore Oil and Natural Gas Operations

Upstream Segment

API RECOMMENDED PRACTICE 70I
FIRST EDITION, MAY 2004

REAFFIRMED, JANUARY 2012

AMERICAN PETROLEUM INSTITUTE

SPECIAL NOTES

This document is intended to offer guidance to members of the petroleum industry engaged in exploration and production operations. 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 or contractor efforts. With respect to particular circumstances, local, state and federal laws and regulations should be reviewed.

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

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

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

FOREWORD

This recommended practice is under the jurisdiction of the American Petroleum Institute Upstream Department's Executive Committee on Drilling and Production Operations. The goal of this voluntary recommended practice is to assist the offshore oil and gas industry in promoting security. THE PUBLICATION DOES NOT, HOWEVER, PURPORT TO BE SO COMPREHENSIVE AS TO PRESENT ALL OF THE RECOMMENDED OPERATING PRACTICES THAT CAN AFFECT SECURITY IN OFFSHORE OIL AND GAS OPERATIONS. API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any national, federal, state, municipal or other regulation with which this publication may conflict.

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

Suggested revisions are invited and should be submitted to API, Standards Department, 1220 L Street, NW, Washington, DC 20005

CONTENTS

Security for Worldwide Offshore Oil and Natural Gas Operations

1 Scope, Purpose and Objective

This publication is intended to assist the offshore oil and natural gas drilling and producing operators and contractors in assessing security needs during the performance of oil and natural gas operations. The offshore oil and natural gas industry uses a wide variety of contractors 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.

2 Definitions

2.1 company security officer (CSO): The CSO is responsible for the maintenance of the Security Plan. The CSO shall have access to relevant security information. The CSO shall determine which information, and by what means, it is communicated. The CSO may delegate duties as necessary to assure timely completion of responsibilities. The CSO may be assigned other duties and responsibilities unrelated to security.

2.2 contractor: the individual, partnership, firm, or corporation that is hired to do a specific job or service, such as a production operator, drilling or well servicing contractor or to provide contract employees to an owner/operator; a contractor is also the individual, partnership, firm, or corporation retained by the owner or operator to perform other work or provide supplies or equipment. The term contractor shall also include subcontractors.

2.3 facility: Any artificial island, installation, or other device permanently or temporarily attached to the subsoil or seabed of offshore locations, erected for the purpose of exploring for, developing, or producing oil, natural gas or mineral resources. This definition includes mobile offshore drilling units (MODUs).

2.4 facility owner/operator: The individual, partnership, firm, or corporation having control or management of offshore operations. The owner/operator may be a lessee, designated agent of the lessee(s), or holder of operating rights under an operating agreement.

2.5 facility security officer (FSO): The individual that is responsible for security duties as specified by the owner/operator at one or more facilities, depending on the number or types of facilities a company operates. Where a person acts as the FSO for more than one facility, it should be clearly identified in the facility security plan for which facilities this person is responsible. The FSO may be a collateral duty provided the person is fully capable to perform the duties and responsibilities required of the FSO.

2.6 point of embarkation: The heliport or dock facility from which personnel and materials are shipped to or received from the offshore facility. Appropriate security measures at these facilities are critical.

2.7 security vulnerability assessment (SVA): A secondary evaluation that examines a facility's characteristics and operations to identify potential threats or vulnerabilities and existing and prospective security measures and procedures designed to protect a facility.

2.8 threshold characteristics/operating conditions: Criteria established by relevant governmental agencies or the facility owner/operator for screening critical offshore facilities. This is the primary Facility evaluation.

3 Relevant Operational Standards and Industry Practices

API and the oil and gas industry maintain a number of design and operational recommended practices that address aspects of safety and security in offshore oil and natural gas operations. 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 offshore oil and natural gas operating facilities.

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.

The following information sources and recommended practices address prevention, safety, communications, 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 T1, O*rientation Program for Personnel Going Offshore for the First Time.*

4 Security Policy

Each owner/operator should develop a policy that clearly defines its security goals and commitments including the protection of personnel, facilities and other assets. A sample policy is included in Appendix B.

5 Security Awareness

5.1 With regard to manned facilities, a key step to improving security and preventing an incident is ensuring that all employees are aware of security issues that could affect their working environment.

5.2 Facility owners/operators and contractors should keep abreast of the latest security alerts and government intelligence information and disseminate this information, as appropriate, throughout the organization. Facility owners/operators should evaluate and respond appropriately to this information to safeguard personnel and assets.

5.3 Facility owners/operators should report, as appropriate, suspicious activities and behaviors, attempted incursions, terrorist threats, or actual events to the appropriate agencies. See Appendix A for an example communications protocol.

5.4 Each facility owner/operator should establish clear communication channels and procedures for assessing, preparing for, and responding to potential or actual threats.

5.5 Each facility owner/operator should establish and maintain effective liaison with local emergency response agencies and organizations, as appropriate.

5.6 Each facility owner/operator should be aware of existing security regulations, standards and operating practices as they relate to their assets.

5.7 Each facility owner/operator should develop a policy for control of relevant security sensitive information (SSI).

6 Security Vulnerability Assessment (SVA)

Prior to conducting the SVA, the first step should be a characterization of the facility or the group of similar facilities attributes, e.g. the quantity of oil and/or natural gas produced, the number of personnel on board, proximity to shipping lanes, physical access to the facility, and existing security measures and procedures already in place, such as at the point(s) of embarkation.

If a facility meets or exceeds any of the threshold characteristics or operating conditions established by the relevant government, or the owner/operator, a SVA may be required. Additionally, a facility may by deemed critical by a particular owner/operator for a variety of other reasons. Each owner/operator should not only review the threshold characteristics/operating conditions, if applicable, they should also determine if a SVA is warranted based on their own unique criteria.

If the characterization results reflect appropriate security measures are already in place at point of embarkation, a SVA and additional measures may not be warranted.

After an initial evaluation to determine which facilities are critical, a security vulnerability assessment (SVA) should be conducted for all critical facilities. It may only be necessary to conduct a SVA for those facilities with similar attributes. The SVA is

a secondary evaluation that examines a facility's characteristics and operations to identify potential threats or vulnerabilities and existing and prospective security measures and procedures designed to protect a facility.

An example methodology and criteria for conducting an SVA is identified in Appendix D. Other recognized SVA methodologies may be used and must be documented.

7 Security Plans

7.1 Security Plan Considerations

Security planning starts with sound policy and procedures in place. The facility owner/operator should develop either an owner/operator-wide, multiple-facility or facility-specific security plan. Refer to Appendix C for an example Model Security Plan.

The security plan should include the following elements:

1. The measures being taken to detect or deter an attack or incursion;
2. The responses that may be considered at various security level conditions, including the response to an actual attack, intrusion, or event,
3. Means of mitigating the consequences of an incident, if any, and;
4. If applicable, any additional security measures identified in the SVA described in Section 6.

The plan should be kept confidential for security reasons. The plan should be reevaluated and updated periodically.

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 recommended practice.

7.2 Security Plan Elements

In developing a security plan, the facility owner/operator should consider several basic elements.

This document 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.

7.2.1 Develop Baseline Security Plan

A plan is developed to address awareness, communication and response actions, as applicable to the most significant risks to the facility. The output of the SVA, if conducted, should be included in the formulation of the plan.

Minimum Elements to be considered:

- Management and employee security responsibilities;
- Communications within the company and with relevant governmental authorities;
- Facility access (personnel, goods and equipment);
- Restricted area(s), if applicable;
- Security training and drills;
- Assessment of security drills and exercises;
- Handling security sensitive related information (SSI) and security related communications;
- Audits and inspections;
- Recordkeeping;
- Additional measures as determined by the SVA, if conducted; and
- Coordination with Point of Embarkation.

7.3 Security Levels

Security Levels are defined as the qualification of the degrees of risk that a security incident will be attempted or will occur.

Level 1: The level for which minimum appropriate protective security measures shall be maintained at all times.

Level 2: The level for which appropriate protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

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

7.4 Security Level Actions

Three levels of escalating threat conditions have been defined.

7.4.1 Security Level 1

Applies when there is a minimal risk of threat activity directed toward the offshore oil and gas industry. The owner/operator shall have a baseline security plan and monitoring of intelligence information in place.

1. Security plan reviews and security exercises are conducted periodically.
2. Security Awareness, Personnel Vigilance and Incident Reporting Programs ongoing.
3. Personnel are advised on the relevant security plan.
4. Communicate threat level and specific security information to appropriate personnel.
5. Periodically review the security plan and communication procedures.

Selected measures from higher threat levels may be considered for application on a consistent or random basis. This level should be capable of being maintained indefinitely.

7.4.2 Security Level 2

The owner/operator should coordinate intelligence continuously and directly with relevant agencies. In addition to Security Level 1 measures, the owner/operator should:

1. Communicate threat level and specific security information to appropriate personnel.
2. Initiate/Maintain surveillance of appropriate facilities.
3. Closely monitor access to Restricted Areas.
4. Restrict access to facilities.
5. Consider pre-positioning of additional personnel resources and logistical support.

6. Verify Emergency Plans.

Activation of this level for more than a short period may begin affecting operations.

7.4.3 Security Level 3

In addition to Levels 1 and 2 measures, the owner/operator should:

1. Communicate threat level and specific security information to appropriate personnel.
2. Increasing or redirecting personnel to address the emerging needs.
3. Mobilize emergency response personnel and other emergency resources.
4. Limit access to facilities.
5. Consider curtailing or suspending non-essential operations.

This level can only be maintained for a short period of time.

APPENDIX I—VOLUNTARY COMMUNICATION PROTOCOL

Communication Procedures to Report Suspicious Activity or Terrorist Operations

General Characteristics of Terrorists

Since September 11, 2001, personnel have been increasingly aware of the threat from terrorist activities. The threat includes any boat, ship or facility and highlights the need for all personnel to be aware of their surroundings and to report anything that appears to be unusual or out of place. This document provides guidance regarding the proper authority to report observations of suspicious activities.

Professional and Public Awareness

All personnel (recreational and commercial fishermen, licensed merchant mariners, offshore oil and gas industry personnel and helicopter pilots and passengers) can help protect resources. By being observant and reporting suspicious or unusual activity to proper authorities, you can greatly increase the effectiveness of our law enforcement agencies. When in doubt, make the report. If it is something that looks out of place to you, then it is worthy of evaluation by proper authorities.

Communications to the Proper Authority

The proper authority to receive reports of suspicious/unusual or potential terrorist activity is the appropriate governmental authority. They will immediately notify appropriate law enforcement and intelligence personnel.

Means of Communication

The following communications systems may be used for contact:

✓ *Primary. Cell Phone or Satellite Phone*

✓ *Secondary. Marine radio*

✓ *Other: If you are out of range for your cell phone or radio, you could attempt to contact a manned offshore facility or offshore service or other vessel who should be able to contact the appropriate governmental authority.*

Note: If you are making a report over the radio, there is a good possibility that you will be overheard by other vessels or facilities including the suspect.

Situation Report Format

The following information should be included when making a report.

✓ *Name, address and phone number of reporting source:*

✓ *Time of Activity:*

✓ *Location: of activity (latitude/longitude, GPS coordinates or Platform #)*

✓ *Incident Description: Describe the suspicious/unusual activity with a description of the suspect vessel or facility (name, call sign, physical description, etc.)*

✓ *Additional Information (as applicable)*

APPENDIX II—EXAMPLE SECURITY POLICY

The owner/operator is committed to enhancing security and safety of personnel, offshore facilities, shore-based facilities, and other assets. The owner/operator's fundamental commitments and principles include:

- Establishment of a Security Program that clearly sets forth relevant and practical guidance and protocols, including managerial and field responsibilities.
- Establishment of a Security Program audit process to provide for continuous improvement.
- Participation in regulatory/law enforcement agency dialogue to produce practical and economically feasible security regulations.
- Reporting all required security incidents to appropriate governmental agencies as soon as practical.
- Participation in relevant Industry Association committees and work groups in connection with the development of recognized industry security standards, solutions and recommended practices.
- Communicate with other stakeholders to validate and mutually enhance parties security programs, avoiding redundancies and clearly establishing responsibilities and obligations.
- Initiating a Security Training Program when and where necessary, including provisions for competency validation.
- Dissemination of applicable security warnings and alerts to appropriate personnel and facilities.
- Maintaining confidentiality of security sensitive information.
- Continued use of background investigations, pursuant to applicable rules and requirements during the employment process, including periodic review of the program elements.
- Empowering employees to openly participate in the Security Program, and to assist the owner/operator in its audit and enhancement processes.

The owner/operator recognizes its duties and obligations relative to security and will endeavor to provide all of the resources necessary to meet its commitments. Adherence to the Security Plan and all associated requirements and recommendations is critical.

APPENDIX III—EXAMPLE MODEL SECURITY PLAN

1 Purpose

The purpose of this Security Plan is to enhance security at (owner/operator) facilities for the protection of personnel and other assets.

2 Reference

This Plan has been prepared utilizing the elements specified in API Recommended Practice (RP) 70I.

3 Scope

This plan is intended to provide security guidance and recommended practices for the owner/operator's offshore facilities, such as any artificial island, installation, or other device permanently or temporarily attached to the subsoil or seabed of offshore locations, erected for the purpose of exploring for, developing, or producing resources, or any such installation or other device (other than a ship or vessel) for the purpose of transporting such resources. This plan includes mobile offshore drilling units.

4 Plan Audit and Review Procedures

This plan will be reviewed periodically by the owner/operators circumstances warrant. Revised plans shall be distributed to all relevant locations and personnel.

5 Security Sensitive Information (SSI)

This plan and other security materials shall be treated with the utmost confidentiality. Only personnel with a legitimate need to know shall review this document and associated security materials. Such restrictions are critical in order to enhance security and protect sensitive information. Copies of the Plan and other SSI shall not be distributed to unauthorized personnel, or third parties.

6 Security Levels

Security Levels are defined as the qualification of the degrees of risk that a security incident will be attempted or will occur.

Level 1: The level for which minimum appropriate protective security measures shall be maintained at all times.

Level 2: The level for which appropriate protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

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

7 Definitions

7.1 company security officer (CSO): The CSO is responsible for the maintenance of the Security Plan. The CSO shall have access to relevant security information. The CSO shall determine which information, and by what means, it is communicated. The CSO may delegate duties as necessary to assure timely completion of responsibilities. The CSO may be assigned other duties and responsibilities unrelated to security.

7.2 contractor: The individual, partnership, firm, or corporation that is hired to do a specific job or service, such as a production operator, drilling or well servicing contractor or to provide contract employees to an owner/operator; a contractor is also the individual, partnership, firm, or corporation retained by the owner or operator to perform other work or provide supplies or equipment. The term contractor shall also include subcontractors.

7.3 facility: Any artificial island, installation, or other device permanently or temporarily attached to the subsoil or seabed of offshore locations, erected for the purpose of exploring for, developing, or producing oil, natural gas or mineral resources. This definition includes mobile offshore drilling units (MODUs).

7.4 facility owner/operator: The individual, partnership, firm, or corporation having control or management of offshore operations. The owner/operator may be a lessee, designated agent of the lessee(s), or holder of operating rights under an operating agreement.

7.5 facility security officer (FSO): The individual that is responsible for security duties as specified by the owner/operator at one or more facilities, depending on the number or types of facilities a company operates. Where a person acts as the FSO for more than one facility, it should be clearly identified in the Facility Security Plan for which facilities this person is responsible. The FSO may be a collateral duty provided the person is fully capable to perform the duties and responsibilities required of the FSO.

7.6 point of embarkation: The heliport or dock facility from which personnel and materials are shipped to or received from the offshore facility. Appropriate security measures at these facilities are critical.

8 Company Security Officer (CSO)

The CSO is responsible for the maintenance of the Security Plan. The CSO shall have access relevant security information. The CSO shall determine which information, and by what means, it is communicated. The CSO, in consultation with senior management, may require certain security mea-

sures, including restriction of operations or evacuation. Other CSO responsibilities include coordination with applicable regulatory and law enforcement agencies and managing the security training function, as applicable. Additionally, the CSO may communicate with other entities (contractors, operators, partners, third parties, etc.) as regards a coordinated approach to the Security Plan or a specific security concern. The CSO may delegate duties as necessary to assure timely completion of responsibilities. The CSO may be assigned other duties and responsibilities unrelated to security. If warranted, consideration should be given to assigning an alternate CSO or co-CSO in the event the CSO is unavailable or incapacitated.

CSO Information:
Name:
Office address:
Office Phone:
Home Phone:
Cell Phone:
Pager:
E-mail address(es):
Emergency Contact Information:

Alternate (if appointed):

9 Facility Security Officer (FSO)

The FSO receives information in connection with security-related matters. The FSO may communicate with other security personnel, such as on-site representatives (contractors, operators, partners, third parties, etc.). The FSO or other designated personnel shall be the person(s) in charge of reporting suspicious activities, pursuant to the communications protocol. The duties of the FSO may be delegated to other qualified personnel, but the FSO is ultimately responsible for these duties. A person designated as the FSO may act as the FSO for one or more facilities, depending on the number or types of facilities a company operates. Where a person acts as the FSO for more than one facility, it should be clearly identified in the facility security plan for which facilities this person is responsible. The FSO may be a collateral duty provided the person is fully capable to perform the duties and responsibilities required of the FSO.

The duties and responsibilities of the offshore FSO include, but are not limited to:

1. Implementing and exercising the facility security plan;
2. Recommending and incorporating, as appropriate, modifications to the facility security plan in order to correct deficiencies and, to update the plan to take into account relevant changes to the facility;
3. Enhancing security awareness and vigilance;
4. Ensuring adequate training for personnel responsible for security of the facility;
5. Reporting to the relevant authorities and maintaining records of occurrences, which threaten the security of the facility.

The FSO for this facility is:
Name:
Position:
State room/office:

10 Restricted Areas

After careful consideration owner/operator has determined the following areas are to be considered Restricted Areas. Each area shall have a sign prominently posted that states **"RESTRICTED AREA—NO UNAUTHORIZED PERSONNEL"**.

The Restricted Areas on this facility are:

_____
_____
_____

Only personnel authorized by the FSO may access a Restricted Area.

The Restricted Area(s) shall be secured in a manner to deter unauthorized entry. Only the FSO and his designee may have the means to open the Restricted Area. If a keyed lock is utilized, a spare key should be kept in a locked box, locker or other secure means, accessible solely by the FSO or his/her designee.

11 Coordination with Point of Embarkation

11.1 Offshore Facility Access-Personnel and Equipment

11.2 Authorization for the shipment of personnel, goods and equipment, shall be coordinated with the Point of Embarkation.

11.3 Additionally, the FSO should follow establish procedures, such as:

1. No unauthorized personnel shall be allowed on the facility.
2. The FSO or his designee should consult with the point of embarkation personnel as to authorizing the shipment of personnel, goods and equipment.
3. Imposing heightened security measures in response to identified threats or as advised by competent authority.

12 Owner/operator Policy on Searches and Inspections

All personnel assigned to the facility, including guests and invitees (third parties, etc.) are subject to the Owner/operator's Policy on Searches and Inspections. These inspections may be conducted on the facility or at the Point of Embarkation. Firearms, weapons, explosive materials and other sub-

stances are strictly prohibited. The complete policy is detailed in *insert reference as appropriate*.

13 Specific Security Measures

The following security measures, listed below each Security Level, are generally utilized. Deviations should be expected.

Security Level 1 *Insert company or facility specific actions or reference as appropriate*

Security Level 2 *Insert company or facility specific actions or reference as appropriate*

Security Level 3 *Insert company or facility specific actions or reference as appropriate*

14 Communication Equipment and Requirements

Each facility shall have two means of two-way communication (e.g., radios, cell/satellite phones) between the facility, CSO and regulatory and law enforcement agencies. The communications system shall be utilized for the receipt of threat information and Alert data from the CSO and other means. Additionally, the FSO will utilize the communications means to communicate with the regulatory and law enforcement agencies as regards threats or suspicious activities. Attachment C specifies the commonly accepted protocol. Deviations should be expected.

The Communications System on this facility is:

Types:
License, if applicable:
Call Sign, if applicable:
Phone number, if applicable:
Regulatory/Law Enforcement Contact Numbers:

Facility Security Training and Drills and Assessments

List as Appropriate

15 Coordination with and among other Security Plans

The Facility owner/operator should coordinate all activities with their contractors or operator as applicable in order to provide a clear understanding of responsibilities for operational decision-making and emergency response.

Attachment A: Company Security Policy
Reference or insert as appropriate

Attachment B: Facility Specific Details
Name of facility, if applicable:
Location:
Call Sign, if applicable:
Type of facility:
Maximum number of personnel:
Official Number, if applicable:
Owner and emergency contact:
Operator and emergency contact:

Attachment C: Communication Protocol
Communication Procedures to Report Suspicious Activity or Terrorist Operations
Reference or insert as appropriate

Attachment D: Company Policy on Prohibited Items and Substances-Insert Company-Specific Policy

APPENDIX IV—SECURITY VULNERABILITY ASSESSMENT (SVA)

The following example methodology and criteria for conducting an SVA is one of many methodologies available. Other methodologies and analyses may be used.

Prior to conducting the SVA, the first step should be a characterization of the facility or the group of similar facilities attributes, e.g. the quantity of oil and/or natural gas produced, the number of personnel on board, proximity to shipping lanes, physical access to the facility, and existing security measures and procedures already in place, such as at the Point(s) of Embarkation. Depending on the results of the characterization, a SVA may be warranted.

The SVA process discussed below is a simplified risk based tool. The SVA process should include the following elements:

- Potential threats
- The consequences of an act or attack
- Vulnerability to an act or attack
- Mitigation

Step 1: Potential Threat

To begin an assessment, the owner/operator needs to consider various scenarios that could be a potential threat to the offshore facility. It is important the scenario or scenarios are within the realm of possibility and be consistent with scenarios used to develop the security plan. Both worse case scenarios and most probable scenarios should be considered. Care should be taken to avoid unnecessarily evaluating an excessive number of scenarios that result in low consequences. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences.

The Table 1 shows potential scenarios that could be considered. This list may not be applicable to all facilities and other scenarios may need to be considered.

Step 2: Consequence Assessment

The potential consequence of the act or attack should be evaluated for each scenario being considered. The Table 2 may be used to assign a consequence level based on the potential for death and injury, significant economic impact or significant environmental impact. In assessing the environmental impact, the facility location in relation to sensitive natural resources should be considered.

Table 1—List of Scenarios

Typical Types of Scenarios		Application Example
Externally attack the facility by...	Ramming with a vessel	Intentionally ramming a platform with a boat or marine vessel to either cause pollution or damage the platform
	Underwater attack by submarine, ROV or diver	Damage well or platform risers
	Launching or shooting weapons from a distance	Damage or destroy bulk storage tanks, production vessels
	Moving explosives adjacent to the platform	USS Cole style attack
Intrude and/or take control of facility and...	Damage/destroy the facility with explosives	Intruder boards the facility from a boat and plants explosives
	Open valves/vents	Intruder opens valves or vents causing pollution or a fire
	Disrupts production	Shuts in production or pipeline systems.
	Disrupts drilling operations	Causes well blowout and subsequent pollution and/or fire
	Takes hostages/kills people	Goal of the intruder is to kill people
Use the facility as a means of transferring...	Materials or people into/out of the country	Use the facility as an offshore staging area for transferring materials or personnel between vessels.

Table 2—Consequence Score

Assign a rating of:	If the impact could be
3	**CATASTROPHIC** = numerous loss of life or injuries, major national or long term economic impact, complete destruction of multiple aspects of the eco-system over a large area
2	**SIGNIFICANT** = multiple loss of life or injuries, major regional economic impact, long-term damage to a portion of the eco-system
1	**MODERATE** = minimal loss of life or injuries, minimal economic impact, or some environmental damage

Step 3: Vulnerability Assessment

Each facility owner/operator should evaluate each scenario in terms of the facility's vulnerability to an attack. The initial evaluation of vulnerability should be viewed with only existing strategies and protective measures, designed to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures (mitigations) considered.

Four elements are normally considered in vulnerability: availability, accessibility, organic security, and facility hardness.

Element	Description
Accessibility	Accessibility of the facility to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
Organic Security	The ability of facility personnel to deter the attack. It may include security plans, communication capabilities and plans, intrusion detection systems and point of embarkation plans.

It is recognized that the facility owners/operator has the most control over the organic security element; therefore, the vulnerability assessment should focus on this element.

Table 3 can be used to assign a vulnerability score.

Table 3—Vulnerability Score

Score	Accessibility & Organic Security
1	Good deterrence capability expected to deter attack (e.g., detailed security plan, effective emergency communication systems, excellent restricted access to facility including both personnel and material from point of embarkation and at the facility, proactive personnel reporting of suspicious activities, effective training and drills for personnel, intrusion deterrence measures in place.
2	Fair deterrence capability (e.g., minimal security plan, emergency communication systems, no intrusion detection capability, restricted access to facility from point of embarkation by personnel, but unrestricted access by material, minimal training of personnel on security issues)
3	No deterrence capability (e.g., no security plan, unrestricted access to facility from point of embarkation or between facilities by personnel and equipment, no detection capability, no training or drills on security issues)

Step 4: Mitigation

The facility owner/operator should determine which scenarios should have mitigation strategies (protective measures) implemented. Table 4 is intended as a broad, relative tool to assist in the development of the facility security plan. "Results" are not intended to be the sole basis to trigger or waive the need for specific measures, but are one tool in identifying potential vulnerabilities and evaluating prospective methods to address them.

Table 4—Vulnerability & Consequence Matrix

		Total Vulnerability Score		
		2	3-4	5-6
Consequence Level (Table 2)	3	Consider	Mitigate	Mitigate
	2	Document	Consider	Mitigate
	1	Document	Document	Consider

Notes: "Consider" means that mitigation strategies should be developed on a case-by-case basis.

"Document" means that the scenario may not need a mitigation measure and therefore needs only to be documented.

"Mitigate" means that mitigation strategies, such as security protective measures and/or procedures, should be considered to reduce risk for that scenario.

To assist the facility owner and/or operator in determining which scenarios may require mitigation methods, the facility owner and/or operator may find it beneficial to use Table 5 provided below. The facility owner and/or operator can record the scenarios considered, the consequence score (Table 2), outcome of the each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category Table 4).

Table 5—Mitigation Determination Worksheet

Step 1	Step 2	Step 3			Step 4
		Vulnerability Score (Table 3)			
Scenario/ Description	Consequence Score (Table 2)	Accessibility + Organic = Total Security Score			Mitigation Results (Table 4)

Step 5: Implementation

The facility owner/operator should document the security vulnerability assessment, including the scenarios considered, the consequence level (Table 2), the vulnerability score (Table 3) and the mitigation category (Table 4). The desire is reduce the overall risk associated with the identified scenario. It is generally easier to reduce vulnerabilities than to reduce consequences or threats.

The facility owner/operator should develop practical mitigation strategies for those situations that score a "consider" or "mitigate". Multiple mitigation strategies may need to be considered. A practical mitigation strategy is one in which the facility owner/operator can implement with little operational impact or funding relative to the prospective reduction in vulnerability. Feasibility of a mitigation strategy may vary based on the Security level. Therefore, some strategies may not be warranted at the lower Security levels, but may be at higher Security levels.

The facility owner/operator should develop a process through which overall security is periodically evaluated.

API®

American Petroleum Institute

2004 Publications Order Form

Effective January 1, 2004.
API Members receive a 50% discount where applicable.

The member discount does not apply to purchases made for the purpose of resale or for incorporation into commercial products, training courses, workshops, or other commercial enterprises.

Available through Global Engineering Documents:

Phone Orders: **1-800-854-7179** (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: **303-397-2740**
Online Orders: **www.global.ihs.com**

Date: _____ ❑ **API Member** (Check if Yes)

Invoice To (❑ Check here if same as "Ship To")

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
E-Mail:

Ship To (UPS will not deliver to a P.O. Box)

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
E-Mail:

Quantity	Product Number	Title	SO★	Unit Price	Total
	G07001	RP 70, Security for Offshore Oil and Natural Gas Operaions		$42.00	
	G74001	RP 74, Occupational Safety for Onshore Oil and Gas Production Operations		$46.00	
	G07503	RP 75, Development for a Safety and Environmental Mgt. Program for Outer Continental Shelf Operations and Facilities		TBD	
	G07601	RP 76, Contractor Safety Mgt. for Oil and Gas Drilling and Production Operations		$60.00	
	G54003	RP 54, Occupational Safety for Oil and Gas Well Drilling and Servicing Operations		$98.00	

❑ **Payment Enclosed** ❑ **P.O. No.** (Enclose Copy) _____

❑ **Charge My Global Account No.** _____

❑ **VISA** ❑ **MasterCard** ❑ **American Express** ❑ **Diners Club** ❑ **Discover**

Credit Card No.:
Print Name (As It Appears on Card):
Expiration Date:
Signature:

Subtotal
Applicable Sales Tax *(see below)*
Rush Shipping Fee *(see below)*
Shipping and Handling *(see below)*
Total *(in U.S. Dollars)*

★ ***To be placed on Standing Order for future editions of this publication, place a check mark in the SO column and sign here:***

Pricing and availability subject to change without notice.

Mail Orders – Payment by check or money order in U.S. dollars is required except for established accounts. State and local taxes, $10 processing fee*, and 5% shipping must be added. Send mail orders to: **API Publications, Global Engineering Documents, 15 Inverness Way East, M/S C303B, Englewood, CO 80112-5776, USA.**
Purchase Orders – Purchase orders are accepted from established accounts. Invoice will include actual freight cost, a $10 processing fee*, plus state and local taxes.
Telephone Orders – If ordering by telephone, a $10 processing fee* and actual freight costs will be added to the order.
Sales Tax – All U.S. purchases must include applicable state and local sales tax. Customers claiming tax-exempt status must provide Global with a copy of their exemption certificate.
Shipping (U.S. Orders) – Orders shipped within the U.S. are sent via traceable means. Most orders are shipped the same day. Subscription updates are sent by First-Class Mail. Other options, including next-day service, air service, and fax transmission are available at additional cost. Call 1-800-854-7179 for more information.
Shipping (International Orders) – Standard international shipping is by air express courier service. Subscription updates are sent by World Mail. Normal delivery is 3-4 days from shipping date.
Rush Shipping Fee – Next Day Delivery orders charge is $20 in addition to the carrier charges. Next Day Delivery orders must be placed by 2:00 p.m. MST to ensure overnight delivery.
Returns – All returns must be pre-approved by calling Global's Customer Service Department at 1-800-624-3974 for information and assistance. There may be a 15% restocking fee. Special order items, electronic documents, and age-dated materials are non-returnable.
***Minimum Order –** There is a $50 minimum for all orders containing hardcopy documents. The $50 minimum applies to the order subtotal including the $10 processing fee, excluding any applicable taxes and freight charges. If the total cost of the documents on the order plus the $10 processing fee is less than $50, the processing fee will be increased to bring the order amount up to the $50 minimum. This processing fee will be applied before any applicable deposit account, quantity or member discounts have been applied. There is no minimum for orders containing only electronically delivered documents.

There's more where this came from.

The American Petroleum Institute provides additional resources and programs to the oil and natural gas industry which are based on API® Standards. For more information, contact:

• API Monogram® Licensing Program	Phone: 202-962-4791 Fax: 202-682-8070
• American Petroleum Institute Quality Registrar (APIQR®)	Phone: 202-962-4791 Fax: 202-682-8070
• API Spec Q1® Registration	Phone: 202-962-4791 Fax: 202-682-8070
• API Perforator Design Registration	Phone: 202-962-4791 Fax: 202-682-8070
• API Training Provider Certification Program	Phone: 202-682-8490 Fax: 202-682-8070
• Individual Certification Programs	Phone: 202-682-8064 Fax: 202-682-8348
• Engine Oil Licensing and Certification System (EOLCS)	Phone: 202-682-8516 Fax: 202-962-4739
• API PetroTEAM™ (Training, Education and Meetings)	Phone: 202-682-8195 Fax: 202-682-8222

Check out the API Publications, Programs, and Services Catalog online at www.api.org.

API®
American Petroleum Institute

Helping You Get The Job Done Right.®

Additional copies are available through Global Engineering Documents at (800) 854-7179 or (303) 397-7956

Information about API Publications, Programs and Services is available on the World Wide Web at: http://www.api.org

American Petroleum Institute

1220 L Street, Northwest
Washington, D.C. 20005-4070
202-682-8000

Product No. G70I01