

Facility Security Plan Methodology for the Oil and Natural Gas Industries

API RECOMMENDED PRACTICE 781
FIRST EDITION, SEPTEMBER 2016



AMERICAN PETROLEUM INSTITUTE

Special Notes

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

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

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 authorities having jurisdiction with which this publication may conflict.

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

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

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

Copyright © 2016 American Petroleum Institute

Foreword

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

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

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, NW, Washington, DC 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

	Page
1 Scope	1
1.1 General	1
1.2 Applicability	1
2 Normative References	1
3 Terms, Definitions, Abbreviations, and Acronyms	2
3.1 Terms and Definitions	2
3.2 Abbreviations and Acronyms	7
4 Security Management System (SMS)	8
5 Security Risk Assessment (SRA)	8
6 Introduction to Facility Security Plan Concepts (FSP)	9
6.1 Introduction	9
6.2 Common elements included in an FSP	9
6.3 Record of Change	9
6.4 Distribution List	10
6.5 Security Administration and Organization of the Facility	11
6.6 Security Training	13
6.7 Drills and Exercises	15
6.8 Record Keeping and Documentation	16
6.9 Response to Change in Alert Level	17
6.10 Communications	18
6.11 Site Maps	19
6.12 Network Segmentation	19
6.13 Security Systems and Equipment Maintenance	20
6.14 Physical Security	20
7 Futures—Additional Integration of Cyber and Physical Systems	22
8 Personnel Surety	22
8.1 General	22
8.2 Background Check	23
8.3 Employees	23
8.4 Contractors	23
8.5 Audit of Personnel Surety Program	24
9 Security Measures for Access Control, Including Designated Public, Controlled, and Restricted Access Areas²⁴	24
9.1 General	24
9.2 Visitors	25
9.3 Deliveries	25
9.4 Government Employees	25
9.5 Screening, Searches, and Inspection	26
9.6 Restricted Areas	27
9.7 Security Countermeasures for Restricted Areas	27
10 Security Measures for Monitoring	28
11 Key Control	29
12 Security Incident Procedures	29

Contents

	Page
13 Audits and Security Plan Amendments	30
13.1 Audits	30
13.2 Audit Amendments	30
13.3 Findings	30
Annex A (informative) Example Security Plan	31
Bibliography	70
Tables	
1 Example Elements of a Security Plan	10
2 Record of Change	10

Facility Security Plan Methodology for the Oil and Natural Gas Industries

1 Scope

1.1 General

The purpose of a facility security plan (FSP) is to provide the framework to establish a secure workplace. The plan provides an overview of the threats facing the facility and describes the security measures and procedures designed to mitigate risk and protect people, assets, operations, and company reputation.

This standard was prepared with guidance and direction from the API Security Committee, to assist the petroleum and petrochemical industries in the preparation of a Facility Security Plan. This standard specifies the requirements for preparing an FSP as well as a discussion of the typical elements included in an FSP.

1.2 Applicability

This standard is intended to be flexible and adaptable to the needs of the user. It is noted that the content of an FSP can vary depending on circumstances such as facility size, location, and operations. This methodology is one approach for preparing an FSP at petroleum and petrochemical facilities. There are other security plan formats available for the industry. It is the responsibility of the user to choose the format and content of the FSP that best meets the needs of a specific facility. The format and content of some FSPs should be dictated by government regulations for covered facilities. This Standard is not intended to supersede the requirements of any regulated facility but may be used as a reference document.

This standard should be limited to the preparation of the FSP. It is recognized that the FSP is only one part of a comprehensive security management system (SMS). The FSP should be prepared after a security risk assessment (SRA) is conducted. The SRA is a process to identify and assess the threats, vulnerabilities and consequences facing a facility. It is important to understand the risks facing the facility before a comprehensive and effective FSP can be developed. The FSP should incorporate procedural, physical and cyber security measures for a holistic and comprehensive plan.

In an era of rapidly advancing technology, no FSP would be complete without inclusion of Information Technology and Operational Technology Security considerations and reference to security measures developed and maintained by these organizations. The interdependence of physical and logical security, as evidenced by the “Internet of Things” (IoT) underscores the criticality of preparing a single, common security strategy to mitigate risk and assure an organization’s resilience in the face of dynamic threats.

2 Normative References

The most recent editions of each of the following standards, codes, and publications are referenced in this RP as useful sources of additional information. Further information may be available from the cited Internet World Wide Web sites or references included in the Bibliography.

API Manual of Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

6 CFR §27.230 ¹, *Chemical Facilities Anti-Terrorism Standards, Risk-Based Performance Standards*

33 CFR §105.100–415 ², *Maritime Transportation Security Act of 2002*

National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity ³

¹ Department of Homeland Security-ISCD, 1421 Jefferson Davis Highway, Arlington, VA 22202.

² U. S. Coast Guard, 2699 Firth Sterling Ave SE, Washington, D.C., www.gocostguard.com.

³ National Institute of Standards and Technology, 100 Bureau Drive, Stop 3460, Gaithersburg, Maryland 20899, www.nist.gov.

3 Terms, Definitions, Abbreviations, and Acronyms

3.1 Terms and Definitions

For the purposes of this document, the following definitions apply.

3.1.1

21st Century Security Strategy

The combined physical and logical/cyber governance strategies (principles, policies and controls) designed to safeguard the organization's assets, including its workforce, facilities, operations, equipment, technology, systems, communications, and information against threats and potential security events and to comply with regulatory frameworks.

3.1.2

asset

Any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to a threat, as well as an owner, although the nature and magnitude of those values may differ.

3.1.3

asset category

Assets may be categorized in many ways such as:

- a) people,
- b) hazardous materials (used or produced),
- c) information,
- d) environment,
- e) equipment,
- f) facilities,
- g) activities/operations, and
- h) company reputation.

3.1.4

attractiveness

An estimate of the value of a target to a threat. Consideration shall be given to the following factors in defining the threat and in determining the need for any enhanced countermeasures:

- a) potential for mass casualties/fatalities;
- b) extensive property damage;
- c) proximity to national assets or landmarks;
- d) possible disruption or damage to critical infrastructure;
- e) disruption of the national, regional, or local economy;
- f) ease of access to target;
- g) media attention or possible interest of the media;
- h) company reputation and brand exposure;
- i) the presence of on-site materials that can be used as a chemical or biological weapon (or precursor materials that can be used to develop chemical or biological weapons).

3.1.5**audit**

An evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party that is intended to identify deficiencies, non-conformities, and inadequacies that would render the assessment or plan insufficient.

3.1.6**baseline risk**

The normal operating condition level of risk that takes into account existing risk mitigation measures.

3.1.7**breach of security**

An incident that has not resulted in security incident, in which security measures have been circumvented, eluded, or violated.

3.1.8**capability**

The potential to accomplish a mission, function, or objective.

3.1.9**consequence**

The potential outcome of an event. A consequence is commonly measured in four ways: human, economic, mission, and psychological. A consequence may also include other factors such as impact on the environment.

3.1.10**countermeasures**

Actions, measures, or devices intended to reduce an identified risk.

3.1.11**critically**

Importance to a mission or function, or continuity of operations.

3.1.12**cyber security**

The process of protecting information by preventing, detecting, and responding to attacks.

3.1.13**dangerous substances or devices**

Any material, substance, or item that reasonably has the potential to cause a security incident.

3.1.14**delay**

To slow the progression of an intentional act.

3.1.15**detect/detection**

The strategy to identify a threat attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the threat.

3.1.16**deter/deterrence**

A countermeasure strategy that is intended to prevent or discourage the occurrence of a breach of security or a security incident.

3.1.17**disparate impact liability**

Arises if an employer uniformly administers a criminal background check that disproportionately excludes people of a particular race, national origin, or other protected characteristic, and is not “job related for the position(s) in question and consistent with business necessity.”

3.1.18**disparate treatment**

Intentional discrimination in employment if a covered employer uses criminal history information differently based on an applicant's or employee's race, national origin, or other protected trait.

3.1.19**escorting**

Ensuring the continuous monitoring through accompaniment or technical means, such as CCTV, in a manner sufficient to observe if the individual is engaged in unauthorized activities.

3.1.20**facility security officer****FSO**

The person designated as responsible for the development, implementation, revision and maintenance of the facility security plan.

3.1.21**facility security plan****FSP**

The document developed to ensure the application of security measures.

3.1.22**intelligence**

Information to characterize specific or general threats when considering a threat's motivation, capabilities, and activities.

3.1.23**intent**

A state of mind or desire to achieve an objective.

3.1.24**Internet of things****IoT**

For purposes of this guideline, IoT means a peer-to-peer network of objects and things that can be sensed, controlled, and programmed, where everything is networked and capable of communicating to each other.

3.1.25**layers of protection****concentric “rings of protection”**

A concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as counter surveillance, counterintelligence, physical security, and cyber security. A second consideration is the balance of the security measures such that equivalent risk exists regardless of the threat's pathway or method.

3.1.26**likelihood**

The chance of something happening, whether defined, measured, or estimated objectively or subjectively or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities.



3.1.27**mitigation**

The ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.

3.1.28**owner/operator**

Means any person or entity that owns or maintains operational control over any facility.

3.1.29**recovery**

The ability of a site to withstand and execute service and site restoration plans for affected assets and the reconstitution of operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

3.1.30**resilience**

The ability to adapt to changing conditions and prepare for, withstand and rapidly recover from disruption.

3.1.31**respond/response**

The act of reacting to detected or actual security incidents either immediately following detection or post incident.

3.1.32**restricted areas**

Locations that require limited access and a higher degree of security protection in accordance with the security plan. The entire facility may be designated the restricted area, as long as the entire facility is provided the appropriate level of security.

3.1.33**risk**

The potential for damage to or loss of an asset.

3.1.34**risk analysis**

The systematic examination of the components and characteristics of risk.

3.1.35**risk assessment**

The process of determining the likelihood of a threat successfully exploiting vulnerability and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for rank ordering of risks and thus establishing priorities for the application of countermeasures.

3.1.36**risk management**

The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

3.1.37**safeguard**

Device, system, or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.

3.1.38**screening**

A reasonable examination of persons, cargo, vehicles, or personal effects.

3.1.39**secure area**

The area over which the owner/operator has implemented security measures for access control in accordance with the security plan.

3.1.40**security incident**

A security event which may compromise an asset and require action.

3.1.41**security risk assessment****SRA**

An assessment for the purposes of determining security risk.

3.1.42**security sweep**

A walkthrough to visually inspect the facility to identify unattended packages, briefcases, luggage, unauthorized persons, or other security breaches and determine that all restricted areas are secure.

3.1.43**security system**

A device or multiple devices designed, installed and operated to monitor, detect, observe, or communicate about activity that may pose a security threat.

3.1.44**target**

An asset, network, system, or geographic area chosen by a threat to be impacted by an attack.

3.1.45**technical security systems**

Technical systems may include electronic systems for increased protection or for other security purposes which may include access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

3.1.46**terrorism**

The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

3.1.47**threat**

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

3.1.48**threat assessment**

A product or process of identifying or evaluating entities, actions, or occurrences that has or has indicated the potential to harm life, information, operations, or property.

3.1.49**threat categories**

Consist of three general areas from which threats or adversaries can be categorized such as:

- a) internal threats,
- b) external threat, and
- c) Internal threats working in collusion with external threats.

3.1.50**undesirable event**

An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

3.1.51**unescorted access**

Having the authority to enter and move about a secure area without escort.

3.1.52**vulnerability**

A weakness that can be exploited by a threat to gain access to an asset.

3.1.53**vulnerability assessment**

A product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to hazards.

3.2 Abbreviations and Acronyms

ACC	American Chemistry Council
ACP	Access Control Point
AFSO	Alternate Facility Security Officer
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
CERT	Corporate Emergency Response Team
CPL	Critical Patrol Log
CCPS	Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE)
CCTV	Closed Circuit Television
CFATS	Chemical Facility Anti-Terrorism Security 6 <i>CFR</i> Part 27
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	U. S. Department of Transportation
EPA	U. S. Environmental Protection Agency
FBI	U. S. Federal Bureau of Investigation
FSO	Facility Security Officer
FSP	Facility Security Plan
HSAS	Homeland Security Advisory System
IoT	Internet of Things
IT	Information Technology

MOC	Management of Change
MTSA	Maritime Transportation Security Act
NIPP	National Infrastructure Protection Plan
RP	Recommended Practice
SMS	Security Management System
SRA	Security Risk Assessment
TSA	Transportation Security Agency
USCG	United States Coast Guard

4 Security Management System (SMS)

The SMS within an organization provides the strategic foundation for managing risk throughout the organization. The SMS empowers the organization to develop policies, establish security objectives, and identify processes to support their effectiveness for minimizing the consequences of a security incident. Key to the success of the SMS is a security policy establishing management's support and commitment to security. The SMS shall be approved and endorsed at the highest levels of executive management. Management's commitment to the SMS should be communicated throughout the organization.

The various elements of the SMS are designed to address the security needs of the organization. Two critical components of the SMS are the SRA and the development of a sound FSP. The elements of the FSP should be flexible within the organization since the threats and appropriate countermeasures should vary depending on the facility's location, size, vulnerabilities and characteristics. The various elements allow each facility to customize and structure an FSP in a manner that addresses the specific risks the facility faces and, at the same time, provides uniformity within the corporation by complying with the elements of the corporate SMS.

5 Security Risk Assessment (SRA)

Risk assessment is an important part of the SMS and the development of an FSP. To develop a rational security plan, a facility must identify critical assets that are at risk, understand the threats impacting these assets, vulnerabilities of the assets, and the potential consequences of a successful attack.

Although threat and risk are often used interchangeably, there is a distinct difference that should be understood.

- a) Risk is used to express the potential for damage to or loss of an asset. Risk, in the context of security, is the potential for a negative outcome whose severity is determined by the likelihood of occurrence and the extent of the consequences.
- b) Threat is used to describe any indication, circumstance, or event that has the potential to cause the loss of or damage to an asset. Threat can also be used to describe the capacity and intent of an adversary to undertake actions that would be detrimental to critical assets. Threat encompasses any individual, group, organization, or government that conducts activities or has the intention and capacity to conduct activities detrimental to critical assets. A threat could include the intelligence service of host nations, third party nations, political and terrorist groups, criminals, disgruntled employees, activists, cyber criminals and private interests. The threat may be internal, external, or internal threats working in collusion with external threats.

The objective of the SRA is to analyze the threats, vulnerabilities, and consequences facing the facility to help management understand the risk and make better informed decisions while considering and selecting cost effective countermeasures. The facility may limit the SRA to terrorism and other security related incidents—such as criminal activity, disgruntled employees, and environmental activists—or may take an all hazards approach and include natural disasters such as hurricanes or floods. This decision should be made after careful consideration of the threats the facility might encounter.

The SRA is a decision tool to identify the facility's vulnerabilities, evaluate the likelihood of an incident and its consequences. This analysis should help the facility identify and prioritize threats based on various factors—including the adversaries' capability, intent, and impact of a successful attack—and then allocate scarce security resources accordingly.

To be effective, the SRA should be considered a dynamic process where the threats are continuously evaluated for change. The SRA process should be revisited at a frequency determined by management in order to maintain the currency of the SRA through monitoring and review. For a detailed discussion of the SRA process refer to ANSI/API 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*, 2013.

6 Introduction to Facility Security Plan Concepts (FSP)

6.1 Introduction

Security addresses a number of key elements related to an organization's security policies, practices, and procedures as well as describing the physical and cyber security features being employed to protect the facility. The elements of the FSP should be selected to address the threats and vulnerabilities identified in the SRA. The organization of this standard is intended to loosely follow the structure set forth in the Chemical Facility Anti-Terrorism Standards (CFATS) and the Maritime Transportation Security Act (MTSA) regulations. It is not intended to supplant the requirements of the regulations but to incorporate rational security measures and to provide guidance for unregulated facilities.

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

The plan and concepts within the plan must comply with federal state and local regulations. The plan, as well as changes and updates, should be reviewed and evaluated by the company's legal advisor. The facility security officer, in conjunction with legal counsel, should ensure that the plan is periodically evaluated to ensure that it continues to meet regulatory standards. During the daily implementation of the plan, legal counsel should be consulted for advice on sensitive individual acts such as search and seizure issues. Legal counsel should also be advised and consulted during any government inspection or visit.

Distribution of FSP shall be restricted to personnel that have a need to know the information in the FSP for purposes of implementing or assessing the security plan for the facility. The facility's information protection policy shall be covered in security training sessions. The FSP shall contain a warning that the information is sensitive and must be protected.

6.2 Common elements included in an FSP

In general, the security plan should be customized to support each owner/operator's unique needs of the facility. Table 1 is an example of certain key elements that may be considered as part of a security plan. The list is not all inclusive and additional elements may be added by the owner/operator to address a particular issue. Additionally, not all of the items listed in Table 1 may be necessary at a particular location. It is up to the facility to determine its security needs based on a sound security risk assessment. If however, a facility elects to include an element, they shall comply with the requirements of that element.

Some facilities, subject to government regulation, may use this Standard as a reference document but shall follow the form and format in the regulation, if specified.

Table 1—Example Elements of a Security Plan

a) Record of Change
b) Distribution List
c) Security Administration and Organization
d) Site Maps
e) Security Training
f) Drills and Exercises
g) Records and Documentation
h) Response to Change in Alert Level
i) Communications
j) Network Segmentation
k) Security Systems & Equipment Maintenance
l) Physical Security
m) Futures Additional Integration of Cyber and Physical Systems
n) Personnel Surety
o) Security Measures for Protected/ Controlled/Restricted Areas
p) Security Measures for Monitoring
q) Key Control
r) Security Incident Procedures
s) Audits & Security Plan Amendments

6.3 Record of Change

The FSP shall include a record of change to document any updates or changes to the plan. The record of change may include the revision number, date, the pages or sections replaced, the document owner, and identify who made the replacement. The record of change should validate that the FSP is up to date and current. See Table 2 for an example of the record of change.

Table 2—Record of Change

REV #	DATE	Replaces Pages/Section	Document Owner ^a	Replacement Made By
Initial Issue	6/4/14	Initial Issue	John Wayne	Initial Issue
1	9/1/14	Section XX pages XX–XX	John Wayne	Should Smith
^a The document owner shall ensure that all relevant changes and updates to the FSP are completed and documented above to demonstrate the plan is current.				

6.4 Distribution List

The security plan contains confidential information and is classified “Business Confidential” in accordance with the company’s information security policies. Distribution of the FSP shall be restricted to those with a “need to know” as shown on the distribution list. The master list is maintained by the FSO. The FSP shall be secured and kept in locked file cabinets or other secured containers. To better track copies of the FSP, each copy of the FSP should be numbered and assigned to the recipient.

6.5 Security Administration and Organization of the Facility

6.5.1 General

This section of the security plan shall describe how security is managed at the facility and identify personnel and groups with security roles and list their responsibilities. All persons listed in this section shall be identified by name, title, and 24 hour contact information.

In this procedure, the term “Facility Management” indicates the facility manager or a person operating as his designated replacement. Also, for issues related to security, the facility security officer (FSO) may be authorized to act on behalf of the facility manager.

The structure and size of the security group may vary depending on the size and complexity of the facility. At a minimum, the facility shall consider the positions listed in 6.5.3. In some facilities, the positions may be full-time positions; however, the positions in less complex facilities may be part-time duties.

6.5.2 Site Maps

Site maps of the facility containing detailed schematics showing the layout of the facility should be included as an Annex in the FSP. The schematics should also identify and clearly mark the following:

- a) public areas, secure areas and restricted areas;
- b) guard post locations;
- c) perimeter fencing;
- d) vehicle gates;
- e) pedestrian gates;
- f) cameras;
- g) parking areas;
- h) muster points; and
- i) operating units, buildings and other assets.

6.5.3 Facility Personnel

The FSP should identify personnel and groups providing security at the facility including their name, title, 24-hour contact information and clearly summarize their duties.

- a) *Owner/Operator*—The owner/operator shall define the security organization in writing and may delegate roles and responsibilities. The owner/operator shall provide each person exercising security duties and responsibilities within this structure the support needed to fulfill those obligations.
- b) *Facility Manager*—Security of the facility is a line item responsibility and rests with the facility manager who should have the overall responsibility for security at the facility.
 - 1) The facility manager should ensure the cooperation of facility personnel with the FSP.
 - 2) The facility manager should ensure that each person exercising security duties and responsibilities within the facility has the support needed to fulfill those obligations and that security receives adequate resources and management support.
- c) *Facility Security Officer*—The FSO shall have the overall responsibility for managing the day-to-day security of the facility. The FSO's responsibilities may include the following:
 - 1) ensures that security risk assessments are conducted at regular intervals and recommendations are addressed and resolved in as appropriate;
 - 2) prepares and updates the FSP;
 - 3) conducts and documents internal security audits on a regular basis;
 - 4) develops security training for all employees based on their security responsibilities and documents the training;
 - 5) develops and conducts drills and exercise and documents the results;
 - 6) maintains liaison and develops relationships with local law enforcement and first responders;
 - 7) is cognizant of current security threats and ensures that security measures in place are adequate to address the risk;
 - 8) documents and communicates changes in threat level or security procedures to all employees;
 - 9) responds to and documents security incidents;
 - 10) ensures that security equipment is properly maintained, calibrated, tested and the results are documented;
 - 11) develops and maintains a system of records as outlined above.
- d) *Alternate Facility Security Officer*—The facility should designate at least one alternate facility security officer (AFSO) who is responsible for managing the security of the facility in the absence of the primary FSO.
- e) *Legal Advisor*—The facility legal advisor will provide guidance to ensure that the plan complies with federal, state, and local security regulations and will be available for consultation on sensitive individual acts within the plan such as search and seizure issues. The Legal Advisor should be advised of any government inspection or visit. The legal advisor may review or provide guidance on security training issues to ensure that it is legally sufficient, especially in regulated facilities.

- f) *Cyber Security Officer*—The cyber security officer is responsible for cyber security issues at the facility. The interrelationship between physical security and cyber security is such that the cyber security officer and the FSO should work together on the FSP to secure the facility's assets including cyber assets.

Cyber events have the capacity to span physical locations. External attacks, as an example, may traverse Internet egress points which are likely to exist within corporate data centers rather than in a facility or field location. A facility would have no means to terminate such access and consequently, there is a need of coordination with corporate information technology (IT) to address a cyber-event.

- g) *Contract Guard Force* (If applicable)—The FSP shall identify the following.

- 1) The number, location, and type of guard posts (e.g. fixed or mobile patrol) in the FSP. The telephone numbers of guard Post so equipped, shall also be listed in the FSP.
- 2) Document security roles, also known as post orders, performed by contract security guards.
- 3) The name, title and, 24 hour contact information of the site supervisor for the contract security force.

6.5.4 Corporate Office

The facility should consider the role, if any, of personnel from the corporate office in a security incident at the facility and identify them by name, title, 24-hour contact information and clearly summarize their duties.

- a) *Corporate Security Representative*—The organization may appoint a corporate security representative to assist the FSO and coordinate security throughout the organization. The corporate security representative may provide oversight of regulatory requirements and provide guidance and assistance to facilities in implementing security throughout the organization.
- b) *Corporate Cybersecurity Representative*—Unlike physical incidents, cyber events may reach outside of the boundaries of the local site and require a coordinated corporate response rather than an individual facility response.
- c) *Other Corporate Personnel*—Identify corporate employees by title with security roles and a description of responsibilities including functional oversight.

6.5.5 Outside Resources

If releases, fires, or injuries occur from a security-related event, additional notification or a response from outside agencies may be required. Please refer to the appropriate facility emergency plan for guidance. The following agencies should be identified and listed in the FSP together with both their emergency and non-emergency contact numbers:

- a) nation, federal and local police departments;
- b) fire department;
- c) other government and regulatory agencies as required.

6.6 Security Training

6.6.1 General

All personnel entering the facility shall receive some level of safety and security training before they are allowed to enter the facility. This section of the FSP should describe the level and frequency of the training. The training may be

a brief security awareness overview for the casual visitor or a more formalized in-depth program for employees with security responsibilities. The level and frequency of training should be proportionate to the individual's security responsibilities and the risk profile of the facility. The legal advisor may review or provide guidance on security training issues to ensure that it is legally sufficient, especially in a regulated facility.

Security awareness training shall be provided through initial briefings upon hiring or arrival at the facility. The facility should consider annual refresher training to all personnel and interim briefings or security advisories as they are received.

Proper training provides security awareness and enables personnel to be better prepared to identify and report suspicious behavior along with unauthorized attempts to enter the facility or other suspicious acts. Well-trained personnel should be more effective at detecting potential security breaches and should provide an increased measure of deterrence against unauthorized activity.

The training program can validate security plans, policies, and procedures or identify weaknesses and areas for improvement. Training also ensures that personnel are familiar with alert notifications, response requirements, and other security procedures that would be implemented during an incident.

The facility should consider including a cyber-security training program to ensure that all personnel are aware that cyber systems are vulnerable to exploitation and they understand their role in keeping the cyber system secure. Employees should receive training in the following basic topics:

- a) general company cyber policy review,
- b) individual roles and responsibilities,
- c) password procedures,
- d) acceptable practices,
- e) where and how to report suspected inappropriate or suspicious behavior.

6.6.2 Facility Security Officer, the Assistant Facility Security Officer, and Other Security Personnel

The FSO and the AFSSO are charged with the overall security of the facility and require the highest level of training. They shall receive in-depth training on the facility security plan and should include the facility's security objectives, security procedures, employee responsibilities and actions to take in the event of a security breach. In addition, they shall have knowledge, through training or equivalent experience in the following areas as appropriate:

- a) prevention and detection of criminal activities;
- b) reporting of threats or actual criminal and terrorist activity;
- c) operations of communications systems;
- d) procedures for notifying all facility personnel when higher security levels are imposed;
- e) security laws and regulations;
- f) current physical and cyber security threats;
- g) recognition and detection of dangerous substances and devices;
- h) recognition of characteristics and behavior patterns of persons who are likely to threaten security;

- i) techniques used to circumvent security measures;
- j) security-related communications;
- k) crowd and traffic management and control techniques;
- l) knowledge of emergency procedures and contingency plans;
- m) operation of security equipment and systems;
- n) testing, calibration, and maintenance of security equipment and systems;
- o) inspections, control, and monitoring techniques;
- p) knowledge and understanding of the Facility Security Plan;
- q) methods of screening persons, personal effects, and vehicles;
- r) other topics are also chosen based on criteria as the unique security characteristics of the facility, likely threats to the site, the introduction new security equipment the introduction of new security procedures, and other topics deemed important by the FSO; and
- s) all security training should encourage personnel to remain vigilant during their time at the facility and to promptly report suspicious activity.

6.6.3 Security Training for All Other Facility Personnel

All other facility personnel, including contractors, whether part-time, full-time, or temporary shall have knowledge of, through training or equivalent job experience in the following areas, as appropriate:

- a) relevant provisions of the facility security plan;
- b) recognition and detection of dangerous substances and devices;
- c) recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and
- d) techniques used to circumvent security measures.

6.6.4 Testing

The facility may require employees and contractors to periodically demonstrate the correct operation of all equipment, procedures, processes, and systems that they are responsible for to ensure that they are competent to properly respond to a security incident.

6.6.5 Visitors

Visitors should receive a brief security awareness overview of current security matters sufficient to enable them to identify and report suspicious behavior. The briefing should include the current threat level and other security issues as appropriate.

6.6.6 Frequency of Training

The facility shall conduct security training on a regular basis. Employees and contractors with security related positions shall receive more in depth training on a more frequent basis than employees and contractors without

security responsibilities. The level of training shall be commensurate with the employee's security responsibilities and clearance.

A facility may choose to provide initial classroom-based security training for personnel with security duties and annual refresher training via computer-based modules. A facility may provide an annual general security awareness computer-based module for general employees as well.

6.7 Drills and Exercises

6.7.1 General

Drills and exercises shall be designed and conducted to test the security plan and procedures that support the security plan to ensure the proficiency of facility personnel implementing elements of the plan. Drills and exercises should be designed to test facility personnel duties at all security condition levels. Evaluation of the drills and exercises should enable the FSO to identify security deficiencies, weaknesses, and vulnerabilities that need to be addressed.

Drills and exercises should not only test physical security countermeasures at the facility, but should also test cyber security measures. Cyber drills and exercises may require help and collaboration from the IT security group.

Security drills and exercises may be combined with other facility exercises involving environmental, health, or safety events (e.g. spill or release response drills). Many of these activities have a security component and may share the same goals, on-site personnel and off-site responders.

Each facility should use this section to document the number of drills and exercises to be conducted and their frequency. Often, the number and frequency of drills and exercises should be driven by the security risk analysis and risk profile of the facility. The facility should consider conducting one drill per quarter and one exercise per year.

6.7.2 Drills

The FSO shall ensure that drills are conducted on a regular basis, according to the frequency established in the FSP or required by regulation. Drills should be designed to test a single element of the FSP, tailoring the scenarios, to take into account the facility's operations, changes in facility personnel, new equipment or processes and other relevant circumstances. Over time the drills should test every major component in the FSP.

The facility may also choose to use a real-world event (e.g. a breach of security) as a drill that can be documented to capture deficiencies, recommendations or lessons-learned to improve security performance however this shall not be used to replace all drills scheduled during the period.

6.7.3 Exercises

The FSO shall ensure that exercises are conducted on a regular basis, according to the frequency established in the FSP or required by regulation. Exercises provide a more comprehensive test of the plan and should often involve multiple groups and off-site responders. The exercise should be a realistic emergency scenario that should test the response of individuals and organizations to the simulated emergency. Scenarios should be designed to evaluate preparedness, improve response capability, test and validate plans, policies, procedures, and systems; as the scenarios should determine the effectiveness of the command, control and communication function as well.

6.7.4 Joint Training Initiatives

Joint training initiatives involve the participation of outside agencies or organizations' such as law enforcement and first responders—participating in the exercise or drill. The FSO should develop relationships with these organizations and encourage them to periodically participate in the security drill or exercise.

6.8 Record Keeping and Documentation

This section of the security plan shall describe the security-related records that should be created and stored. The records may be created in the either written or electronic form. The FSP and all documentation related to the security of the facility shall be classified and protected from unauthorized disclosure in accordance with the facility's information protection policy. To the extent possible, existing facility record keeping systems may be utilized to avoid duplication and overlap. Before an existing system is selected and used, however, the system administrator shall assure the FSO that access to the records can be restricted to authorized personnel and protected from unauthorized disclosure. The records shall be retained in accordance with the facility's record retention policy unless superseded by regulations.

The facility shall maintain the records listed below. This list is not all inclusive and the facility may identify additional categories.

- a) *Security Training*—The facility shall record the date and location of each training session, the topics discussed, the instructor and his qualifications, the duration, the attendees and the results of any evaluation or testing.
- b) *Drills and Exercises*—Documentation shall be maintained for each drill and exercise conducted. Documentation shall include a description of the drill or exercise, the date of the event and any deficiencies to be corrected, other recommendations to be addressed, or lessons learned. Based on the results and recommendations of the drills and exercises, the facility's security plan shall be revised as necessary.
- c) *Suspicious Activity and Security Breaches*—All suspicious activity and security breaches shall be investigated and recorded. The facility shall record the date and time of the incident or breach, the location within the facility where the incident or breach occurred, a description of the incident or breach, the identity of the individual who received the report and a description of the response or investigation. If the facility is required to report threats to a governmental agency, the date and time the incident was reported to the agency and who within the agency received the information.
- d) *Maintenance, Testing, and Calibration of Security Equipment*—Security equipment shall be maintained and tested in accordance with manufacturer's recommendations. The facility shall record equipment malfunction, repairs, replacement of equipment, and routine maintenance of equipment. The equipment shall be identified by location and serial number. Each entry shall include the date and time; name and qualifications of the technician; and the specific security equipment involved for each occurrence of maintenance, calibration, and testing
- e) *Threats to the Personnel/Facility/Operations/Company*—The facility shall maintain records of all security threats and record the date and time of occurrence, how it was communicated to the facility, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response. If the facility is required to report threats to a governmental agency, the date and time the incident was reported to the agency and who within the agency received the information.
- f) *Audits*—The facility shall maintain records of security audits to include the type of audit, results of the audit, and the names of the auditors. Audit findings and recommendations shall be tracked until they are completed or resolved.

6.9 Response to Change in Alert Level

6.9.1 General

This section of the security plan shall describe the security alert system in use at the site or company. Threats are fluid and can increase or decrease unexpectedly based on changes in world conditions. These changes may be known or unknown to the general public, which makes it difficult to determine the risk to the facility at any given time. Changes to security levels are usually initiated by information received from a government agency advising that there is an increased threat to the country, industry, or the facility.

To help prepare and address the potential changes to the threat level, the facility shall first establish its baseline security measures for normal operations. Once the baseline security measures are established, the facility shall define the elevated alert levels and design a tiered approach to apply appropriate security measures for the duration of the elevated threats.

The results from the security risk assessment should assist the facility identify the threat, recognize the risk, and select appropriate countermeasures for the baseline security measures. The facility shall define at least two additional alert levels such as an *elevated threat alert*, which indicates that there is a credible terrorist threat, and an *imminent threat alert*, which warns of a credible, specific, and impending terrorist threat. The facility may add additional threat levels between the baseline and Imminent Threat Alert to have a more gradual security increase if desired. The threat levels are based on a preplanned layered approach to implementing security measures. As the threat level increases, the recommended measures build on the security measures already deployed from the previous threat level.

The facility may detect a threat within the facility and decide to raise the alert level without any communication from the government. The relative threat to the facility is dynamic and should increase and decrease as the risk of the threat rises or falls. As the threat to the facility escalates, temporary security upgrades shall be implemented to counter the new threat level. The facility shall develop and document a plan to increase security measures commensurate with the elevated threat. The preplanned response to increased threat levels allows the facility to quickly respond, make incremental adjustments, and employ appropriate countermeasures. The plan shall outline the process to raise the alert level and designate who has the authority to order the change.

The enhanced security should reduce the likelihood of a successful attack. The facility shall develop a scalable set of security measures to augment the facility's security posture proportionate to the elevated threat level.

Once the facility is aware of the increased threat level, it shall implement the enhanced security measures without unnecessary delay. The facility shall document the date and time it became aware of the increased threat, how the threat was communicated, who communicated the threat, who the threat was communicated to, and record the date and time the enhanced security measures were implemented. If the facility is required to notify a regulating authority when the enhanced security measures have been implemented, the facility shall record the date and time the report was made and to whom it was reported.

Appendix C in the example plan in Annex A should describe security countermeasures that may be deployed in the event of an elevation in threat level. The specific countermeasures deployed should depend on the nature of the threat (e.g. physical or cyber), intelligence received, and operational conditions at the facility.

6.10 Communications

6.10.1 General

This section of the security plan shall describe the communications capabilities of the facility to implement the security plan and operate during an emergency. Communication systems and procedures shall be regularly tested and should allow for effective and continuous communications between the facility, security personnel, operations personnel, vessels interfacing with the facility (if applicable), and national and local authorities. Any deficiencies shall be documented and corrected as soon as possible.

The facility shall have a backup means for both internal and external communications (e.g. cell phones, land-lines, fax, and email). The plan shall provide for the regular testing of communications equipment and prompt correct any deficiencies.

Warning—It should be noted that during an emergency accompanied by widespread telephone landline disruption or outage, the cell phone system may become overloaded, making cell phone usage sporadic and possibly unreliable.

The facility shall develop and document in the plan how the facility should communicate the increased threat level to employees and contractors; how the facility should communicate with vessels that may be docked (if applicable); how