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.

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

Contents

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.gocoastguard.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 *CFR* 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 AFSO 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

the facility should communicate and instruct off-duty employees and contractors; and the communications capabilities between employees (e.g. radio, telephone, etc.).

The plan should address the communication and security of data by identifying which computer systems and networks are critical to security (e.g. process control systems, electronic access control systems, etc.), including a general description of the cyber security provisions for these systems as well as any redundancies or backup capabilities.

This section of the plan shall also describe the communication strategy between the facility and external entities that may play a role in a security response at the facility (e.g. local fire and police departments). In addition, the facility should consider reaching out to neighboring businesses and residences to encourage them to report any suspicious activity that they may observe around the facility and provide them with appropriate contact numbers to use for reporting such activity.

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

Security systems and equipment shall be maintained in good working order to ensure its continuous and effective operation. It shall be inspected, tested, calibrated, and maintained according to the manufacturers' recommendations by qualified technicians. Malfunctions shall be noted and necessary repairs or replacements shall be made by qualified technicians as soon as possible but without any unnecessary delay.

6.11 Site Maps

This section of the plan shall contain detailed schematics showing the layout of the facility. 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, and

h) muster points.

6.12 Network Segmentation

The FSO should work with appropriate information technology personnel to segment computer networks to manage risk of disparate user and system communities. Segmenting populations with different risk tolerances allows for the application of specific controls like disabling of unnecessary services (e.g. email on process control networks). Minimizing the number of available services reduces attack surface and therefore helps to maintain system availability and avoid health, safety, and environmental impacts.

Segmentation should also be used to separate networked physical security and monitoring devices like CCTV and electronic sensors from the systems/sites they are intended to monitor. Physical security devices may seem innocuous but they have a different purpose than the business or operational networks under their purveyance.

Placing such devices on business/operational networks mixes risk tolerances and increases attack surface; there have been documented cases where perpetrators have compromised physical security devices and then operational (SCADA) systems connected on the same network. The 2008 Baku-Tbilisi-Ceyhan (BTC) pipeline explosion is one example where perpetrators exploited vulnerabilities within surveillance cameras to gain network access and then manipulated SCADA systems residing on the same network. [4]

In cyber security a DMC or demilitarized zone is used to increase security to the facility's internal network by segmenting and isolating publicly accessible servers to prevent an external network from accessing and compromising the facility's internal network. Ultimate segmentation (which is also referred to as "air-gapping" and occurs where a network is completely disconnected from others) is generally not possible in contemporary environments either because some external access is needed (e.g., maintenance) or information on one network is of value to another network. Connections between disparate networks should be designed with pass-through zones (DMZ); other controls, such as one way data transmission, should be considered in order to reduce the possibility of compromises through the extended network.

6.13 Security Systems and Equipment Maintenance

This section of the security plan shall describe the inspection, testing, and preventive maintenance program for the site's security systems and equipment. All security systems and equipment shall be inspected, tested, calibrated, and maintained according to the manufacturer's recommendations by qualified technicians to ensure that the security systems and equipment at the facility are in good working order for a continuous and effective operation. Malfunctions shall be noted and necessary repairs or replacements made by qualified technicians as soon as possible with no unnecessary delays. When security equipment malfunctions or is out-of-service, the FSO shall evaluate the situations to determine what alternate means of security are required to mitigate the security lapse. Alternate means could include the use of portable lighting, deployment of additional security personnel, closure of access gates, etc.

Cyber security hardware and software, such as firewalls, intrusion detection systems, anti-virus, etc., shall likewise be validated and alternative controls implemented when security devices are found to be defective. The testing, maintenance, and repair of cyber systems must be done by qualified technicians.

6.14 Physical Security

6.14.1 General

The facility shall employ multiple security systems working together to form a layered approach to security that may include countermeasures, such as perimeter fencing, designated restricted areas, barriers, closed-circuit television (CCTV), intrusion detection sensors, and controlled access points. The above list is not all inclusive. The countermeasures chosen for a facility should be unique to that facility and should depend on the size, configuration, facility type, operations, and the perceived value of the facility as a target from an adversary's point of view.

Physical security is distinguished from cyber or network security. However, elements of physical security may incorporate cyber measures in areas such as access control, perimeter protection, intrusion detection, and CCTV. The physical security systems and cyber systems complement each other and work together and are supported by the facility's policies, plans, and procedures to form a robust security system. The facility shall employ a strategy of "Defense in Depth" by placing layers of increased protection between access points and critical assets.

The facility shall integrate both physical and cyber security measures in a comprehensive system to provide a layered approach to protect people, the facility, and other assets. The mix of security measures chosen should deter, detect, delay, or respond to an incident. The facility shall ensure security measures are implemented to:

a) deter the adversary from attempting to breach the facility's security;

[4] Jordan Robertson Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar" [Webpage], (December 10, 2014), http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

b) control access to the facility;

c) deter the unauthorized introduction of dangerous substances and devices into the facility;

d) secure dangerous substances and devices that are authorized to be on site; and

e) protect critical information from unauthorized disclosure.

6.14.2 Fencing/Clear Zones/Visual Observations

Fencing, clear zones, and visual observations are the first layers of defense for the facility by marking the boundaries of the facility, providing a psychological deterrent discouraging unauthorized persons from entering the facility, and providing a temporary delay for those that try.

The facility shall establish permanent perimeter fencing that meets company standards or industry standards (if there are no company standards). Current fencing that does not meet the company standards shall be upgraded when the fence is replaced due to damage or other wear.

The facility shall develop written programs to inspect, repair, and upgrade fences. To be effective, fencing must be checked and repaired on a regular basis. Frequently, the fence fabric is not properly attached to the support poles and the bottom wire is not secure. Erosion of the ground under the fence often results in gaps or washouts that may permit someone to crawl under the fence. Another common problem is that vegetation is allowed to grow up close to the fence providing cover for potential adversaries or a possible platform for climbing over the fence.

Each facility shall develop written programs to inspect and maintain perimeter clear zones. A perimeter clear zone of a minimum of 10 ft to 15 ft, is recommended beyond the fence line perimeter (if the facility owns the property) in order to allow for detection of intruders. Additional clear zones may be required along perimeters adjacent to rivers, streams, and wooded or forested areas.

6.14.3 Gates

Properly designed gates, in conjunction with the perimeter fence, channel both vehicles and pedestrians to a limited number of access control points where their identity can be verified before they are granted access to the facility. All gates should be secured or monitored utilizing manpower or CCTV. The facility shall limit the number of gates to the number necessary to safely operate the facility. Any unnecessary gates should be removed and replaced with the perimeter fence.

6.14.4 Vehicle Barriers

Vehicle barriers are designed to control vehicular access to protect critical assets by delaying or preventing forced entry. Barriers are placed strategically around the perimeter where terrain might permit a vehicle to gain enough speed to breach the perimeter fence. Barriers may also be placed in roadways approaching access points to slow vehicles as they approach the facility. The need for vehicle barriers should be determined by the security risk assessment.

If the facility concludes vehicle barriers should be employed, there is a wide range of acceptable barriers to choose from. If crash barriers are utilized, the barrier ratings shall be determined by verification of actual crash data. Barriers that have not been crash tested shall not be used.

6.14.5 Natural Barriers

Natural barriers such as excavations, ditches, and berms can also be effective passive barriers.

6.14.6 Security Lighting

Adequate security lighting at the perimeter access is a deterrent to unauthorized personnel penetrating the perimeter. Lighting also assists monitoring of the perimeter and detection of attempts to breach the fence. All security lighting shall meet company or industry standards to provide proper illumination.

Lighting around guard posts shall be designed to allow for visual inspection of credentials. Preferred lighting is full spectrum (white light). The lighting shall be placed to illuminate areas outside the guardhouse and prevent a visitor from seeing inside the guardhouse.

Lighting in the intruder detection and assessment zone shall be designed to allow for observation by security personnel and CCTV systems. No light fixtures should be in the field of view of CCTV cameras.

Facilities shall periodically ensure lighting levels are adequate using a light meter and document the survey. The facility shall also develop and implement a system to inspect and maintain security lighting on a regular schedule. Defective lights shall be reported and documented. A work order shall be prepared and tracked pending completion.

6.14.7 CCTV and Electronic Sensors

The facility shall monitor security events by combining a variety of electronic sensors providing real-time remote alarms and images with human oversight. In the event a remote alarm or sensor is activated, the facility shall assess the incident by evaluating the alarm and confirming the incident utilizing the CCTV system. The effectiveness of CCTV systems is greatly enhanced when it is combined with an intelligent video system that detects anomalies and triggers an alarm to alert the operator.

The integrated technical security system often includes:

a) sensors;

b) CCTV or thermal imaging cameras with an intelligent video system that detects anomalies and triggers an alarm to alert the operator;

c) electronic access control; and

d) a system to monitor, control, and display security event information so it can be evaluated and acted upon if necessary.

7 Futures—Additional Integration of Cyber and Physical Systems

The FSO should further integrate cyber and physical security concepts as “Internet of Things” (IoT), the next step change in information technology, becomes a reality. IoT currently lacks a definitive definition but a good working concept is an environment where everything is networked, connected to the Internet, and capable of exchanging information with other machines and/or humans. Tens of billions of IoT devices are projected to be Internet connected within the decade with this growth fueled by lower cost sensors, ubiquitous wireless networking, and consumer mobile devices. Common, everyday items like light bulbs, projectors, electric meters, and photocopiers are even now being “computerized” and networked. IoT compromises may have both cyber and physical ramifications; an attack which disables light bulbs may make a building impossible to occupy during evening hours.

The FSO should conduct risk assessments to understand the risk of IoT deployments and work with appropriate information technology personnel and supply chain to apply needed controls. At a minimum IoT devices and networks should be monitored for suspicious behavior with the monitoring informed by threat modeling and integrated intelligence.

8 Personnel Surety

8.1 General

This section of the plan shall describe how the facility vets its employees, contractors, and visitors prior to granting them access to the facility. When permitted by law, the facility shall ensure that appropriate background checks are conducted on all facility personnel to evaluate their suitability for admission to the facility.

Personnel surety includes confirmation of identity and credentials as listed on the application or resume. Personnel surety forms the foundation of an access control system built on trust and provides a degree of confidence that an individual is who he or she represents himself or herself to be with the skills and experience claimed. An effective personal surety program can help the hiring manager more accurately evaluate the candidates for the position and should enhance the facility's ability to deter, detect and reduce the likelihood of insider threats. At a minimum, a personnel surety program shall include the following:

a) measures designed to verify and validate identity;

b) measures designed to check criminal history;

c) measures designed to verify and validate legal authorization to work;

d) measures to validate education and prior work as appropriate;

e) motor vehicle record if the individual's position requires driving (where permitted by law); and

f) professional references, as appropriate.

8.2 Background Check

The background check should involve a search of publicly or commercially available databases and repositories for jurisdictions in which an individual has worked or resided for the last seven years. The criminal history search shall be limited to convictions, outstanding warrants, pending indictments, sentencing, and disposition dates. There are several privacy concerns with the personal surety program because background checks collect highly sensitive personal information that shall only be collected and utilized to make employment decisions as allowed by law. The permissible use of the information collected during the background investigation is regulated in most jurisdictions. Background investigations shall only be conducted by trained individuals who are familiar with the restrictions and permissible uses of the information. The hiring manager should also be familiar with the restrictions and permissible uses of the information.

Disqualifying employment decisions should be made in consultation with human resources or the legal department who are familiar with the facility's background check policy and relevant laws and regulations governing hiring decisions that are based on criminal history information. To avoid charges of disparate treatment or disparate impact resulting in potential liability, the facility should consider using a two-step process to evaluate an application when the applicant has a criminal record.

In the first step the facility uses a "targeted" screen of criminal records. A "targeted" screen considers the nature of the crime, the time elapsed since the offense, and the nature of the job. The facility should demonstrate that its targeted screen is always job related and consistent with business necessity.

Once the targeted screen has been administered, the facility should consider providing opportunities for individualized assessment for those who were screened out. Using individualized assessment in this manner provides a way for employers to ensure that they are not mistakenly screening out qualified applicants or employees based on incorrect, incomplete, or irrelevant information, and for individuals to correct errors in their records.

8.3 Employees

All personnel having unescorted access to the facility should undergo a background check to determine their suitability. The Company should conduct background checks on employees and applicants who have been offered employment contingent upon successful completion of the background check.

The company may consider hiring a third party, who specializes in background investigations, to conduct the investigation and report the results for evaluation.

8.4 Contractors

All full-time and long-term contractors having unescorted access to the facility shall undergo a background check equivalent to the background check conducted on facility employees. The contractor may conduct the background check on their employees internally or by contracting with a third-party. The contractor shall be required to certify that background checks have been completed and that their employees have met the standard established by the facility. The contractors' background check program shall be subject to annual audit by the facility.

8.5 Audit of Personnel Surety Program

The personal surety program shall be audited annually to verify compliance with both the FSP and all related regulations.

9 Security Measures for Access Control, Including Designated Public, Controlled, and Restricted Access Areas

9.1 General

Access control is a process by which entry into and internal movement within the facility is managed. The FSO shall evaluate the complex in order to define and designate public access areas, secure access areas, and restricted access areas with public access areas having the least restrictions and restricted areas having the most restrictions. Each area shall become progressively more restrictive by imposing additional security restrictions and requiring additional authorizations. A key component of a successful access control program is knowing who is allowed on site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted facility access.

This section of the plan shall describe how access to the facility is controlled to prevent unauthorized access and the unauthorized introduction of dangerous substances and devices intended to cause damage to persons or to the facility. The part of the plan shall focus on the identification, screening, and inspection of individuals and vehicles as they enter and exit the facility or restricted areas within the facility.

External service providers, business partners and vendors present a potential risk to the facility's systems, information, and intellectual property when they are given access to the facility's cyber assets. The facility shall ensure that background checks are conducted prior to granting them access to the facility's IT infrastructure. The facility should also consider having them sign memoranda of agreements, nondisclosure agreements, confidentiality agreements, and conflict of interest agreements.

The facility shall ensure that a system is established for checking the identification of facility personnel or other persons seeking access to the facility and describe the means used to identify who is authorized to be in the facility. Examples of acceptable personnel identification include the following.

a) A government-issued photo identification card such as a driver's license. Individuals arriving on motorcycles shall remove their helmets when presenting a photo identification card.

b) The facility may issue photo identification badges to individuals permitted access to the facility. The facility shall verify the individual's identity before providing the identification badge to the individual. The access control system is further enhanced and more effective if a background check is performed once the individual's identity is confirmed (see 6.12).

c) The company or facility may use photo identification badges that are linked with an electronic access control system. The electronic access control system can recognize invalid or deactivated badges and can be programmed to only allow authorized personnel access to restricted areas. The access control system also maintains a record of the date and time that the badge has been used to access the facility and the specific areas within the facility.

d) The badge should be worn where it should be visible to others in the facility. If the individual is working in an area where the badge could present a safety hazard, the employee should remove the badge but have it readily available to display upon request.

e) Lost, stolen, or misplaced badges shall be reported to security immediately.

f) When entering an access controlled area in a vehicle, each occupant in the vehicle shall display or swipe their badge.

g) The facility should consider installing Vehicle Control Points to help manage vehicular access to the facility by slowing or calming traffic as they approach the facility access point. The vehicle control points should lead to an inspection point where the driver and passengers can be screened prior to entering the facility. This procedure provides an opportunity for the vehicle to be identified and permitted to enter the facility or to be denied access. There should be a rejection lane where unauthorized vehicles and persons can be turned away prior to entering the facility.

h) The facility may choose to use speed bumps, a circular or serpentine roadway, jersey barriers, etc. or any combination to create the control points.

i) The plan shall contain a description of the general access control countermeasures deployed at the facility (e.g. fencing, gates and locks, jersey barriers or other types of barricades, "No Trespassing" or related signage posted at the facility, intrusion detection systems, etc.).

9.2 Visitors

Visitors to the facility should be limited, as much as possible, to meeting business or public relations objectives. All visitors should be processed in accordance with this section of the plan.

a) To the extent possible, all visitors shall be scheduled and registered in advance of the visit. Unregistered visitors may be asked to remain outside the facility until their desired contact person authorizes their visit.

b) Arriving visitors shall be directed to an initial identification point where they can be screened and their vehicle may be inspected. The facility however, shall reserve the right to search all persons, vehicles, and packages entering the facility and to deny entry to anyone refusing to be searched. Appropriate signage shall be placed at all entrances (see 6.9.4).

c) The facility should ensure that visitors sign in and out upon their arrival and departure. They should receive a security and safety briefing before being admitted to the facility. The facility should also consider a visitor badge to identify the visitor as someone who may have limited knowledge of the facility, restricted areas, danger areas, and how to react if there is an emergency.

d) Visitors shall be escorted at all times while they are in a secure or restricted area.

9.3 Deliveries

Deliveries, especially unexpected or unscheduled deliveries, have the potential to introduce dangerous objects to the facility. All deliveries should be processed in accordance with this section of the plan.

a) Arriving deliveries shall be directed to an initial inspection point where security personnel can screen the delivery and inspect the delivery tickets, bills of lading, and the delivery vehicle.

b) Vehicles without a valid bill of lading or that are making an unexpected delivery shall not be admitted to the facility until the shipment is thoroughly inspected and cleared for delivery by warehouse personnel.

9.4 Government Employees

In certain regulated facilities, authorized government officials may enter to inspect and audit the property, equipment, operations and records of the covered facility.

a) The FSO should be familiar with the regulations covering the facility and authorities given to government employees to enter the facility either announced or unannounced. The government official must be authorized by the regulation, conducting official business and present a valid government organization photo ID prior to entry. Government officials, not authorized by regulation, seeking admission to the facility should be considered on a case by case basis. The FSO, facility manager and legal counsel should be included in the discussion and decision to deny or grant access to the official.

b) The facility manager, FSO and legal counsel should be advised immediately of the arrival of any governmental official seeking access to the facility.

9.5 Screening, Searches, and Inspection

The facility may screen employees and visitors, conduct searches of personnel and vehicles, and inspect packages, bags and briefcases in accordance with this section of the plan to deter and detect the unauthorized introduction of dangerous devices or the unauthorized removal of company assets.

a) The facility may select from a variety of measures to perform screening. These measures include verification of personal identification, inspecting hand-carried items, vehicle identification, and vehicle inspections. Inspections and searches shall be conducted by trained personnel familiar with company policy and legal requirements.

b) Searches conducted by the facility generally fall under three categories as follows.

   1) *Gate Search*—A gate search is the routine inspection of persons and vehicles entering or leaving the facility. The facility may choose to search 100 % of persons and vehicles or develop a plan to search persons and vehicles on a random basis. The method used by the facility to search persons or vehicles on a random basis shall be structured and documented to ensure that the selection process is fair and equitable. The procedure shall be transparent and developed to limit the discretion of the searcher when selecting the person or vehicle to be searched. Every search shall be documented in such a manner to demonstrate that protocol was followed and the search was random.

   2) *Search for Cause*—A search for cause is the search of a specific individual, their vehicle, or their possessions, who is suspected of committing a violation of company policies.

   3) *Contraband Items Search*—A contraband items search is an unannounced search of personnel, their work areas, locker rooms, or vehicles for prohibited items.

c) The employee, contractor, or visitor must consent to the search or inspection. Failure to consent may result in denial of access, removal from the site, and, for employees, disciplinary action.

d) Inspections may include a visual inspection, trained dogs, ionic explosives detection, x-ray inspections, and metal detectors.

e) If a dangerous substance or device is discovered, the FSO and facility manager shall be advised immediately and ensure that the following actions, as applicable to the situation, are taken:

1) evacuate the surrounding area and prevent reentry;

2) instruct all personnel to not to touch or move the suspicious object;

3) prohibit the use of cell phones and radios if the suspicious object appears to be an explosive device;

4) notify police that a suspicious substance or object has been discovered and wait for them to remove the device; and

5) search to determine if additional devices or substances have been placed once the device is removed.

Each active access control point (ACP) should be listed in the plan. ACPs are those control points used on a daily basis to control ingress/egress to the facility. The list should include a description of the operation of the ACP (e.g. chain-driven vehicle gate), hours of operation, and the security countermeasures utilized at the ACP (e.g. manned vs unmanned countermeasures, CCTV coverage, card readers, etc.).

9.6 Restricted Areas

Restricted areas are areas within the facility that require a higher degree of security protection. Access to restricted areas shall be limited to employees, contractors and service personnel who have a documented need to be in the restricted area. The FSO, may designate the entire facility as a restricted area or limit the designation to certain areas of the facility. Access shall be restricted in areas that have the potential to cause the most harm to people, the facility, and the company. In general, areas containing sensitive information, critical processes, hazardous material, process controls, etc. shall be designated as restricted areas. Many times the following locations are designated as restricted areas:

a) manufacturing or process areas and control rooms;

b) SCADA control systems, other process control systems, IT infrastructure locations;

c) systems and areas where sensitive security information is stored;

d) areas containing security equipment, surveillance equipment and their controls;

e) electrical sub-stations;

f) water supplies;

g) telecommunication system locations;

h) HVAC intakes; and

i) areas containing dangerous or hazardous substances.

In this section, the plan shall clearly identify the location of these restricted areas and systems, identify which facility personnel are authorized to have access to those areas and systems, identify persons—other than facility personnel (e.g. contract technicians)—who are authorized to have access, and the conditions required to be met before access is granted to such individuals. The facility shall escort contractors, repairman, and technicians in restricted areas until they have been completely vetted.

9.7 Security Countermeasures for Restricted Areas

The plan shall recognize that restricted areas are the most sensitive areas in the facility because they have the potential to cause the most harm to people, the facility, and the company. The plan shall also describe the additional security countermeasures deployed to protect these areas from unauthorized access.

Cyber systems can be compromised physically as well as electronically and thus require the same or higher physical security measures needed to protect physical assets. To protect critical cyber assets, the facility shall restrict access to sensitive IT areas, such as control rooms, LAN and server rooms, wiring closets, and workstations operating sensitive applications (e.g. access control system and the CCTV monitoring area etc.).

Examples of security countermeasures for restricted areas include (but are not limited to) the following.

a) Clearly marking all restricted areas that indicate access to the area is restricted and that any unauthorized access constitutes a breach of security.

b) Utilizing defense in depth principles by adding additional layers of security (e.g. locked doors, fencing, barriers, badge readers, two-factor authentication, etc.).

c) Employing physical barriers to impede movement through access points.

d) Securing or eliminating all unnecessary entry points into a restricted area that are not routinely used.

e) Assigning personnel to control access to restricted areas.

f) Restricting IT areas (IT areas can be accessed by going over or under the buildings internal petitions such as low hanging panel ceilings or raised floors. The facility should consider protecting sensitive IT areas with true floor to true ceiling walls. An alternative is to secure the areas below the floor or above the ceiling with wire partitions and alarms to detect intrusion).

g) Conducting screening and inspections of pedestrians and vehicles entering and leaving a restricted area.

h) Patrolling or monitoring the perimeter of restricted areas or systems.

i) Using automatic intrusion detection devices or surveillance equipment to detect unauthorized entry or movement within restricted areas systems.

j) Directing the parking, loading, and unloading of vehicles within a restricted area.

10 Security Measures for Monitoring

This section of the plan shall describe how the facility is continuously monitored for unauthorized access. The facility shall implement security countermeasures that have the capability to continuously monitor the facility, its approaches on land and water (where applicable), and the restricted areas with a combination of lighting, patrols, automatic intrusion detection systems, or surveillance equipment. The primary method most facilities should use for monitoring is human oversight by facility personnel (or security guards if applicable). Personnel, while performing routine job responsibilities, also shall remain vigilant in detecting and reporting suspicious activity. Consideration should be given to developing a security-specific critical patrol log (CPL) that facility personnel could utilize on a random basis to

increase facility monitoring performance. Items to incorporate into the CPL include (but are not limited to) the following.

a) Each perimeter access control point (both active and inactive).

b) Remote facility locations not readily observed that could provide an adversary with concealment.

c) Lighting locations—particularly along the perimeter.

d) Perimeter areas prone to environmental degradation (e.g. erosion).

e) Restricted areas within the facility.

f) Random patrols to detect suspicious vehicles, persons, and packages along the facility perimeter.

g) Adequate facility lighting, which is also critical for monitoring a facility against unauthorized access. All areas of the perimeter should be illuminated to the degree that suspicious persons, vehicles, or objects can be readily detected by facility personnel.

As discussed in 6.7, the facility should consider reaching out to neighboring businesses and residences in order to encourage them to report any suspicious activity that they may observe around the facility. The means that neighbors should use for reporting such activity should be documented in this section of the plan. Incorporating the participation of neighboring businesses and residences provides additional “eyes and ears” to monitor the facility for unauthorized access or suspicious activity.

Higher risk facilities may also consider deploying surveillance cameras to monitor the facility perimeter and approaches to the facility. If feasible, the facility may want to look beyond the fence to detect suspicious activity prior to a breach or an attempted breach. The placement of these cameras should provide the most benefit if the facility can estimate the most likely approaches to the facility based on a credible risk analysis.

Additionally, automatic intrusion detection systems may be deployed (e.g. fence disturbance sensors, microwave sensors, buried line sensors, etc.).

This section of the plan should also describe how the facility’s cyber assets are monitored against unauthorized intrusion. Intrusion detection/prevention systems should be deployed to identify known malicious activity (e.g. worms, viruses, unexpected protocols, etc.) while activity contrary to standard business practices could be detected with additional network analyses.

11 Key Control

This section of the plan shall describe how keys are issued, tracked, returned, reported lost or stolen, and the unauthorized use of duplicate keys and loaned keys. The following procedures should be incorporated into this section of the plan.

a) Distribution of keys shall be authorized in writing and entered into a Key Control Log. The log should be a computer-based key control program.

b) Keys shall only be issued to employees and contractors who have a demonstrated need to access that area.

c) Lost or stolen keys shall be reported immediately. The security manager and the facility manager shall determine if security has been compromised and if the lock needs to be changed. Employees shall not duplicate keys or loan keys to another employee. Keys shall not be left unattended.

d) All issued keys shall be returned when an employee or contractor leaves the facility. The return keys should be validated against the Key Control Log.

12 Security Incident Procedures

The identification, investigation, reporting, recording, and evaluation of security incidents or security breaches is an essential component in providing adequate security for the facility. Thorough investigations and complete incident reports enable the FSO to evaluate potential threats, identify weaknesses in the security plan, and to employ appropriate countermeasures.

This section of the plan shall define what constitutes a security breach, security incident, or suspicious activity, the personnel to be notified of the security breach, security incident, or suspicious activity, and the order of such notification. Additionally, the plan shall describe the procedure to investigate the incidents, document the findings, and maintain records of security breaches, security incidents, or suspicious activity. This section should also generally describe or reference the site emergency response plan and the company crisis management plan, if applicable. Examples of possible security incidents include (but are not limited to):

a) theft or loss of company property;

b) possible incidents of pre-operational surveillance (e.g. picture taking, phishing email, etc.);

c) unauthorized entry into the facility;

d) refusal to submit to a search;

e) presentation of false identification;

f) observed attempt to defeat a security system; and

g) attempts to bring unauthorized dangerous devices or materials into the facility.

13 Audits and Security Plan Amendments

13.1 Audits

The FSO shall ensure that the FSP is audited on a regular basis. The FSP should also be audited if there is a change in ownership, and significant modifications to the facility, the property, physical structures, emergency response procedures, security measures, or operations.

13.2 Audit Amendments

If the audit indicates that the FSP requires an amendment, the FSO shall submit a proposed amendment to the facility manager, document owner, approving authority, and other individuals or entities designated by the company policy not later than 30 days after the completion of the audit. Once the amendment is approved, it shall be distributed to all authorized FSP holders, inserted in the FSP, and recorded in the record of change set forth in Table 2.

13.3 Findings

Any deficiency identified or recommendation may as a result of the audit shall be documented and tracked until the issue is resolved.

Annex A
(informative)

Example Security Plan

Facility Security Plan
ABC FACILITY
DATE

A.1 Record of Change

REV #	DATE	Replaces Pages/Section	Document Owner*	Replacement Made BY
Initial Issue	6/4/2014	Initial Issue	John Doe	Initial Issue
1	9/1/2014	Section XX, pages XX-XX	John Doe	Jane Doe

A.2 Distribution

Distribution:
FSP Copy #

1. John Wayne
2. Bill Burris
3. John Smith
4. Roger Hillman
5. Billy Johnson

Example—This document contains confidential information and must be protected from unauthorized disclosure. It is not to be copied or distributed without the approval of the Facility Security Officer.

Copy number X of X.

A.3 Security Administration and Organization of (Facility name and type)

A.3.1 Definitions

Definitions used in this Facility Security Plan are attached in Appendix D.

A.3.2 Facility Personnel

This section of the security plan identifies personnel and groups with security roles, lists their responsibilities, and describes how security is managed at the facility. All persons listed in this section are identified by name, title, and 24 hour contact information.

Position	Name	Office Phone	Cell Phone
Facility Manager			
Facility Security Officer (FSO)			
Facility Security Officer (Alternate)			
Facility Security Officer (Alternate)			
Legal Advisor			
Cyber Security Officer			
Corporate Security Officer			
Contract Security Supervisor			
Add any other persons needing notification			

A.3.3 Outside Resources

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

Police Department: _____

Fire Department: _____

National Law Enforcement: _____

Other Government and regulatory agencies as required: _____

Phone numbers are for notification of security-related events. If releases, fires, or injuries occur from a security-related event, additional notifications to a Response Center, etc. may be required. Please refer to the appropriate facility Emergency Plan for guidance.

In this standard, the term “facility management” indicates the facility manager or a person operating as his designated replacement. All actions required by the FSO that are not covered by this procedure should be communicated immediately to facility management.

A.3.4 Facility Personnel

A.3.4.1 General

This section of the security plan describes how security is managed at the facility, identifies personnel and groups with security roles and enumerates their responsibilities. All persons listed in this section shall be identified by name, title, and 24 hour contact information. In smaller facilities, it is not uncommon for someone to assume more than one role.

A.3.4.2 Owner/Operator

The owner/operator defines the security organization in writing, delegating 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.

A.3.4.3 Facility Manager

Security of the facility is a line item responsibility and rests with the facility manager who has the overall responsibility for security at the facility. The facility manager also ensures that facility personnel comply with the FSP, 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.

A.3.4.4 Facility Security Officer

The facility security officer (FSO) has the overall responsibility for managing the day-to-day security of the facility. The FSO's responsibilities may include the following:

a) ensures that security risk assessments are conducted at regular intervals and recommendations are addressed and resolved as appropriate;

b) prepares and updates the FSP;

c) conducts and documents internal security audits on a regular basis;

d) develops security training for all employees based on their security responsibilities and documents the training;

e) develops and conducts drills and exercise and documents the results;

f) maintains liaison and develops relationships with local law enforcement and first responders;

g) is cognizant of current security threats and ensures that security measures in place are adequate to address the risk;

h) documents and communicates changes in threat level or security procedures to all employees;

i) responds to and documents security incidents;

j) ensures that security equipment is properly maintained, calibrated, and tested; this shall be documented; and

k) develops and maintains a system of records as outlined above.

A.3.4.5 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.

A.3.4.6 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.

A.3.4.7 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. 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.

A.3.4.8 Contract Guard Force (if applicable)

The FSP shall identify the following.

a) 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.

b) Document security roles, also known as post orders, performed by contract security guards. (A copy of the post orders are attached as Appendix A.)

c) The name, title, and 24 hour contact information of the site supervisor for the contract security force.

A.3.4.9 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 Officer.** 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) **The 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.

A.3.4.10 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) Police Department,

b) Fire Department,

c) National Police,

d) Customs,

e) other government and regulatory agencies as required.

A.3.5 Site Maps

Site maps containing detailed schematics showing the layout of the facility are attached in Appendix B. The schematics identify and clearly mark the following:

a) public areas, secure areas, and restricted areas;

b) perimeter fencing; guard post locations;

c) vehicle gates;

d) pedestrian gates;

e) cameras;

f) parking areas; and

g) muster points.

A.4 Security Training

A.4.1 Facility Security Officer (FSO), the Assistant Facility Security Officer (AFSO), and Others with Security Duties

Facility personnel with security duties may include the FSO, the AFSO, proprietary security officers, contract security officers and other employees with security duties that have been designated in section 5.3. Personnel with security duties should complete an initial security awareness program designed or approved by the FSO. In addition, both

proprietary and contract security officers should complete a training program designed by the FSO specific to the security requirements of the facility.

In general, the contract security company is responsible for training their officers to a level that meets or exceeds the requirements for facility employees with security duties. The contract security company must document and retain security training records. Training may be provided via on-the-job training, computer-based training, videos, PowerPoint presentations or classroom instruction.

A.4.2 Duties of the Facility Security Officer and the Assistant Facility Security Officer

The Facility Security Officer (FSO) and the Assistant Facility Security Officer (AFSO) are charged with the overall security of the facility and require the highest level of training. They receive in-depth training on the Facility Security Plan, the facility's security objectives, security procedures, employee responsibilities, and actions to take in the event of a security breach. In addition, they must 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) topics are also chosen based on such items as the unique security characteristics of the facility, likely threats to the site, the introduction new security equipment and/or procedures, and other topics deemed important by the Facility Security Officer; and

s) all security training should encourage personnel to remain vigilant during their time at the facility and to promptly report suspicious activity.

A.4.3 Facility Personnel with Security Duties

Facility personnel with security duties should be given an annual awareness training refresher course to ensure their training is current. The security officer's training program is reviewed annually by the FSO or contract security supervisor, and security officers are re-certified annually by the FSO or contract security supervisor.

A.4.4 Security Training for All Other Facility Personnel

All other facility personnel, including contractors, whether part-time, full-time, or temporary receive initial security awareness training that includes the following:

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.

The FSO or his designee may incorporate this training into the facility safety orientation.

The FSO shall provide awareness level training for all personnel via on-the-job training, computer based training, video format, PowerPoint presentation, or formal presentation as appropriate.

A.4.5 Testing

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

A.4.6 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.

A.4.7 Frequency of Training

The facility should provide security training on an annual 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 need to know.

A.5 Drills and Exercises

A.5.1 Drills

Security drills are conducted on a quarterly basis (more or less often as determined by the FSO) or as required by regulation. Drills are designed to test a single element of the Facility Security Plan. The scenarios, should be designed 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 Facility Security Plan. Results of the drill should be documented and retained.

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.

Drills test individual elements of the FSP including responses to security threats and incidents. Drills should take into account the types of operations of the facility, facility personnel changes, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities. The FSO shall identify security related deficiencies during drills/exercises and correct facility deficiencies and pass on management program related deficiencies that could pose problems at other facilities.

A.5.2 Exercises

The FSO shall ensure that exercises are conducted on a regular basis (annually), 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 offsite 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 well as determining the effectiveness of the command, control and communication function.

A.5.3 Exercise Content

The FSO may include the following in each exercise but is not limited to the following list:

a) security administration;

b) emergency preparedness, response, contingency, recovery, and continuity planning;

c) responsibilities and functions of other involved organizations;

d) relevant government legislation and regulations;

e) risk, threats, and vulnerability assessments;

f) security assessments and inspections;

g) facility security measures;

h) emergency preparedness, response, and contingency planning;

i) handling sensitive security-related information and security-related communications;

j) knowledge of current security threats and patterns;

k) assessment of security drills and exercises;

l) review of the Facility Security Plan (FSP).

A.5.4 Exercise Formats

Each exercise should test communication, notification, coordination, resources and response. Exercises are a full test of the security program to include company, crew, facility, and government resources. These exercises may be coordinated with a Corporate Emergency Preparedness Group. Exercises may be:

a) full scale or live;

b) tabletop simulation or seminar;

c) combined with other appropriate exercise.

A.5.5 Drill/Exercise Documentation

Drill and exercise documentation should include the following:

a) training/drill/exercise session;

b) duration of session/drill/exercise;

c) description of training/drill/exercise;

d) list of attendees/participants;

e) lessons learned;

f) best/smart practices identified.

A.5.6 Joint Training Initiatives

The FSO should develop relationships with law enforcement agencies and other first responders to a potential incident at the facility and, where practical, invite them to participate in the facility's drills and or exercises.

A.6 Record Keeping and Documentation

A.6.1 General

This section of the security plan describes 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 is classified in accordance with the company's protection of information policy and protected from unauthorized disclosure, deletion, destruction, or amendment.

Records should be maintained and secured in the same fashion as payroll or personnel files and at minimum under lock and key by the FSO or designee. Electronic files should be maintained, secured, and protected by the use of

passwords and personal identification codes. Additional electronic document protection is provided against document alteration and destruction through the use of network security settings and password protection, which control individual access of read only, rewrite, edit, and deletion access.

The list of security related documents below is a suggested list of documents the facility should consider. The list is not all inclusive nor is every document applicable to all facilities. The FSO should review the list and select records applicable to the facility. The FSO should designate the retention period and storage location for each record category listed in the FSP.

A.6.2 Security Training

The FSO should 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.

A.6.3 Drills and Exercises

The FSO should document each drill and exercise conducted to 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 should be revised if necessary. The plan should designate the number of drills and exercises per year (e.g. the facility should conduct quarterly drills and an annual exercise).

A.6.4 Suspicious Activity, Security Breaches, and Security Incidents

The FSO should ensure that all suspicious activity, security breaches and security incidents are investigated and recorded. The record should include 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 should be recorded.

A.6.5 Maintenance, Testing, and Calibration of Security Equipment

Security equipment shall be maintained and tested in accordance with manufacturer's recommendations. The FSO should record equipment malfunction, repairs, replacement of equipment, and routine maintenance of equipment. The equipment shall be identified by location and serial number. Each entry should 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.

A.6.6 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 that the incident was reported to the agency, and who within the agency received the information.

A.6.7 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.

A.7 Response to Change in Alert Level

This section of the security plan describes 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 the facility adjust to changes in the threat level, the facility should establish its baseline security measures for normal operations. Once the baseline security measures are established, the facility should define the elevated alert levels and design a tiered approach to apply appropriate security measures for the duration of the elevated threats.

The baseline security measures are determined by the results obtained from the Security Risk Assessment that should assist the facility identify the threat, recognize the risk, and select appropriate countermeasures for the baseline security measures once the baseline security measures are established, the facility defines at least two additional 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 company's Security Conditions system describes a progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to the facility, company assets, and/or personnel. The purpose of the Security Condition system is to establish standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of local management prior to and during a threat or crisis. Once one of the three Security Condition levels is declared, the associated protective measures should be implemented, as soon as possible, to the extent that they apply to the individual site or facility. Sites/facilities should coordinate Security Condition status through the Corporate Emergency Response Team (CERT) process. Measures associated with each Security Condition are not prioritized, but should be initiated concurrently, when practical. A record of specific actions taken, or to be taken, for each Security Condition measure should be maintained by local Facility Management.

Appendix C of the FSP describes 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.

A.8 Communications

This section of the security plan describes the communications capabilities of the facility to implement the security plan and operate during an emergency. FSO shall develop and maintain a communication system and, at a minimum, address the following protocols.

a) Notification of Security Conditions to personnel via telephone, verbal, email, two-way radio, cellular telephone, or by fax.

b) Contact information at entry point for local, state, and federal agencies via verbal, telephone, or cellular telephone.

c) Secondary facility communication system for internal and external announcements via telephone, verbal, email, two-way radio, cellular telephone, or by fax.

d) Communication system and procedures should allow effective and continuous communications between the facility security personnel, and local or federal authorities, via verbal, telephone, email, two-way radio, cellular telephone, or by fax. Communication systems and equipment shall be maintained in good working order to ensure its continuous and effective operation. The plan shall provide for the regular testing of communications equipment and prompt correctness of any deficiencies.

e) Hand-held VHF walkie-talkies carried by contract security officers are battery powered. A sufficient supply of charged batteries is maintained in the event of a power failure.

f) 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.

A.9 Network Segmentation

The FSO should work with appropriate information technology personnel to segment computer networks to manage risk of disparate user and system communities. Segmenting populations with different risk tolerances allows for the application of specific controls like disabling of unnecessary services such as email on process control networks). Minimizing the number of available services reduces attack surface and therefore helps to maintain system availability and avoid health, safety, and environmental impacts.

Segmentation should also be used to separate networked physical security and monitoring devices like CCTV and electronic sensors from the systems/sites they are intended to monitor. Physical security devices may seem innocuous but they have a different purpose than the business or operational networks under their purveyance. Placing such devices on business/operational networks mixes risk tolerances and increases attack surface; there have been documented cases where perpetrators have compromised physical security devices and then operational (SCADA) systems connected on the same network. (The 2008 Baku-Tbilisi-Ceyhan (BTC) pipeline explosion is one example where perpetrators exploited vulnerabilities within surveillance cameras to gain network access and then manipulated SCADA systems residing on the same network.)

Ultimate segmentation, which is also referred to as air-gapping, is where a network is completely disconnected from others and is generally not possible in contemporary environments either because some external access is needed (for maintenance potentially) or information on one network is of value to devices or users on another network. Connections between disparate networks should be constructed with pass-through zones (“DMZ”) and can consider other controls (one way data transmission as an example) to reduce the possibility of compromise through this extended network.

A.10 Security Systems and Equipment Maintenance

The FSO should ensure the facility’s physical security systems and equipment is maintained in good working order. To maintain the security systems and equipment in good working order to ensure its continuous and effective operation.

a) It must be inspected, tested, calibrated, and maintained according to the manufacturer’s recommendations by trained and qualified technicians.

b) Malfunctions shall be noted and necessary repairs or replacements made by trained and qualified technicians as soon as possible but without any unnecessary delay.

c) When security equipment malfunctions or should be out-of-service, the Facility Security Officer shall evaluate the situations to determine what alternate means of security are required to mitigate the security lapse. Alternate means could include use of portable lighting, deployment of additional security personnel, closure of access gates, etc.

d) Upon noting test deficiencies, the FSO shall ensure that the appropriate vendor, contractor or business unit is notified for resolution of the deficiency. The FSO should develop a maintenance, calibration and testing log of security equipment. The log shall at a minimum address the following:

   — date of the maintenance, calibration and testing;

   — time of maintenance, calibration and testing;

   — specific security equipment tested, calibrated, and maintained.

e) Cyber security hardware and software, such as firewalls, intrusion detection systems, anti-virus, etc., shall likewise be validated and alternative controls implemented when security devices are found to be defected. The testing, maintenance, and repair of cyber systems must be done by trained and qualified technicians.

A.11 Physical Security

A.11.1 General

The term “physical security” refers to equipment, building and ground design and security practices designed to prevent physical attacks against the facility’s people, property, or information. The facility employs multiple security systems working together to form a layered approach to security that may include perimeter fencing, designated restricted areas, barriers, closed-circuit television (CCTV) intrusion detection sensors, and controlled access points. The countermeasures chosen for a facility should be unique to that facility and should depend on the size, configuration, type of facility, operations, and the perceived value of the facility, as a target, from an adversary’s point of view.

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.

Physical security is distinguished from cyber or network security; however, elements of physical security may incorporate cyber measures in areas such as access control, perimeter protection, intrusion detection, and CCTV. The physical security systems and cyber systems complement each other and work together and are supported by the facility’s policies, plans, and procedures to form a robust security system. The facility shall employ a strategy of “Defense in Depth” by placing layers of increased protection between access points and critical assets.

A.11.2 Physical Security and Cyber Security Integration

The facility integrates both physical and cyber security measures in a comprehensive system to provide a layered approach to protect people, the facility, and other assets. The mix of security measures chosen should deter, detect, delay, or respond to an incident. The facility shall ensure security measures are implemented to:

— deter the adversary from attempting to breach the facility security;

— control access to the facility;

— deter the unauthorized introduction of dangerous substances and devices into the facility;

— secure dangerous substances and devices that are authorized to be on site; and

— protect critical information from unauthorized disclosure.

A.11.3 Fencing/Clear Zones/Visual Observation

A.11.3.1 General

Fencing, Clear Zones, and Visual Observations are the first layers of defense for the facility by marking the boundaries of the facility, providing a psychological deterrent discouraging unauthorized persons from entering the facility, and providing a temporary delay for those that try.

A.11.3.2 Fencing Standard

The facility shall establish permanent perimeter fencing that meets company or industry standards. Current fencing that does not meet this standard shall be upgraded when the fence is replaced due to damage or other wear.

A.11.3.3 Temporary Fence

Each Company facility shall establish a plan to ensure that temporary fencing is installed per specification when required for construction projects.

A.11.3.4 Periodic Inspection

Each Company facility should develop written programs to inspect and repair/upgrade fences. To be effective, fencing must be checked and repaired on a regular basis. Frequently, the fence fabric is not properly attached to the support poles and the bottom wire is not secure. Erosion of the ground under the fence often results in gaps or washouts that may permit someone to crawl under the fence.

A.11.3.5 Perimeter Clear Zone

Each facility shall develop written programs to inspect and maintain perimeter clear zones. A perimeter clear zone, of a minimum of 10 ft to 15 ft, is recommended beyond the fence line perimeter to allow for detection of intruders, if the facility owns the property. The facility should maintain a clear zone along the fence line to deny a potential adversary concealment.

A.11.4 Gates/Barriers

A.11.4.1 General

Properly designed gates, in conjunction with the perimeter fence, channel both vehicles and pedestrians to a limited number of access control points where their identity can be verified before they are granted access to the facility. All gates shall be secured or monitored utilizing manpower or CCTV. The facility shall limit the number of gates to the number necessary to safely operate the facility. Each facility shall develop written procedures to ensure that when normally closed gates are opened, a security guard or designee is posted for the time the gate is opened.

Any unnecessary gates should be removed and replaced with the perimeter fence.

A.11.4.2 Vehicle Barriers

Vehicle barriers are designed to protect critical assets by to controlling vehicular access by delaying or preventing forced entry. Barriers may be placed strategically around the perimeter where terrain might permit a vehicle to gain enough speed to breach the perimeter fence. Barriers may also be placed in roadways approaching access points to slow vehicles as they approach the facility. The need for vehicle barriers should be determined by the Security Risk Assessment.

If the facility concludes vehicle barriers should be employed, there is a wide range of acceptable barriers to choose from. If crash barriers are utilized, the barrier ratings shall be determined by verification of actual crash data. Barriers that have not been crash tested shall not be used.

A.11.4.3 Natural Barriers

Natural barriers such as excavations, ditches, and berms can also be effective passive barriers.

A.11.5 Security Lighting

A.11.5.1 General

Adequate security lighting at the perimeter access is a deterrent to unauthorized personnel penetrating the perimeter. Lighting also assists monitoring of the perimeter and detection of attempts to breach the fence. All security lighting shall meet company or industry standards to provide proper illumination.

A.11.5.2 Standard Levels

Lighting around guard posts shall be designed to allow for visual inspection of credentials. Preferred lighting is full spectrum (white light). The lighting shall be placed to illuminate areas outside the guardhouse and prevent a visitor from seeing inside the guardhouse

A.11.5.3 Lighting in the Intruder Detection and Assessment Zone

Lighting in the intruder detection and assessment zone shall be designed to allow for observation by security personnel and Closed Circuit TV (CCTV) systems. No light fixtures should be in the field of view of CCTV cameras.

A.11.5.4 Periodic Inspection

Facilities shall periodically ensure lighting levels are adequate using a light meter and document the survey, and develop plans to inspect and maintain security lighting.

A.11.6 CCTV and Electronic Sensors

A.11.6.1 Monitoring and Video Surveillance

A properly installed and maintained CCTV system provides a cost-effective and reliable system to provide situational awareness and can be used to control access and detect potential intruders. The facility shall monitor security events by combining a variety of electronic sensors providing real-time remote alarms and images with human oversight. Facilities shall ensure that CCTV systems are monitored. The operator shall have written procedures to follow in the event of an alarm. In the event of a remote alarm or sensor is activated, the facility shall assess the incident and respond in accordance with the operators written instructions. The effectiveness of CCTV systems is greatly enhanced when it is combined with an intelligent video system that detects anomalies and triggers an alarm to alert the operator.

A.11.6.2 Integrated Technical Security System

The integrated technical security system often includes:

a) sensors;

b) CCTV or thermal imaging cameras;

c) electronic access control; and

d) a system to monitor, control, and display security event information so it can be evaluated and acted upon if necessary.

A.11.7 Futures—Additional Integration of Cyber and Physical Systems

The FSO should need to be further integrate cyber and physical security concepts as Internet of Things (IoT), the next step change in information technology, becomes reality. IoT currently lacks a definitive definition but a good working concept is an environment where everything is networked, connected to the Internet, and capable of exchanging information with other machines and/or humans. Tens of billions of IoT devices are projected to be Internet connected within the decade with this growth fueled by lower cost sensors, ubiquitous wireless networking, and consumer mobile devices. Common, everyday items like light bulbs, projectors, electric meters, and photocopiers are even now being “computerized” and networked. IoT compromises may have both cyber and physical ramifications; an attack which disables light bulbs may make a building impossible to occupy during evening hours.

The FSO should conduct risk assessments to understand the risk of IoT deployments and work with appropriate information technology personnel and supply chain to apply needed controls. At a minimum, IoT devices and networks should need to be monitored for suspicious behavior with the monitoring informed by threat modeling and integrated intelligence.

A.12 Personal Surety

A.12.1 General

This section of the plan shall describe how the facility vets its employees, contractors, and visitors prior to granting them access to the facility. When permitted by law, the facility shall ensure that appropriate background checks are conducted on all facility personnel to evaluate their suitability for admission to the facility.

Personnel surety includes confirmation of identity and credentials as listed on the application or resume. Personnel surety forms the foundation of an access control system built on trust and provides a degree of confidence that an individual is who he or she represents himself or herself to be with the skills and experience claimed. An effective personal surety program can help the hiring manager more accurately evaluate the candidates for the position and should enhance the facility's ability to deter, detect and reduce the likelihood of insider threats.

A.12.2 Employees

All personnel having unescorted access to the facility should undergo a background check to determine their suitability. The ABC Company should conduct background checks on employees and applicants who have been offered employment contingent upon successful completion of the background check.

A.12.3 Contractors

All full-time and long-term contractors having unescorted access to the facility should undergo a background check, equivalent to the background check conducted on facility employees. The contractor may conduct the background check on their employees internally or a hire a third-party. The contractor should be required to certify the background check has been completed and their employees have met the standard established by the facility. The contractors background check program should be subject to annual audit by the facility.

A.12.4 Contractor Background Screening

This background check should include the following:

a) measures designed to verify and validate identity;

b) measures designed to check criminal history;

c) measures designed to verify and validate legal authorization to work;

d) measures to validate education and prior work as appropriate;

e) motor vehicle record if the individual's position requires driving (where permitted by law); and

f) professional references, as appropriate.

The background check should involve a search of publicly or commercially available databases and repositories for jurisdictions in which an individual has worked or resided for the last 7 years. The criminal history search should be limited to convictions, outstanding warrants, pending indictments, sentencing, disposition, and dates.

Disqualifying decisions shall be made in consultation with someone in human resources or the legal department who is familiar with the facility's background check policy and relevant laws and regulations governing hiring decisions that are based on criminal history information. To avoid charges of disparate treatment or disparate impact resulting in

potential liability, the facility should consider using a two-step process to evaluate an application when the applicant has a criminal record.

In the first step the facility uses a “targeted” screen of criminal records. A “targeted” screen considers at least the nature of the crime, the time elapsed since the offense, and the nature of the job. The facility shall demonstrate that its targeted screen is always job related and consistent with business necessity.

Once the targeted screen has been administered, the facility should consider providing opportunities for individualized assessment for those people who were screened out. Using individualized assessment in this manner provides a way for employers to ensure that they are not mistakenly screening out qualified applicants or employees based on incorrect, incomplete, or irrelevant information, and for individuals to correct errors in their records.

The personal surety program shall be audited annually to verify compliance with both the FSP and all related regulations.

A.13 Security Measures for Access Control, Including Designated Public, Controlled, and Restricted Access Areas

A.13.1 General

Access Control is a process by which entry into and internal movement within the facility is managed. The FSO shall evaluate the complex in order to define and designate public access areas, secure access areas, and restricted access areas. Each area shall become progressively more restrictive, by Imposing additional security restrictions and requiring additional authorizations, for public access areas, secure areas, and restricted areas with public access areas having the least restrictions and restricted areas having the most restrictions. A key component of a successful access control program is knowing who is allowed on site. Personnel identification measures help a facility quickly determine whether or not an individual is permitted facility access.

This section of the plan shall describe how access to the facility is controlled to prevent unauthorized access and the unauthorized introduction of dangerous substances and devices intended to cause damage to persons or to the facility. The part of the plan shall focus on the identification, screening, and inspection of individuals and vehicles as they enter and exit the facility or restricted areas within the facility.

When given access to the facility’s cyber assets, external service providers, business partners, and vendors present a potential risk to the facility’s systems, information, and intellectual property. The facility shall ensure that background checks are conducted prior to granting them access to the facility’s IT infrastructure. The facility should also consider having them sign Memoranda of Agreements, Nondisclosure Agreements, Confidentiality Agreements, and Conflict of Interest Agreements.

All persons entering the facility should show valid, company or government issued photo identification (ID) to gain access. Individuals arriving by motorcycle should remove helmets to assist in identification. Security officers, or other competent authority, shall verify that the ID matches the person presenting it. While at the facility, all personnel shall possess a valid ID which shall be presented upon request by security, Facility Management, or a government representative. While conducting roving patrols, security officers or other competent authority shall challenge unknown, or suspicious individuals, to identify themselves with a photo ID. If the security officer does not know that the person has a valid business purpose at the facility, he/she shall contact FSO or Facility Management for authorization prior to entry and revoke entry until the person’s authorization can be verified.

If an individual is challenged on the premises and refuses, fails or is unwilling to identify themselves with a photo ID, this individual is immediately escorted to the FSO or security office for resolution.

At access points, conspicuous signage should be posted to demonstrated “restricted areas” and the company reserves the right at any time to conduct reasonable search and inspections of all persons, personal property, and vehicles on company premises or engaged in company business. Any person failing to consent to screening/ inspection should result in denial or revocation of authorization to facility. Employees may be subjected to disciplinary action, including discharge, and referred to law enforcement officials. All restricted areas must clearly state that unauthorized presence constitutes a breach of security.

A.13.2 Facility Employees

The facility should develop a system to control employees access to the facility and restricted areas. The system should incorporate several levels of security including but not limited by the following.

a) Facility employees should be issued keys, gate code, or badge to the security gate by the FSO or designee. He should maintain a log of personnel who have keys, gate codes, or badges issued. The security gate shall be locked or monitored at all times.

b) Facility employees who do not have keys to the security gate should show company-issued photo ID prior to entry. If the facility does not issue a company-photo ID, employees should show other valid photo ID which the FSO should verify against the list of facility employees.

c) The facility may issue photo identification badges to individuals permitted access to the facility. The facility shall verify the individual’s identity before providing the identification badge to the individual. The access control system is further enhanced and more effective if a background check is performed once the individual’s identity is confirmed.

d) The company or facility may use photo identification badges that are linked with an electronic access control system. The electronic access control system can recognize invalid or deactivated badges and can be programmed to only allow authorized personnel access to restricted areas. The access control system also maintains a record of the date and time that the badge has been used to access the facility and the specific areas within the facility.

A.13.3 Visitors

Whenever possible, visitors shall be scheduled in advance. If not, entry is not permitted until authorized by Facility Management or designee. This should ensure that visitors have a valid business purpose at the facility. Unregistered visitors should not be granted access to the facility until the sponsor is contacted and approves the visit.

a) All visitors shall show valid photo ID prior to entry.

b) Visitors shall sign the visitor log.

c) All visitors should be escorted by the sponsor at all times while inside the facility.

d) All visitors are required to enter the facility through the main gate.

e) Vehicle search procedures apply to private vehicles entering the facility.

A.13.4 Vendors/Contractors

The facility should develop a system to control Vendors and Contractors access to the facility and restricted areas. The system should incorporate several levels of security including but not limited by the following.

a) Vendors and contractors shall show valid photo ID prior to entry.

b) Vendors and contractors should be scheduled in advance. The sponsor shall provide the visitor or vendor's name to the security staff.

c) Vendors not registered in advance should not be admitted to the facility until their sponsor confirms the visit.

d) All contractors/vendors should have a comprehensive background check that is approved by the company.

e) The contractor must supply proof that the background process has been initiated.

f) The FSO should provide a list to the security officer of pre-authorized or regularly scheduled vendors.

g) Non-scheduled visits should be cleared with the FSO or Facility Management prior to entry.

h) Vehicle Search Procedures apply if private vehicles are driven into the facility.

A.13.5 Deliveries

Deliveries, especially unexpected or unscheduled deliveries, have the potential to introduce dangerous objects to the facility. All deliveries should be received and processed in accordance with this section of the plan.

a) All truck drivers shall show valid photo ID prior to entry.

b) Arriving deliveries shall be directed to an initial inspection point where security personnel can screen the delivery and inspect the delivery tickets, bills of lading, and the delivery vehicle.

c) Vehicles without a valid bill of lading should not be admitted to the facility.

d) Vehicles making an unexpected delivery shall not be admitted to the facility until the shipment is thoroughly inspected and cleared for delivery by the warehouse.

A.13.6 Government Employees

This section of the plan addresses the authority of government officials to enter the facility. In certain regulated facilities, authorized government officials may enter to inspect and audit the property, equipment, operations and records of the covered facility. The FSO should be familiar with the regulations covering the facility and authorities given to government employees to enter the facility either announced or unannounced. Each security regulation covering the facility should be listed in the plan and outline the authority granted to officials to enter the facility and list the facility's responsibilities. The government official must be authorized by the regulation, conducting official business and present a valid government organization photo ID prior to entry. Government officials, not authorized by regulation, seeking admission to the facility should be considered on a case by case basis. The FSO, facility manager, and legal counsel should be included in this discussion.

The facility manager, FSO, and legal counsel should be advised immediately of the arrival of any governmental official seeking access to the facility.

A.13.7 Vehicle and Personnel Searches

A.13.7.1 The facility may employ several procedures to screen employees and visitors, conduct searches of personnel and vehicles, and inspect packages, bags, and briefcases to deter and detect the unauthorized introduction of dangerous devices or the unauthorized removal of company assets.

a) The facility uses a variety of measures to perform screening. These measures include verification of personal identification, inspecting hand-carried items, vehicle identification and vehicle inspections. Inspections and searches shall be conducted by trained personnel familiar with company policy and legal requirements.

b) Appropriate signage stating that all persons, vehicles and personal effects are subject to search prior to entering the facility shall be placed at all access points.

c) The facility should conduct three types of searches as follows.

1) Gate Search: A Gate Search is the routine inspection of persons and vehicles entering or leaving the facility. Vehicles to be inspected shall be selected on a random basis using a random number random number generator, capable of generating numbers between 1 and 100.

I. At security condition three the facility should inspect and search 25 % of the vehicles entering the facility. Vehicles entering the facility should be selected for inspection when the number on the generator is between 1 and 25.

II. At security condition two, the facility should inspect and search 50 % of the vehicles entering the facility. Vehicles entering the facility should be selected for inspection when the number on the generator is between 1 and 50.

III. At security condition one the facility should search and inspect all vehicles

IV. The method used by the facility to search persons or vehicles on a random basis shall be structured and documented to ensure that the selection process is fair and equitable. The procedure shall be transparent and developed to limit the discretion of the searcher when selecting the person or vehicle to be searched. Every search shall be documented in such a manner to demonstrate that protocol was followed and the search was random.

2) Search for Cause: A Search for Cause is the search of a specific individual, their vehicle or possessions, who is suspected of committing a violation of company policies.

3) Contraband Items Search: A Contraband Items Search is an unannounced search of personnel, their work areas, locker rooms and/or vehicles for prohibited items.

4) The employee, contractor, or visitor must consent to the search or inspection. Failure to consent should result in denial of access, removal from the site, and, for employees, disciplinary action.

5) Inspections may include a visual inspection, trained dogs, ionic explosives detection, x-ray inspections, and metal detectors.

A.13.7.2 If a dangerous substance or device is discovered, the FSO and facility manager shall be advised immediately and ensure that the following action, as applicable, is taken:

a) evacuate the surrounding area and prevent reentry;

b) stress to all personnel not to touch or move the suspicious object;

c) prohibit the use of cell phones and radios if the suspicious object appears to be an explosive device;

d) notify police that a suspicious substance or object has been discovered and wait for them to remove the device; and

e) search to determine if additional devices or substances have been placed once the device is removed.

A.13.8 Access Control Points

Each Active Access Control Point (ACP) should be listed in the plan. ACPs are those control points used on a daily basis to control ingress/egress to the facility. The list should include a description of the operation of the ACP (e.g. chain-driven vehicle gate), hours of operation, and the security countermeasures utilized at the ACP (e.g. manned vs. unmanned countermeasures, CCTV coverage, card readers, etc.).

A.13.9 Acceptable Identification

ID cards shall be tamper-resistant and laminated with a photograph. ID cards shall show the relevant details of the holder (e.g. name, description, or other pertinent data) and are to be issued by an appropriate control authority such as the port authority, employer, or government agency. Acceptable identification includes:

a) state-issued driver's license,

b) photo ID card issued by government agency,

c) passport,

d) union photo ID card,

e) port employee photo ID card,

f) employer photo ID card.

A.13.10 Facility Access Control

A.13.10.1 Gates

Properly designed gates, in conjunction with the perimeter fence, channel both vehicles and pedestrians to a limited number of access control points where their identity can be verified before they are granted access to the facility.

a) The main gate shall be closed or monitored at all times. An automatic gate is acceptable at terminals that should have truck traffic in and out of the facility.

b) The pedestrian personnel gate shall be locked at all times. Keys shall be issued by the FSO and logged.

Example—This document contains confidential information and must be protected from unauthorized disclosure. It is not to be copied or distributed without the approval of the Facility Security Officer.

Copy number X of X.

c) Other perimeter gates shall be locked at all times. Ensure that locking gates does not interfere with emergency evacuation.

A.13.10.2 Deliveries (of Supplies and Services)

Deliveries, especially unexpected or unscheduled deliveries, have the potential to introduce dangerous objects to the facility. All deliveries should be processed in accordance with this section of the plan.

a) All packages entering or leaving the facility are subject to search. Signs are posted advising of this requirement at principal facility entry gates.

b) Deliveries shall be scheduled in advance. When not scheduled in advance, deliveries are prohibited until approved by Facility Management. The FSO, or FSO designee, should maintain a list to security of regularly authorized delivery companies having permission to bring vehicles onto the facility.

c) Acceptance of hazardous materials (supplies) is verified by the FSO, or FSO designee, as to their validity, safety, and security prior to acceptance.

A.13.10.3 Control of Automobiles and Supplier/Contractor Vehicles

Vehicles entering and exiting the facility or restricted areas within the facility will be processed in accordance with this section of the plan.

a) Automobile entry at the main facility gate is limited to government vehicles, and specified facility personnel vehicles when approved by Facility Management, and pre-approved supplier/contractors.

b) All vehicles entering or leaving the main facility gate are subject to search. Signs are posted at the main gate advising of this requirement.

c) Parking inside the facility for automobiles and supplier/contractor vehicles is restricted to specific areas.

A.13.10.4 Key/ID/Access Card Control

Keys should be issued, tracked, returned, reported lost or stolen, and policies concerning the unauthorized use of duplicate keys and loaned keys should be incorporated into this section of the plan.

a) The FSO issues keys to specific areas of the facility and keeps a log of all persons issued such keys.

b) Locks are inspected regularly and malfunctioning locks are replaced if found in bad order.

c) Only case-hardened locks and chains are used and, where used, are permanently attached to gates.

d) Facility equipment is kept inside the locked perimeter fence to avoid access by unauthorized personnel.

A.13.10.5 Security Rounds

The primary function of roving security is detection, reporting and documenting “anomalies.” All anomalies should be reported immediately to FSO or Facility Management. Facility Management should notify the company reporting hotline, and law enforcement agencies as appropriate.

a) Employees in the facility on a regular basis and should be trained to report suspicious events, activities or anomalies such as:

I. unauthorized or improperly parked vehicles on the facility;

II. unauthorized vessel moored at the facility;

III. bomb threat;

IV. suspicious persons or activity in or in the immediate vicinity of the facility;

V. loss of electrical power;

VI. discovery of unknown/suspicious package(s) on the facility;

VII. breach of perimeter fence.

b) Security rounds by security personnel should be documented in the daily patrol log. This log would include such items as the following.

c) Each perimeter access control point (both active and inactive). Each access control point should be numbered and/or named.

d) Remote facility locations not readily observed that could provide an adversary with concealment.

e) Lighting locations, particularly along the perimeter. Key security lights should be numbered and/or named.

f) Perimeter areas prone to environmental degradation (e.g. washout).

g) Location of possible Hostile Surveillance Points.

A.13.10.6 Restricted Areas

Restricted areas are areas within the facility that require a higher degree of security protection. Access to restricted areas shall be limited to employees, contractors and service personnel who have a documented need to be in the restricted area. The Facility Security Officer, may designate the entire facility as a restricted area or limit the designation to certain areas of the facility. Access shall be restricted in areas that have the potential to cause the most harm to people, the facility, and the company. In general, areas containing sensitive information, critical processes, hazardous material, process controls, etc. shall be designated as restricted areas.

This section, the plan shall clearly identify the location of these restricted areas and systems, identify which facility personnel are authorized to have access to those areas and systems, identify persons—other than facility personnel (e.g. contract technicians)—who are authorized to have access, and the conditions required to be met before access is granted to such individuals. The facility shall escort contractors, repairman, and technicians in restricted areas until they have been completely vetted. Locations within the facility that may be designated as restricted areas could include the following:

a) manufacturing or process areas and control rooms;

b) SCADA control systems, other process control systems, IT infrastructure locations;

c) systems and areas where sensitive security information is stored;

d) areas containing security equipment, surveillance equipment and their controls;

e) electrical sub-stations;

f) water supplies;

g) telecommunication system locations;

h) areas containing dangerous or hazardous substances;

i) facility offices containing critical or sensitive information;

j) pipeline manifolds;

k) pipeline pump areas;

l) critical Infrastructure (Water supply, telecommunications, electrical systems, control rooms, processing areas and access points for ventilation and air-conditioning systems).

A.13.10.7 Security Countermeasures for Restricted Areas

At restricted areas and access gates, conspicuous signage must be posted to demonstrated “restricted areas” and the company reserves the right at any time to conduct reasonable search and inspections of all persons, personal property, and vehicles on company premises or engaged in company business. Any person failing to consent to screening/inspection should result in denial or revocation of authorization to enter a company facility. The person may be subjected to disciplinary action, including discharge, and referred to law enforcement officials.

Cyber systems can be compromised not only electronically but physically and require the same or higher physical security measures needed to protect physical assets. To protect critical cyber assets the facility shall restrict access to sensitive IT areas, such as control rooms, LAN and server rooms, wiring closets and workstations operating sensitive applications such as the access control system and the CCTV monitoring area etc. Potential countermeasures may include (but are not limited to) the following.

a) Clearly mark all restricted areas that indicate access to the area is restricted and that any unauthorized access constitutes a breach of security.

b) Utilize defense in depth principles by adding additional layers of security (e.g. locked doors, fencing, barriers, badge readers, two-factor authentication, etc.).

c) Employ physical barriers to impede movement through access points.

d) Secure or eliminate all unnecessary entry points into a restricted area that are not routinely used.

e) Assign personnel to control access to restricted areas.

f) Restricted IT areas can be accessed by going over or under the buildings internal petitions such as low hanging panel ceilings or raised floors. The facility should consider protecting sensitive IT areas with true floor to true ceiling walls. An alternative is to secure the areas below the floor or above the ceiling with wire partitions and alarms to detect intrusion.

g) Conduct screening and inspections of pedestrians and vehicles entering and leaving a restricted area.

h) Patrol or monitor the perimeter of restricted areas or systems.

i) Use automatic intrusion detection devices or surveillance equipment to detect unauthorized entry or movement within restricted areas systems.

j) Direct the parking, loading, and unloading of vehicles within a restricted area.

A.14 Security Measures for Monitoring

This section of the plan shall describe how the facility is continuously monitored for unauthorized access. The facility shall implement security countermeasures that have the capability to continuously monitor the facility, its approaches on land and water (where applicable), and the restricted areas with a combination of lighting, patrols, automatic intrusion detection systems, or surveillance equipment. The FSO should ensure security monitoring at all Security Condition levels, of the following areas.

a) Facility and its approaches should be monitored by employees with security responsibilities, security guards and or CCTV coverage.

b) Restricted areas within the facility should be monitored by employees with security responsibilities, security guards or CCTV coverage.

c) Each perimeter access control point (both active and inactive).

d) Remote facility locations not readily observed that could provide an adversary with concealment.

e) Lighting locations—particularly along the perimeter.

f) Perimeter areas prone to environmental degradation (e.g. erosion).

g) Restricted areas within the facility.

h) Random patrols to detect suspicious vehicles, persons, and packages along the facility perimeter.

i) Adequate facility lighting, which is also critical for monitoring a facility against unauthorized access. All areas of the perimeter should be illuminated to the degree that suspicious persons, vehicles, or objects can be readily detected by facility personnel.

A.15 Key Control

This section of the plan should be based on a written lock and key control policy and shall describe how keys are issued, tracked, returned, reported lost or stolen, and the unauthorized use of duplicate keys and loaned keys. The locking system must be planned and administered by the FSO or his designee. The following procedures shall be incorporated into this section of the plan.

a) Distribution of keys shall be authorized in writing and entered into a Key Control Log. The log shall be a computer-based key control program.

b) Keys shall only be issued to employees and contractors who have a demonstrated need to access that area.

c) Lost or stolen keys shall be reported immediately. The security manager and the facility manager shall determine if security has been compromised and if the lock needs to be changed.

d) Employees shall not duplicate keys or loan keys to another employee. Keys shall not be left unattended; and

e) All issued keys shall be returned when an employee or contractor leaves the facility. The return keys should be validated against the Key Control Log.

f) Locks are inspected regularly and malfunctioning locks are replaced if found in bad order.

g) Only case-hardened locks and chains are used and, where used, are permanently attached to gates.

h) Facility equipment is kept inside the locked perimeter fence to avoid access by unauthorized personnel.

A.16 Security Incident Procedures

A.16.1 A security incident report is completed on all suspicious activity, breaches of security, or security incidents. Appropriate investigations are conducted by the Company Operating Security Components, Company Safety and Security, or an assigned designee.

By keeping detailed records of security incidents, corporate security and management may be able to spot trends and piece together facts that lead to successful investigations and conclusions. Security incident data may also be shared with peer groups, regulatory agencies, and law enforcement agencies for improved evaluation, monitoring, and trending of security incidents. Incident data should only be available for analysis if incidents are reported and recorded. Employees should be encouraged to report security-related incidents and events.

A.16.2 All security incidents involving company property or other crimes committed against persons must be reported immediately Examples of incidents that require immediate notification are:

a) bomb threats by mail or telephone;

b) threats or intentions to inflict injury to a person(s) or facility(s);

c) abandoned vehicles parked at or near a facility;

d) physical attacks against a person(s) or facility(s);

e) civil disturbance;

f) sabotage against company property, equipment, information systems, and manufacturing processes, which affect company production;

g) kidnapping of an employee;

h) extortion of an employee;

i) a non-employee;

j) sexual assault;

k) breach of facility access control (fake ID card, stolen ID card, etc.) by robbery;

l) trespassing;

m) vandalism;

n) loitering and/or picture taking or videotaping of a facility;

o) unknown individual(s) parking a vehicle(s) in close proximity to a facility with no apparent reason or purpose;

p) suspicious individual(s) asking questions about security or facility design;

q) arson;

r) explosion;

s) confidential information theft;

t) blackmail;

u) embezzlement;

v) bribery.

The FSO should log any security incident, breaches of security, and security incidents on a security log sheet and file the detailed report.

A.17 Audits and Security Plan Amendments

The FSO should conduct a periodic audit of the facility security plan. The FSP should be also audited if there is a change in ownership, operator, the property, physical structures, emergency response procedures, security measures, operations, or interfacing procedures. The facility may also be subject to corporate or management audits. All audit findings must be tracked until approved resolution.

If the audit identifies a weakness or gap in the FSP, the plan must be amended and tested address these weaknesses.

Example—This document contains confidential information and must be protected from unauthorized disclosure. It is not to be copied or distributed without the approval of the Facility Security Officer.

Copy number X of X.

[Example] Appendix A

Guard Force Post Orders

Insert a copy of the guard force post orders.

[Example] Appendix B

Site Maps

B. 1. General

This section of the plan shall contain detailed schematics showing the layout of the facility. 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; and

h) muster points;

i) operating units, buildings and other assets

[Example] Appendix C

Response to Changes in Alert Level

C.1 General

The company's Security Conditions system describes a progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all company facilities, assets, and personnel. The purpose of the Security Condition system is to establish standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of local management prior to and during a threat or crisis. Once one of the three Security Condition levels is declared, the associated protective measures should be implemented, as soon as possible, to the extent that they apply to the individual site or facility. Sites and facilities should coordinate Security Condition status through the corporate emergency response team (CERT) process. Measures associated with each Security Condition are not prioritized, but should be initiated concurrently, when practical. A record of specific actions taken, or to be taken, for each Security Condition measure shall be maintained by local facility management. The facility should review the suggested security measures for each Security Condition and select those that are appropriate for the facility. The list is not all inclusive and the facility may add additional measures as applicable.

This procedure is based on three levels of security depending on the potential of terrorist or other threat of unlawful activity, as communicated to the FSO by the company.

Security Condition Level 1 **Baseline Security Measures.** This condition exists when a general threat of possible terrorist activity exists, but warrants only routine security measures associated with daily operations.

Security Condition Level 2 **Elevated Threat Level.** This condition is used when an increased and more predictable threat of terrorist activity exists and may increase access controls to include additional personnel and vehicle barriers.

Security Condition Level 3 **Imminent Threat Alert.** This is the most serious condition declared in the immediate area where a terrorist attack has occurred which may affect the site or when an attack is initiated on the site. This significantly increases protective measures and may require additional protective elements along with those in Security Condition 2.

C.2 Detailed Explanation of Security Conditions and Measures

C.2.1 General

A detailed explanation of each Security Condition and security measure is illustrated in A.2.2, A.2.3, and A.2.4.

C.2.2 Security Condition 1—Baseline Security Measures

Security Condition 1 exists when a general threat of possible malevolent or terrorist activity exists, but warrants only a routine security posture. Security Condition 1 employs baseline security measures established following the SRA. This level is also known as the normal operating condition.

Measure 1. Pre-planning and reviewing of protective measures. Conspicuously post signs with language indicating "All persons are subjected to screening or inspection of person or items, and failure

to consent or submit to a screening or inspection process should result in the denial to enter a facility."

Measure 2. At regular intervals, visually examine facilities for vulnerabilities and risk.

Measure 3. Contractors and visitors shall sign-in/out when entering and exiting the facility (manned and unmanned stations) and access control shall be maintained at all times. Visitor and contractors must be clearly identified and have a legitimate business purpose for entering the facility. Deny or revoke a person's authorization to be on the facility, if the person is unable or unwilling to provide an approved form of identification.

Measure 4. Escort all visitors while inside the facility. Visually screen persons, baggage, personal effects, and vehicles, including delivery vehicle.

Measure 5. Caution employees not to talk to outside persons about the facility or security-related issues concerning the facility.

Measure 6. Secure a list of security firms or contractors that can assist with 24-hour security coverage for the facility. Communicate with company security when new contracts are necessary for additional security firms/contractors.

Measure 7. Ensure that existing security measures, such as: fencing, locks, and lighting are in place and functioning properly. Identify additional security measures and resources to enhance security for higher threat condition levels.

Measure 8. Review facility shutdown procedures with personnel on an annual basis.

Measure 9. Ensure contingency and business continuity plans are current and include a response to terrorist threats.

Measure 10. Check all security systems such as lighting and intruder alarms to ensure they are functioning. Modify lighting levels, as appropriate, to address changing security needs.

Measure 11. Ensure that a company response can be mobilized and review facility emergency plans, security plans and security procedures. Test security and emergency communications procedures and protocols.

Measure 12. Review all operations plans, personnel details, and logistics requirements that pertain to implementing a higher Security Condition.

Measure 13. Confirm availability of security resources that can assist with 24/7 coverage of critical facilities.

Measure 14. Reserve for site/facility use.

Measure 15. Require positive identification of all personnel entering the facility and limit access to only those with a legitimate and verifiable need to be in the facility.

Measure 16. Inspect the interior and exterior of buildings in regular use for suspicious activity or unattended packages at the beginning and end of each workday and at frequent intervals. Report any signs of tampering or indications of unauthorized entry.

Measure 17. Inspect other deliveries and locally designated common use facilities to identify explosives and incendiary devices. Use trained teams for some screening inspections, when available. Instruct site personnel to report suspicious packages to supervisor or security and refrain from handling them until cleared by appropriate authority.

Measure 18. Inform employees of the general threat situation. Limit visitors as much as possible. Ensure that all visitors are escorted by company personnel. Periodically update designated personnel as the situation changes to stop rumors and prevent unnecessary alarm.

Measure 19. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving their vehicle.

Measure 20. Ensure that security personnel have immediate access to building floor plans and emergency/evacuation plans for designated site facilities. Ensure that security personnel are able to seal off an area immediately. Ensure that key personnel required to implement security plans are on-call and readily available. Maintain the site emergency response team (ERT) on 2-hour recall. Review and be prepared to exercise bomb threat procedures.

C.2.3 Security Condition 2—Elevated Threat Level

Security Condition 2 applies when an increased and more predictable threat of malevolent or terrorist activity exists. The measures in this Security Condition must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, or aggravating relations with the local community. In addition to the measures required by Security Condition 1, the following measures should be implemented.

Measure 21. At regular intervals, warn all personnel to report the following people to security or to the supervisor:

a) suspicious personnel—particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about site operations or security measures;

b) unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of the site or near site facilities; and

c) abandoned parcels or suitcases; any other activity considered suspicious.

Measure 22. Secure and seal buildings, rooms, and storage areas not in regular use. Maintain a list of secured areas.

Measure 23. Increase unannounced security screenings (e.g. the inspection of personal identification documents, vehicle registration, vehicle content, suitcases, briefcases, and any other containers, etc.) at access points for the facilities.

Measure 24. Reduce the number of access points for vehicles, vessels, and personnel to minimum levels, consistent with the requirement to maintain a reasonable flow of traffic.

Measure 25. Review security measures for critical/sensitive personnel (e.g. executives, managers, members of special access/security programs, etc.) and implement additional measures warranted by the threat and existing vulnerabilities (e.g. identified personnel should alter established patterns of behavior when traveling in public areas).

Measure 26. Increase contacts with local law enforcement, intelligence community, and domestic security agencies to monitor the threat to site personnel and facilities. Notify local law enforcement agencies and the domestic security agencies concerning Security Condition 2 measures that, if implemented, could affect their operations in the local community.

Measure 27. Maintain ERT personnel on 2-hour recall; periodically exercise recall to ensure readiness. Keep other designated personnel involved in implementing special response/contingency plans on call. Identify, contact, and brief key personnel that may be required for unique contingencies; coordinate lines of communication.

Measure 28. Review provisions of all operations plans and orders, and special operating procedures associated with implementing Security Condition 1.

Measure 29. Move automobiles and objects, such as trash containers, newspaper boxes, crates, etc., at least 30 yards from designated facilities, particularly buildings of a sensitive nature. Identify any areas where an improvised explosive device could be hidden (e.g. pallet stacks, trash piles, stacked construction supplies, etc.). If the configuration of the facility or area precludes implementation of this measure, take appropriate alternative action. Consider centralized parking.

Measure 30. Secure, seal, and regularly inspect designated buildings, rooms, and storage areas that can be isolated with minimum facility impact.

Measure 31. Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. If available, have local police explosive ordinance disposal (EOD) trained teams inspect suspicious items. Provide guidance concerning suspicious packages. Encourage employees to inspect their individual mail, report suspicious items to security, and refrain from handling such items until cleared by appropriate authority.

Measure 32. Increase security force surveillance of locally designated targets to improve deterrence and build confidence among facility and vessel personnel.

Measure 33. Brief representatives of all activities on the site concerning the threat and security measures implemented in response to the threat. Explain reasons for actions. Implement procedures to provide periodic updates.

Measure 34. Verify the identity of all personnel entering the facility, and sensitive or restricted areas (e.g. inspect identification badges and grant access based on visual recognition). Visually inspect the interior of all vehicles and the exterior of designated suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of detailed inspections of suitcases, briefcases, and other containers.

Measure 35. Increase the frequency of random identity checks (inspection of security badges and vehicle registration documents).

Measure 36. Limit visitors to the facility, and confirm that visitors are expected. Search and screen all employees, contractors and visitors, boxes, suitcases, briefcases, packages, and other containers.

Measure 37. Implement additional security measures for critical/sensitive personnel in accordance with existing plans.

Measure 38. Brief designated security force personnel concerning the threat and policies governing use of force and pursuit. Ensure there is no misunderstanding of these instructions. Repeat this briefing on a periodic basis.

Measure 39. Implement business contingency and continuity plans as appropriate. Erect barriers to control direction of traffic flow. (Company safety and security has the responsibility to direct company facilities to erect barriers, upon review of any threat information or intelligence against industry.)

Measure 40. Increase contacts with local police, security agencies, and Domestic Security Agencies to monitor the threat to site personnel and facilities. Notify local police agencies of measures that, if implemented, could affect the local community. Each facility should also make an introduction with neighboring businesses to increase security and community awareness.

Measure 41. Survey the surrounding area to determine if operational activities near the area might create emergencies/contingencies that could affect the facility. (e.g. airports, government facilities, industrial facilities, railroads, etc.).

Measure 42. Reserve for facility/vessel use.

Measure 43. Secure 24/7 trained and knowledgeable personnel to perform security functions to staff the impacted facilities; ensure that all security personnel have been briefed concerning policies governing the use of force.

C.2.4 Security Condition 3—Imminent Threat Alert

This condition applies in the immediate area where a malevolent or terrorist attack has occurred that may affect the site, or when an attack is initiated on the site. Implementing this Security Condition should create hardship and affect the activities of the site and its personnel. Normally, this Security Condition is declared as a localized condition at the affected facility. The following measures should be implemented.

Measure 44. Continue all Security Condition 1 and Security Condition 2 measures, or introduce those that have not already been implemented.

Measure 45. Initiate 24-hour operation of the local Emergency Operations Center (EOC). Notify emergency response team to place the emergency strike team on standby alert. Keep designated personnel responsible for implementing special/response contingency plans at their places of duty. Review facility evacuation plans.

Measure 46. Reduce facility access points to the absolute minimum necessary for continued operation.

Measure 47. Verify the identity of all personnel entering the facilities or vessels, including appropriate off-site facilities under company control. Inspect all security badges for tampering. Visually inspect the interior of designated vehicles and the exterior of designated suitcases, briefcases, and other containers.

Measure 48. Implement centralized parking and shuttle bus service where required.

Measure 49. Ensure that designated security personnel have been briefed concerning policies governing the use of force and pursuit. Ensure that non-security supervisory personnel are familiar with the above mentioned policies and procedures, if applicable.

Measure 50. Increase security patrol activity to the maximum level sustainable.

Measure 51. Position security force personnel in the vicinity of critical facilities and restricted areas.

Measure 52. Erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.

Measure 53. Consult local authorities about closing public roads and facilities that might make sites more vulnerable to terrorist attacks.

Measure 54. Reserve for site/facility use. If intelligence or threat information is deemed credible against our industry and/or a direct threat is issued or deployed against a company facility, affected locations may be suspended or closed until the situation has been resolved and the facility is deemed safe. Closure of offices or facilities is directed by the company officers in coordination with the company security department, security threat assessment team, and the component facility management. Employees with laptops can work remotely, if instructed to do so by the component Vice President or designee.

Measure 55. Secure trained and knowledgeable personnel to perform security functions to staff the impacted facilities (as appropriate for impacted company facilities). (If this is a shared-company facility, the shared components should coordinate security efforts to ensure this measure is met.)

Measure 56. Cancel or delay all non-vital facility work conducted by contractors, or continuously monitor their work with company personnel.

Measure 57. Augment security forces to ensure absolute control over access to the site, facilities, and other potential target areas. Establish surveillance points. (If this is a shared-company facility, the shared components should coordinate security efforts to ensure this measure is met.)

Measure 58. Working closely with facility management, identify the owners of all vehicles already on the site. In those cases where the presence of a vehicle cannot be explained (owner is not present and the vehicle has no obvious site affiliation), inspect the vehicle for explosives, incendiary devices, or other dangerous items, and remove the vehicle from the vicinity of facilities and other sensitive areas, as soon as possible.

Measure 59. Inspect designated vehicles entering the site. Inspections should include cargo storage areas, undercarriage, glove boxes, and other areas where explosives, incendiary devices, or other dangerous items could be concealed.

Measure 60. Limit access to the site, facilities, and other areas to those personnel with a legitimate and verifiable need to enter. Implement positive identification of all personnel. There shall be no exceptions.

Measure 61. Inspect all baggage, such as suitcases, packages, and briefcases, brought on the site for presence of explosives, incendiary, chemical, or biological devices, or other dangerous items.

Measure 62. Implement frequent inspections of the exterior of buildings (including roof areas) and parking areas.

Measure 63. Coordinate with the emergency operations center and CERT team leader to establish communications, responsibilities, and authorities before, during, and after attack.

Measure 64. Request that local authorities close those public roads and facilities in the vicinity of the site/facilities that might facilitate execution of a malevolent or terrorist attack.

Measure 65. Reserve for site/facility use.

Measure 66. In the event of a direct threat, shut down affected facilities (or portions of facilities) and operations in accordance with established procedures unless there is a compelling reason not to and evaluate the situation before resuming operations.

Measure 67. Consult with local, state, and federal authorities for assistance on securing the facility.

[Example] Appendix D

Terms and Definitions

Insert terms and definitions here.

Bibliography

This standard was developed for the industry as an adjunct to other available references, which include the following.

[1] American Petroleum Institute, *Security Guidelines for the Petroleum Industry*, American Petroleum Institute, May 2003

[2] API Recommended Practice 70, *Security for Offshore Oil and Natural Gas Operations*, First Edition, American Petroleum Institute, April 2003

[3] API/ANSI Standard 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*, First Edition, American Petroleum Institute, May 2013

[4] *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), August 2002 [5]

[5] Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF), Sandia National Laboratories, 2002 [6]

[6] DOT 49 *CFR* 172 HM-232, U.S. Department of Transportation, 2005 [7]

[7] *Maritime Transportation Security Act of 2002*, Public Law 107-295-Nov 25, 2002 [8]

[8] Department of Homeland Security, 6 *CFR* Part 27, *Chemical Facility Anti-Terrorism Standards*, Final Rule [9]

[9] Pipeline Security Information Circular, *Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities*, U. S. Transportation Security Administration, 2002 [10]

[10] SPC-1.2009, *Organizational Resilience, Security, Preparedness, and Continuity Management Systems, Requirements with Guidance for Use*, ASIS, 2009

[11] *National Infrastructure Protection Plan*, Department of Homeland Security, 2009

[12] *DHS Risk Lexicon*, 2010 Edition, Risk Steering Committee, U.S. Department of Homeland Security, September 2010

[13] *Chemical Facility Vulnerability Assessment Methodology*, NIJ Special Report, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, July, 2002 [11]

[14] CSA Z246.1-09, *Security Management for Natural Gas and Petroleum Industry Systems*, CSA, 2009 [12]

[15] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*

---

5 American Institute of Chemical Engineers, Center for Chemical Process Safety, 3 Park Avenue, 19th Floor, New York, New York 10016, www.aiche.org/ccps.

6 Sandia National Laboratories, 1515 Eubank SE, Albuquerque, NM 87123.

7 Department of Transportation. The *Code of Federal Regulations* is available from the U.S. Government Printing Office, Washington, D.C. 20402. www.gpoaccess.gov.

8 U.S. Coast Guard Marine Safety Center (part of DOT), 2100 Second Street, S.W., Washington, DC 20593, www.uscg.mil.

9 U.S. Department of Homeland Security, Infrastructure Security Compliance Division (ISCD), 1421 Jefferson Davis Highway, Arlington, VA 22202.

10 U.S. Department of Homeland Security, Transportation Security Administration, 601 South 12 Street, Arlington, VA 20598.

11 National Institute of Justice, 810 Seventh Street, NW, Washington, D.C. 20531, www.nij.gov.

12 Canadian Standards Association, 178 Rexdale Boulevard, Toronto, ON, Canada M9W 1R3.

[16] Fey, J. J. (1999), *Model Security Policies, Plans and Procedures*, Burlington, MA, Butterworth-Heinemann [13]

[17] American Society for Industrial Security (2011), P*rotection of Assets—Applications*. Alexandria, VA, ASIS International [14]

[18] American Society for Industrial Security (2011), *Protection of Assets—Security Management*, Alexandria, VA, ASIS International.

[19] American Society for Industrial Security (2011), Protection of Assets—Physical Security, Alexandria, VA, ASIS International.

[20] Garcia, Mary Lynn (2006), *Vulnerability Assessment of Physical Security Systems*, Burlington, MA, Butterworth-Heinemann.

[21] Norman, Thomas L, CPP/PSP/CSC (2010), Risk Analysis and Security Countermeasures Selection, Boca Raton, Florida: CRC Press, Taylor and Francis Group [15]

[13] Butterworth-Heinemann, 200 Wheeler Rd., Burlington, MA 01803.
[14] ASIS International, 1625 Prince Street, Alexandria, Virginia 22314-2882, www.asisonline.org.
[15] CRC Press, Taylor and Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, Florida 33487.

AMERICAN PETROLEUM INSTITUTE

1220 L Street, NW
Washington, DC 20005-4070
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

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	

Information about API publications, programs and services is available on the web at www.api.org.

Product No. K78101