Integrated Automation and Security for an LNG Offshore Terminal

Faced with declining natural gas production in the Gulf of Mexico and elsewhere domestically, there is a growing awareness that Liquefied Natural Gas (LNG) imports will be needed to meet future natural gas demand in the US. Due to its nature, LNG and the regasification facilities are perceived as a risk for cryogenic spill, gas release, explosion, fire, and as a target for a terrorist attack. With persistent public concerns about LNG safety – and now security – Congress has reviewed the safety and security provisions in the federal LNG regulations. To meet public concerns Congress has directed the U.S. Coast Guard (USCG), under the Department of Homeland Security, to produce and enforce regulations to address safety, environmental and security requirements for U.S. offshore oil and gas production facilities. The USCG currently maintains and enforces two sets of regulations which address maritime security; one for docks, and one for offshore oil and gas production facilities. Neither of these specific sets of regulations addresses offshore LNG regasification terminals directly. However, both sets of regulations require that these facilities meet minimum security requirements and have an approved security plan in place before they are allowed to operate. This paper is written to:

- Provide our understanding of the regulatory environment which will apply to this facility.
- Give guidance on what should be considered for a security system for an offshore regasification facility.
- Offer an overview of the technology that is available to meet the security regulations.
- Present our thoughts on the steps to developing a security solution that make sense for an offshore regasification facility.

This paper is based on Front End Engineering Design (FEED) work recently performed by J. Ray McDermott Engineering – Houston for an offshore LNG terminal located in federal waters in the Gulf of Mexico.
During the review of our client’s preliminary security plan, we identified specific implementation requirements for the security system for the LNG regasification terminal. Their plan included several systems not normally required for a typical facility in the Gulf of Mexico. Our proposed solution for the site went beyond a simple closed circuit television (CCTV) system with random surveillance cameras, and included identification cards, perimeter monitoring, RADAR, and personal identity recording. We recommended a comprehensive security solution to meet federal regulatory requirements and to provide a security environment that protects the owner's assets.

Introduction

Security implementation on large offshore oil and gas production facilities is significantly different from similar onshore facilities. Offshore facilities carry a minimum number of staff and each staff member wears multiple hats. Onshore facilities typically have different personal for process-operation, maintenance, and administration as well as other tasks. Typically, offshore facility operators perform maintenance functions as well as the process-operation tasks. The facility we have been designing consists of one platform for the living quarters, another platform for the regasification facility, two gravity structures for the storage tanks, and an unloading platform. The staffing requirement varies according to facility size and complexity, so that one solution does not fit all facilities.

There are approximately 4,400 offshore production facilities (primarily oil and gas) in the Gulf of Mexico. The USCG regulations 33 CFR 106, Marine Security: Outer Continental Shelf (OCS) Facilities, requires approximately 49 of them to have approved security plans and operate under a Declaration of Security. Offshore LNG regasification terminals will be among those required to have an approved security plan and Declaration of Security in place.

Adding security requirements to an offshore facility means either adding additional personnel or adding security responsibilities to the limited-size staff that is already wearing multiple hats. This forces us to think about how best to meet these requirements. One solution is to have the operators learn a completely new security system on top of their day-to-day job. We also had to consider the additional footprint requirements for the security workstations. Offshore the footprint for a workstation is worth approximately $10,000, if you have to make the platform larger for the additional space, then the cost could be millions. Our solution is to integrate the control system and the security system so that operators have as few new tools to learn as possible. Our goal is to make security and operational functions fit together like hand and glove so that, when a security event comes up, operators get the security information they need in a manner similar to how they get normal operating information.
The client nominated Honeywell’s Experian PKS™ and its human-machine interface (HMI) as the facility’s process-control platform. Therefore, our design is to use the same Experian HMI for the security system.

**USCG Requirements**


The FEED facility is 11 miles offshore. There is a question as to which set of regulations would apply. That confusion seems to have been cleared up in recent testimony before Congress by the Commandant of the U.S. Coast Guard - from this our understanding is that the Coast Guard intends to use 33 CFR 106 as the basis for LNG terminal security requirements. The USCG is currently preparing a Navigation and Vessel Inspection Circular (NAVIC) to provide clarity to the security requirements for an offshore regasification terminal. Thus, our design conforms to 33 CFR Part 106, but could readily be adapted to meet 33 CFR Part 105. A copy of 33 CFR Part 106 is included with this paper as Appendix A.

Under 33 CFR 106, your facility has to have an approved security plan, you have to train the people on the facility to use the plan, you have to then practice that plan with drills and exercises, and finally, you have to maintain records of everything that has gone on. After fulfilling these requirements, you can get a Declaration of Security from the USCG.

The facility security plan must address the following:

- Deter unauthorized introduction of dangerous substance and devices on to the facility;
- Secure dangerous substances and devices that are authorized by the facility owner and operator to be onboard;
- Control access to the facility;
- Allow temporary continuous access to personnel and visitors through the use of badges and/or other systems to verify their identity;
- Identify access points that must be secured or attended to deter unauthorized access;
- Lock or otherwise prevent access to unattended spaces that adjoin areas to which facility personnel and visitors have access;
• Ensure that facility personnel are not required to engage in or be subjected to screening of personnel or personal effects unless required for security clearance;
• Provide designated secure areas on board;
• Respond to presence of unauthorized personnel onboard.

General Considerations

An offshore production facility is a unique environment. The limited staff typically works a 12-hour shift seven days a week. When they finished their shift, they don’t go home. They remain on that facility 24 hours a day during their tour of duty, which is typically two weeks on/two weeks off.

Remote Monitoring

In the Gulf of Mexico there will be times, such as a tropical storm or hurricane enters the Gulf, when personnel have to be evacuated from the platform for safety reasons. LNG boils at approximately -280°F, therefore, it is essential that certain cryogenic portions of the regasification facility remain in service. If this cannot be done then the evolving gas is vented to the atmosphere and the restart of the facility requires more involved (and potentially hazardous) procedure. A well thought out security system provides the means for operating personnel to monitor the minimum operations on the evacuated platforms and to monitor for unauthorized access.

Integrated HMI

Since operating personnel on a facility multitask, it is important that the control system and the security system have an HMI with a look and feel that minimizes training requirements. Another consideration impelling us to integrate the security HMI into the process operation HMI is that the security HMI will be most needed in high-stress situations. Providing operators with a familiar look and feel reduces the chance of task-overload-induced errors. Finally, integrating the security system HMI with the process system HMI facilitates compliance with security procedures. If good security practice is integrated with process operation routine, it becomes automatic.

Networked Security

Figure 1 shows the architecture under consideration for the security system. Overall, it is built around a facility-wide Ethernet network with workstations running Experian PKS incorporating Honeywell’s security system hardware and software, integrating them so that operators can view both process and security information
via a single HMI.

The control system and the security system use separate Ethernet networks in a modified star topology with a backbone of interconnected switches. To ensure the security of the information and control of the facility the control system and the security system networks are segregated from each other as well as from the onshore facilities by firewalls and other security means. The security system information is communicated to the control system for display and control via a security server acting as a gateway. The control system has a server which acts as a gateway to the control system.

The security system switches sit at the center of a star-shaped constellation of nodes. A security system node can be a server, smart camera, an analog camera digitizer, RADAR, or security gate. Nodes can be networks themselves. For example, for a CCTV system using analog cameras, a security server may control monitors and recording equipment. This is itself a node on the network. In this way, authorized personnel have the ability to view pickups from any camera on any workstation.

The Experian PKS workstation HMI resides on the control system network and it is from the Experian PKS workstation that the operator monitors information and can
take action as required. There will be a few specialized security workstations to perform supervisor level operations such as granting authorization to a new person. It is the same philosophy used with the safety system. The operator can view the status of the safety system and of the safety logic on the operator workstation, but they cannot make any changes, adds or deletes from the operator workstation. The system architecture requires anyone needing to make a change to go to the safety system engineering workstation for those actions.

We have applied the same philosophy to the security system. Personnel will need to go to the security-system engineering workstation to create badges and temporary passes, etc. This applies a management authorization step to any changes to the security or to the safety system.

**Available Technologies**

Security systems rely on a wide range of technologies to detect threats. Each security node in the system may utilize different technologies to provide its function.

*Personnel Monitoring*

It is important to identify and track personnel as they move on and off the facility via a badge/key card system. This system provides access for people authorized to go into different areas. The “badge/key” does not necessarily have to be an actual badge pinned to someone’s jacket, or a key hanging from a lanyard around their neck. A more viable system might take advantage of biometrics, such as voice recognition, thumbprints, etc.

*CCTV*

Until recently, the highest of high-tech security monitoring was closed-circuit television (CCTV). CCTV elements include cameras, TV monitors, recorders, coaxial cables to interconnect them and switch to route the signals. Since the regasification facility is made up of multiple platform, living quarters, regasification, storage, and unloading, a large number of cameras are required to cover all areas of concern. These include:

- Access points, such as docks;
- Corridors, stairwells and bridges within the facility;
- Compartments where unauthorized personnel might hide;
- Critical process areas, such as motor control centers, emergency generators, control panels, or cryogenic process;
- Peripheral areas, such as platform legs.
The advantage CCTV brings is flexibility. By extending the operators’ vision to remote locations, CCTV allows them to perceive threats that nobody has foreseen. It also exploits human operators’ ability to recognize features. An operator glancing at a monitor showing a person walking through a pump room can instantly recognize whether that person is one who goes into that particular area in the normal course of their duties, or someone who has no business being there at all.

CCTV combines aspects of safety as well as security. For example, a camera in a stairwell would instantly show a person who has fallen when otherwise it might be hours before anyone found them.

In the recent past the question for CCTV has been color or back and white? Today CCTV cameras can detect images at multiple wavelengths and lighting levels. One now has to consider not only black and white or color, but low light, Infrared, and thermal imaging.

Color visible light cameras are excellent for providing high-definition images in full daylight. Black and white cameras are excellent in both full daylight and in low light conditions. Many color cameras work in low light conditions by automatically switching to back and white image mode in low light.

When ambient light is not available or not sufficient, infrared (IR) cameras are required. An IR camera uses an infrared light source to illuminating the area, thus allowing the camera to see an object.

Thermal imager cameras use the natural temperature differences between objects to display them, displaying differential infrared emissions. All objects such as shorelines or floating objects have a certain temperature (heat signature) that is the result of daytime heat absorption. Other objects such as people, motors, buildings or boats have their own heat signature. Thermal sensors detect the difference between the heat signature of any object and the surrounding area or other objects. These differences are projected onto a detector with "hot" objects giving a bright area and "cool" objects giving a dark area, producing an image that resembles a photographic negative.

Fog renders visible light cameras blind, the infrared (IR) and the thermal imaging cameras provide a solution to this problem. Factors which equalize or mask the heat signature of different objects such as dense fog, heavy rain or heavy spray or even the length of time after sunset can significantly reduce the effectiveness of thermal imaging. To improve performance of the CCTV the combination of thermal imaging cameras with IR or low light visible cameras can overcome the limits of unaided vision.
In addition to the expansion of camera sensing technology, smart cameras have become available. The smart camera has been developed to respond to changes in the observed environment. The smart cameras have microprocessors built into them allowing them to be nodes on the network through built-in Ethernet ports.

Emerging imaging technology is also being applied to security systems. CCTV images are either obtained from an analog camera whose signal is converted to digitized video or from a Smart camera that provides digital video directly. The digitized images can be analyzed to determine if an object has moved in or out of a selected area. Security servers use motion algorithms to analyze the digitized video. The motion software provides alerts to the operators. The operator can then investigate the alert. Honeywell Security Systems provides such technology from their commercial and industrial security division. This technology is being used in many locations such as airports to help monitor security personal to ensure that they are at their post. At an offshore facility it could alert an operator to an intruder under a platform. The algorithm could be trained to differentiate between a wave and an individual moving into an area that they should not be in and alert the operator to the intrusion.

Access Gates

The federal regulation requires access control to the facility in general and to selective areas within the facility. There are two possible solutions to this issue: by policy or by physical means such as access gates and doors. Personal at the facility have to be trained in the facility policies and procedures. Traditionally on offshore oil and gas production facilities, non-operating staff is limited in their access rights. In the design, access points such as boat landings and helidecks are monitored visually and may have manually locked gates. Equipment and telecommunication room, Motor Control Centers, and Substation doors are locked. If this is acceptable to the regulatory authority then the requirements for access control have been met.

Another operations issue that was considered for an LNG regasification terminal is that every four days an LNG carrier will arrive to offload its cargo. There is a possibility that a ship’s crew member or passenger could disembark and gain access to the facility. For this reason we have considered the addition of access gates within the facility. The number and location will be determined during detail design and review by the regulatory authority. When adding security gates, facility operations and response to process upsets and emergencies must also be considered. The facility has a safety instrumented system to monitor the process for hazardous process conditions, fire, or the release of gas. If a hazardous condition occurs, consideration should be given to allowing the safety system to unlock access gates and door locks to facilitate personal evacuation and emergency
response. A balance must be struck between security and safety.

**Perimeter Monitoring**

Unlike an onshore facility, access to an offshore LNG terminal is restricted by location. For an offshore facility there are two means of access to the facility - by helicopter or by boat. Considering that the lower levels of the platform are subject to tidal and storm waves, fences are typically not considered. Therefore, the fiber optic based intrusion alert systems have not been considered. Area monitoring will be based on video cameras with the possible use of video-intrusion software to assist the operator, RADAR and personal awareness.

The LNG regasification facility will have an exclusion zone around it. This area will be noted on the navigational charts. Fishing and boat traffic are required to avoid this area. To monitor the exclusion zone active RADAR will be employed to monitor and track all traffic around and within the exclusion zone.

Another technology that is available is underwater sonar surveillance. We have discounted this as being subject to numerous false positives. The facility is in an area that is rich with sea life. Since a dolphin is about the size of a man, a sonar system would be hard put to differentiate a dolphin from a man – thus limiting the usefulness of the technology.

**Consultants**

While not a technology *per se*, employing security consultants is a very important in developing the security system. During the FEED, several security consultants were interviewed. The project execution plan includes the use of security consultants during detail design and construction. We were able to draw on the expertise of consultants who have broad (and often classified) experience with security issues.

**Development Process**

A summary of the lesson learned regarding the development of a security system for an LNG regasification facility can be broken down in to five major steps.

*Determine your regulatory requirements* – In this case, the basic requirements were defined by the relevant federal regulations. For an offshore facility, USCG is the pivotal agency. It was necessary to determine from the USCG which regulations they would apply to our facility.

*Determine your general requirements* – Despite the fact that system-component
salespeople often deride customers for claiming "My situation is different," most situations really are the same, "except" – and it is the details that must be considered. Each offshore facility is going to have a different location, personnel count, layout, equipment complement, and many other attributes that set it apart from similar facilities. It is important to identify those characteristics of your facility that are similar to and different from other facilities that might be used as models. Look especially for constraints that will affect how your security system can operate.

Review available technologies – Available technologies include not only what security cameras and fingerprint readers are available (those are end effectors at your system’s periphery), but computer software and hardware to process the information your system collects and network-communications technology that helps you make sense of it. Look at earlier technology that might be a robust solution for part of your system as well as technology in development that might be ready by the time you’re ready to install your system.

Develop a strategy – In our case, we found that our customer was already committed to using Honeywell’s Experion PKS for their process control. PKS’ flexibility and integrability with other systems made our strategy of integrating the security system tightly with the process control system viable. That PKS is effective in a networked environment led us to use the relatively new security-network paradigm for the system architecture.

Teamwork – Security systems by their nature interact with people’s lives. The development of a workable security system requires the involvement of operating personnel, maintenance personnel, engineering, risk management specialists, Health-Safety-Environmental specialists, Human Resources specialists, corporate security specialists, security consultants, and regulatory agencies. We relied on Honeywell Experion experts as well as outside consultants and our own in-house expertise to ensure the best possible decisions at every step of the way. At every stage, the project team was large, varied and well qualified.

Results

At the end of the FEED the design has not been finalized. The framework of the security system has been identified. Issues remain on the number and type of sensors to be used, what security issues will be handled by policy or technology. These will be determined during detail design. The largest unknown is how the existing federal regulations will be applied to an LNG regasification terminal. The forthcoming NAVIC is expected to address this issue.

The result of the FEED and our approach for the security system is a clear path
forward to providing a security system that is integrated into the operator’s work tools. Second, by carefully reviewing the regulatory requirements, we are sure that the system we are proposing has an excellent chance of being approved. Third, our methodical process has allowed us to prepare a ±10% estimate based on a rational list of available technical solutions needed to implement the security plan. The system, as planned, has the flexibility to incorporate new technologies and sensors as they become available without a complete redesign.

The bottom line is:

A methodical development process can reduce the risk for the project team going for funding. Having a good project definition helps ensure success.

J. Ray McDermott Engineering-Houston is currently involved on an offshore LNG Regasification Terminal FEED to be located in the Gulf of Mexico. McDermott is a leading worldwide marine solutions company. Services include engineering, design, fabrication, transportation and installation of offshore platforms, and installation of offshore pipelines. Engineering and fabrication facilities are located in the Americas, Middle East, Caspian and Asia-Pacific.

About the Speakers

**Randy Marek, P.E., J. Ray McDermott Engineering**

Randy Marek is the Automation Section Leader for J. Ray McDermott Engineering, Houston, Tex. and is responsible for overseeing all project control systems. He works with the client and project teams to develop conceptual designs and implementation plans for control systems to meet project needs for process, safety, and regulatory requirements. Randy has been practicing for 27 years in the areas of process design, instrument engineering, process control system engineering, safety system engineering, and application of advanced process controls. Randy has a Bachelor of Science in Chemical Engineering from the University of Houston, Victoria, Texas, 1978. He is a Registered Professional Engineer in Control Systems in Texas, as well as a member of the 2005 Texas Control System Exam Committee and a Senior Member of ISA.

**Stephen Gorgey, P.E., J. Ray McDermott Engineering**

Stephen is a Senior Consultant for Instrument Engineering at J. Ray McDermott Engineering, Houston, Tex. with more than 25 years of instrumentation and controls experience in process automation for the oil & gas industry and nuclear, coal-fired, gas-fired, and hydroelectric power generation. His duties include providing
specifications for instrumentation and automated controls systems for offshore oil and gas facilities, managing instrument data using instrument-design software packages, manipulating project electronic data in the export and population of customer instrument databases, performing factory and onsite precommissioning inspections of supplier-furnished distributed control systems, reviewing instrument supplier design documentation for compliance with project specifications, and preparing manhour estimates, reports, and supplier bid package evaluations. He earned a Certificate in Nuclear Engineer at Sir Sanford Flemming College, Peterborough, Ontario and a Higher National Certificate in Electrical/Mechanical Engineering in Melbourne, Australia.
Appendix A: 33CFR Part 106

Title 33--Navigation and Navigable Waters

Chapter I--Coast Guard, Department of Homeland Security

Part 106: Marine Security: Outer Continental Shelf (OCS) Facilities

Subpart A: General

Sec.
106.100 Definitions.
106.105 Applicability.
106.110 Compliance dates.
106.115 Compliance documentation.
106.120 Noncompliance.
106.125 Waivers.
106.130 Equivalents.
106.135 Alternative Security Program.
106.145 Right to appeal.

Subpart B: Outer Continental Shelf (OCS) Facility Security Requirements

106.200 Owner or operator.
106.205 Company Security Officer (CSO).
106.210 Facility Security Officer (FSO).
106.215 Company or OCS facility personnel with security duties.
106.220 Security training for all other OCS facility personnel.
106.225 Drill and exercise requirements.
106.230 OCS facility recordkeeping requirements.

[[Page 383]]

106.235 Maritime Security (MARSEC) Level coordination and
implementation.

106.240 Communications.
106.245 Procedures for interfacing with vessels.
106.250 Declaration of Security (DoS).
106.255 Security systems and equipment maintenance.
106.260 Security measures for access control.
106.265 Security measures for restricted areas.
106.270 Security measures for delivery of stores and industrial supplies.
106.275 Security measures for monitoring.
106.280 Security incident procedures.

Subpart C_Outer Continental Shelf (OCS) Facility Security Assessment (FSA)

106.300 General.
106.305 Facility Security Assessment (FSA) requirements.
106.310 Submission requirements.

Subpart D_Outer Continental Shelf (OCS) Facility Security Plan (FSP)

106.400 General.
106.405 Format and Content of the Facility Security Plan (FSP).
106.410 Submission and approval.
106.415 Amendment and audit.


Source: USCG-2003-14759, 68 FR 39345, July 1, 2003, unless otherwise noted.

Subpart A_General

Sec. 106.100 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

Sec. 106.105 Applicability.

The requirements in this part apply to owners and operators of any
fixed or floating facility, including MODUs not subject to part 104 of this subchapter, operating on the Outer Continental Shelf (OCS) of the United States for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N, that meet the following operating conditions:

(a) Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more;
(b) Produces greater than 100,000 barrels of oil per day; or
(c) Produces greater than 200 million cubic feet of natural gas per day.

Sec. 106.110 Compliance dates.

(a) On or before December 31, 2003, OCS facility owners or operators must submit to the cognizant District Commander for each OCS facility--
(1) The Facility Security Plan described in subpart D of this part for review and approval; or
(2) If intending to operate under an approved Alternative Security Program, a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.
(b) On or before July 1, 2004, each OCS facility owner or operator must be operating in compliance with this part.
(c) OCS facilities built on or after July 1, 2004, must submit for approval an FSP 60 days prior to beginning operations.


Sec. 106.115 Compliance documentation.

Each OCS facility owner or operator subject to this part must ensure before July 1, 2004, that copies of the following documentation are available at the OCS facility and are made available to the Coast Guard upon request:

(a) The approved Facility Security Plan (FSP) and any approved revisions or amendments thereto, and a letter of approval from the cognizant District Commander dated within the last 5 years;
(b) The FSP submitted for approval and current written acknowledgment from the cognizant District Commander, stating that the Coast Guard is currently reviewing the FSP submitted for approval and that the OCS facility may continue to operate so long as the OCS
facility remains in compliance with the submitted FSP; or

(c) For OCS facilities operating under a Coast Guard-approved Alternative Security Program as provided in Sec. 106.135, a copy of the Alternative Security Program the OCS facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in Sec. 101.120(b)(3) of this subchapter, and a letter signed by the OCS facility owner or operator, stating which Alternative Security Program the OCS facility is using and certifying that the OCS facility is in full compliance with that program.


Sec. 106.120 Noncompliance.

When an OCS facility must temporarily deviate from the requirements of this part, the OCS facility owner or operator must notify the cognizant District Commander, and either suspend operations or request and receive permission from the District Commander to continue operating.


Sec. 106.125 Waivers.

Any OCS facility owner or operator may apply for a waiver of any requirement of this part that the OCS facility owner or operator considers unnecessary in light of the nature or operating conditions of the OCS facility. A request for a waiver must be submitted in writing with justification to the cognizant District Commander. The cognizant District Commander may require the OCS facility owner or operator to provide additional data for use in determining the validity of the requested waiver. The cognizant District Commander may grant a waiver, in writing, with or without conditions only if the waiver will not reduce the overall security of the OCS facility, its personnel, or visiting vessels.

Sec. 106.130 Equivalents.
For any measure required by this part, the OCS facility owner or operator may propose an equivalent, as provided in Sec. 101.130 of this subchapter.

Sec. 106.135 Alternative Security Program.

An OCS facility owner or operator may use an Alternative Security Program approved under Sec. 101.120 of this subchapter if:
(a) The Alternative Security Program is appropriate to that OCS facility;
(b) The OCS facility does not serve vessels on international voyages; and
(c) The Alternative Security Program is implemented in its entirety.


All OCS facility owners or operators subject to this part must comply with any instructions contained in a MARSEC Directive issued under Sec. 101.405 of this subchapter.

Sec. 106.145 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in Sec. 101.420 of this subchapter.

Subpart B_Outer Continental Shelf (OCS) Facility Security Requirements

Sec. 106.200 Owner or operator.

(a) Each OCS facility owner or operator must ensure that the OCS facility operates in compliance with the requirements of this part.
(b) For each OCS facility, the OCS facility owner or operator must:
(1) Define the security organizational structure for each OCS Facility and provide each person exercising security duties or responsibilities within that structure the support needed to fulfill those obligations;
(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS Facility and identify how those officers can be contacted at any time;
(3) Ensure that a Facility Security Assessment (FSA) is conducted;
(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);
(5) Ensure that the OCS facility operates in compliance with the approved FSP;

(6) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(7) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required by the FSP for the new MARSEC Level;

(8) Ensure all breaches of security and security incidents are reported in accordance with part 101 of this subchapter; and

(9) Ensure consistency between security requirements and safety requirements.


Sec. 106.205 Company Security Officer (CSO).

(a) General. (1) An OCS facility owner or operator may designate a single CSO for all its OCS facilities to which this part applies, or may designate more than one CSO, in which case the owner or operator must clearly identify the OCS facilities for which each CSO is responsible.

(2) A CSO may perform other duties within the owner’s or operator’s organization, including the duties of a Facility Security Officer, provided he or she is able to perform the duties and responsibilities required of the CSO.

(3) The CSO may delegate duties required by this part, but remains responsible for the performance of those duties.

(b) Qualifications. The CSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Security administration and organization of the OCS facility;

(2) OCS facility and vessel operations and conditions;

(3) OCS facility and vessel security measures including the meaning and consequential requirements of the different MARSEC Levels;

(4) Emergency preparedness and response and contingency planning;

(5) Security equipment and systems and their operational limitations;

(6) Methods of conducting audits, inspection, control, and monitoring; and

(7) Techniques for security training and education, including
security measures and procedures.

(c) In addition to the knowledge and training in paragraph (b) of this section, the CSO must have general knowledge, through training or equivalent job experience, in the following, as appropriate:

(1) Relevant international conventions, codes, and recommendations;
(2) Relevant government legislation and regulations;
(3) Responsibilities and functions of other security organizations;
(4) Methodology of Facility Security Assessment.
(5) Methods of OCS facility security surveys and inspections;
(6) Handling sensitive security information (SSI) and security related communications;
(7) Knowledge of current security threats and patterns;
(8) Recognition and detection of dangerous substances and devices;
(9) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
(10) Techniques used to circumvent security measures;
(11) Methods of physical screening and non-intrusive inspections; and
(12) Conducting and assessing security drills and exercises.

(d) Responsibilities. In addition to any other duties required by this part, for each OCS facility for which the CSO is responsible, the CSO must:

(1) Keep the OCS facility apprised of potential threats or other information relevant to its security;
(2) Ensure that a Facility Security Assessment (FSA) is carried out in compliance with this part;
(3) Ensure that a Facility Security Plan (FSP) is developed, approved, maintained, and implemented in compliance with this part;
(4) Ensure that the FSP is modified when necessary to comply with this part;
(5) Ensure that OCS facility security activities are audited in compliance with this part;
(6) Ensure the timely correction of problems identified by audits or inspections;
(7) Enhance security awareness and vigilance within the owner's or operator's organization;
(8) Ensure relevant personnel receive adequate security training in compliance with this part;
(9) Ensure communication and cooperation between the OCS facility and

[[Page 386]]
vessels that interface with it, in compliance with this part;

(10) Ensure consistency between security requirements and safety requirements in compliance with this part;

(11) Ensure that if a common FSP is prepared for more than one similar OCS facility, the FSP reflects any OCS facility specific characteristics; and

(12) Ensure compliance with an Alternative Security Program or equivalents approved under this subchapter, if appropriate.


Sec. 106.210 OCS Facility Security Officer (FSO).

(a) General. (1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO of each such OCS facility.

(2) The same person may serve as the FSO for more than one OCS facility, provided the facilities are within a reasonable proximity to each other. If a person serves as the FSO for more than one OCS facility, the name of each OCS facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each OCS facility for which he or she is the FSO.

(3) The FSO may assign security duties to other OCS facility personnel; however, the FSO remains responsible for these duties.

(b) Qualifications. The FSO must have general knowledge, through training or equivalent job experience, in the following:

(1) Those items listed in Sec. 106.205(b), and as appropriate Sec. 106.205(c), of this part;

(2) OCS facility layout;

(3) The FSP and related procedures; and

(4) Operation, testing and maintenance of security equipment and systems.

(c) Responsibilities. In addition to any other responsibilities specified elsewhere in this part, the FSO must, for each OCS facility for which he or she has been designated:

(1) Regularly inspect the OCS facility to ensure that security measures are maintained in compliance with this part;

(2) Ensure the maintenance of and supervision of the implementation of the FSP, and any amendments to the FSP, in compliance with this part;

(3) Ensure the coordination and handling of stores and industrial supplies in compliance with this part;
(4) Where applicable, propose modifications to the FSP to the Company Security Officer (CSO);

(5) Ensure that any problems identified during audits or inspections are reported to the CSO, and promptly implement any corrective actions;

(6) Ensure security awareness and vigilance on board the OCS facility;

(7) Ensure adequate security training for OCS facility personnel in compliance with this part;

(8) Ensure the reporting and recording of all security incidents in compliance with this part;

(9) Ensure the coordinated implementation of the FSP with the CSO;

(10) Ensure that security equipment is properly operated, tested, calibrated and maintained in compliance with this part;

(11) Ensure consistency between security requirements and the proper treatment of OCS facility personnel affected by those requirements;

(12) Ensure that occurrences that threaten the security of the OCS facility are recorded and reported to the CSO;

(13) Ensure that when changes in the MARSEC Level are attained they are recorded and reported to the CSO, OCS facility owner or operator, and the cognizant District Commander; and

(14) Have prompt access to a copy of the FSA, along with an approved copy of the FSP.

Sec. 106.215 Company or OCS facility personnel with security duties.

Company or OCS facility personnel responsible for security duties must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current and anticipated security threats and patterns.

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Recognition of techniques used to circumvent security measures;

(e) Security related communications;

(f) Knowledge of emergency procedures and contingency plans;

(g) Operation of security equipment and systems;

(h) Testing, calibration, and maintenance of security equipment and systems;

(i) Inspection, control, and monitoring techniques;
Sec. 106.220 Security training for all other OCS facility personnel.

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

(a) Relevant provisions of the Facility Security Plan (FSP);
(b) The meaning and the consequential requirements of the different MARSEC Levels including emergency procedures and contingency plans;
(c) Recognition and detection of dangerous substances and devices;
(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and
(e) Recognition of techniques used to circumvent security measures.

Sec. 106.225 Drill and exercise requirements.

(a) General. (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the FSO reports attainment to the cognizant District Commander.

(b) Drills. (1) From the date of the FSP approval, the FSO must ensure that at least one security drill is conducted every 3 months. Security drills may be held in conjunction with non-security drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the OCS facility, OCS facility
personnel changes, the types of vessels calling at the OCS facility, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of appropriate authorities.

(3) If a vessel is conducting operations with the OCS facility on the date the OCS facility has planned to conduct any drills, the OCS facility may include, but cannot require, the vessel or vessel personnel to participate in the OCS facility's scheduled drill.

(c) Exercises. (1) From the date of the FSP approval, exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;
(ii) Tabletop simulation;
(iii) Combined with other appropriate exercises held; or
(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the Facility Security Plan and must include substantial and active participation of relevant company and OCS facility personnel, and may include governmental authorities and vessels depending on the scope and the nature of the exercise.


Sec. 106.230 OCS facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized access, deletion, destruction, amendment, and disclosure.
The following records must be kept:

(1) Training. For training under Sec. 106.215, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) Drills and exercises. For each drill or exercise, the date held, a description of the drill or exercise, a list of participants, and any best practices or lessons learned which may improve the FSP;

(3) Incidents and breaches of security. Date and time of occurrence, location within the OCS facility, a description of the incident or breach, the identity of the individual to whom it was reported, and a description of the response;

(4) Changes in MARSEC Levels. Date and time of the notification received, and the time of compliance with additional requirements;

(5) Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;

(6) Security threats. Date and time of occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response;

(7) Declaration of Security (DoS). A copy of each DoS for at least 90 days after the end of its effective period; and

(8) Annual audit of the Facility Security Plan (FSP). For each annual audit, a letter certified by the FSO stating the date the audit was conducted.


Sec. 106.235 Maritime Security (MARSEC) Level coordination and implementation.

(a) The OCS facility owner or operator must ensure the OCS facility operates in compliance with the security requirements in this part for the MARSEC Level in effect for the OCS facility.

(b) When notified of an increase in the MARSEC Level, the OCS facility owner or operator must ensure:

(1) Vessels conducting operations with the OCS facility and vessels scheduled to arrive at the OCS facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security (DoS), if applicable, is revised as necessary;

(2) The OCS facility complies with the required additional security measures within 12 hours; and
(3) The OCS facility reports compliance or noncompliance to the cognizant District Commander.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer (FSO) must inform all OCS facility personnel about identified threats, emphasize reporting procedures, and stress the need for increased vigilance.

(d) An OCS facility owner or operator whose facility is not in compliance with the requirements of this section must so inform the cognizant District Commander and obtain approval prior to interfacing with another vessel or prior to continuing operations.


Sec. 106.240 Communications.

(a) The Facility Security Officer (FSO) must have a means to effectively notify OCS facility personnel of changes in security conditions at the OCS facility.

(b) Communication systems and procedures must allow effective and continuous communications between the OCS facility security personnel, vessels interfacing with the OCS facility, the cognizant District Commander, and national and local authorities with security responsibilities.

(c) Facility communications systems must have a backup means for both internal and external communications.


Sec. 106.245 Procedures for interfacing with vessels.

The OCS facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

Sec. 106.250 Declaration of Security (DoS).

(a) Each OCS facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from vessels.

(b) At MARSEC Level 1, owners or operators of OCS facilities interfacing with a manned vessel carrying Certain Dangerous Cargoes, in
bulk, must:

(1) Prior to the arrival of a vessel to the OCS facility, ensure the Facility Security Officer (FSO) and Master, Vessel Security Officer (VSO), or their designated representatives coordinate security needs and procedures, and agree upon the contents of a DoS for the period of time the vessel is at the OCS facility; and

(2) Upon the arrival of the vessel at the OCS facility, the FSO and Master, VSO, or their designated representatives, must sign the written DoS.

(c) Neither the OCS facility nor the vessel may embark or disembark personnel, or transfer stores or industrial supplies until the DoS has been signed.

(d) At MARSEC Levels 2 and 3, the FSOS of OCS facilities interfacing with manned vessels subject to part 104 of this chapter, or their designated representatives, must sign and implement DoSs as required in paragraphs (b)(1) and (b)(2) of this section.

(e) At MARSEC Levels 1 and 2, FSOS of OCS facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.


Sec. 106.255 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in Sec. 106.230(b)(5) of this part.

(c) The Facility Security Plan (FSP) must include procedures for identifying and responding to security system and equipment failures or malfunctions.
Sec. 106.260 Security measures for access control.

(a) General. The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board; and

(3) Control access to the OCS facility.

(b) The OCS facility owner or operator must ensure that the following are specified:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them; and

(3) The means of identification required to allow individuals to access the OCS facility and remain on the OCS facility without challenge.

(c) The OCS facility owner or operator must ensure that an identification system is established for checking the identification of OCS facility personnel or other persons seeking access to the OCS facility that:

(1) Provides for identification of authorized and unauthorized persons at any MARSEC Level;

(2) Is coordinated, when practicable, with identification systems used by vessels or other transportation conveyances conducting operations with the OCS facility;

(3) Is updated regularly; and

(4) Allows temporary or continuing access for OCS facility personnel and visitors through the use of a badge or other system to verify their identity.

(d) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(e) MARSEC Level 1. The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Screen persons and personal effects going aboard the OCS
facility for dangerous substances and devices at the rate specified in the approved FSP;

(2) Conspicuously post signs that describe security measures currently in effect and clearly stating that:
   (i) Boarding an OCS facility is deemed valid consent to screening or inspection; and
   (ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(3) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors;

(4) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel, to establish his or her identity or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(5) Deter unauthorized access to the OCS facility;

(6) Identify access points that must be secured or attended to deter unauthorized access;

(7) Lock or otherwise prevent access to unattended spaces that adjoin areas to which OCS facility personnel and visitors have access;

(8) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(9) Provide a designated secure area on board, or in liaison with a vessel interfacing with the OCS facility, for conducting inspections and screening of people and their personal effects; and

(10) Respond to the presence of unauthorized persons on board.

(f) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

   (1) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

   (2) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

   (3) Limiting the number of access points to the OCS facility by closing and securing some access points; or

   (4) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

(g) MARSEC Level 3. In addition to the security measures required
for MARSEC Level 1 and MARSEC Level 2, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. The additional security measures may include:

1. Screening all persons and personal effects for dangerous substances and devices;
2. Being prepared to cooperate with responders;
3. Limiting access to the OCS facility to a single, controlled access point;
4. Granting access to only those responding to the security incident or threat thereof;
5. Suspending embarkation and/or disembarkation of personnel;
6. Suspending the onloading of stores or industrial supplies;
7. Evacuating the OCS facility; or
8. Preparing for a full or partial search of the OCS facility.


Sec. 106.265 Security measures for restricted areas.

(a) General. The OCS facility owner or operator must ensure the designation of restricted areas in order to:
1. Prevent or deter unauthorized access;
2. Protect persons authorized to be in the OCS facility;
3. Protect the OCS facility;
4. Protect vessels using and serving the OCS facility;
5. Protect sensitive security areas within the OCS facility;
6. Protect security and surveillance equipment and systems; and
7. Protect stores and industrial supplies from tampering.

(b) Designation of restricted areas. The OCS facility owner or operator must ensure restricted areas are designated within the OCS facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The OCS facility owner or operator may designate the entire OCS facility as a restricted area. Restricted areas must include, as appropriate:
1. Areas containing sensitive security information;
2. Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and
(3) Areas containing critical OCS facility infrastructure equipment, including:

(i) Water supplies;
(ii) Telecommunications;
(iii) Power distribution system;
(iv) Access points for ventilation and air-conditioning systems;
(v) Manufacturing areas and control rooms;
(vi) Areas designated for loading, unloading or storage of stores and industrial supplies; and
(vii) Areas containing hazardous materials.

(c) The OCS facility owner or operator must ensure that the Facility Security Plan (FSP) includes measures for restricted areas to:

(1) Identify which OCS facility personnel are authorized to have access;
(2) Determine which persons other than OCS facility personnel are authorized to have access;
(3) Determine the conditions under which that access may take place;
(4) Define the extent of any restricted area; and
(5) Define the times when access restrictions apply.

(d) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;
(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;
(3) Verifying the identification and authorization of all persons seeking entry;
(4) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry to or movement within restricted areas; or
(5) Designating temporary restricted areas to accommodate OCS facility operations. If temporary restricted areas are designated, the FSP must include security requirements to conduct a security sweep of the designated temporary restricted areas both before and after the area has been established.

(e) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility...
owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Enhancing the effectiveness of the barriers surrounding restricted areas, for example, by the use of patrols or automatic intrusion detection devices;

(2) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(3) Further restricting access to the restricted areas and movements and storage within them;

(4) Using continuously monitored and recorded surveillance equipment;

(5) Increasing the number and frequency of patrols, including the use of waterborne patrols; or

(6) Restricting access to areas adjacent to the restricted areas.

(f) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas; or

(3) Searching restricted areas as part of a security sweep of all or part of the OCS facility.


Sec. 106.270 Security measures for delivery of stores and industrial supplies.

(a) General. The OCS facility owner or operator must ensure that security measures relating to the delivery of stores or industrial supplies to the OCS facility are implemented to:

(1) Check stores or industrial supplies for package integrity;

(2) Prevent stores or industrial supplies from being accepted without inspection;

(3) Deter tampering; and

(4) Prevent stores and industrial supplies from being accepted unless ordered. For any vessels that routinely use an OCS facility, an OCS facility owner or operator may establish and implement standing arrangements between the OCS facility, its suppliers, and any vessel delivering stores or industrial supplies regarding notification and the
timing of deliveries and their documentation.

(b) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of measures to:

(1) Inspect stores or industrial supplies before being accepted; and
(2) Check that stores or industrial supplies match the order prior to being brought on board.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved Facility Security Plan (FSP). These additional security measures may include:

(1) Intensifying inspection of the stores or industrial supplies during delivery; or
(2) Checking stores or industrial supplies prior to receiving them on board.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Checking all OCS facility stores or industrial supplies more extensively;
(2) Restricting or suspending delivery of stores or industrial supplies; or
(3) Refusing to accept stores or industrial supplies on board.

[[Page 393]]

Sec. 106.275 Security measures for monitoring.

(a) General. (1) The OCS facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, watchkeepers, security guards, deck watches, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment as specified in their approved Facility Security Plan (FSP), the:

(i) OCS facility;
(ii) Restricted areas on board the OCS facility; and
(iii) The area surrounding the OCS facility.

(2) The following must be considered when establishing the appropriate level and location of lighting:

(i) OCS facility personnel should be able to detect activities on
and around OCS facilities;

(ii) Coverage should facilitate personnel identification at access points; and

(iii) Lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(b) MARSEC Level 1. At MARSEC Level 1, the OCS facility owner or operator must ensure the implementation of security measures, which may be implemented in coordination with a vessel interfacing with the OCS facility, to:

(1) Monitor the OCS facility, particularly OCS facility access points and restricted areas;

(2) Be able to conduct emergency searches of the OCS facility;

(3) Ensure that equipment or system failures or malfunctions are identified and corrected;

(4) Ensure that any automatic intrusion detection device, sets off an audible or visual alarm, or both, at a location that is continuously attended or monitored; and

(5) Light deck and OCS facility access points during the period between sunset and sunrise and periods of limited visibility sufficiently to allow visual identification of persons seeking access to the OCS facility.

(c) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of security patrols;

(2) Using (if not already in use) or increasing the use of security and surveillance equipment;

(3) Assigning additional personnel as security lookouts; or

(4) Coordinating with boat patrols, when provided.

(d) MARSEC Level 3. In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Cooperating with responders;

(2) Switching on all lights;

(3) Switching on all surveillance equipment capable of recording activities on, or in the vicinity of, the OCS facility;

(4) Maximizing the length of time such surveillance equipment (if not already in use) can continue to record; or

(5) Preparing for underwater inspection of the OCS facility.
Sec. 106.280 Security incident procedures.

For each MARSEC Level, the OCS facility owner or operator must ensure the Facility Security Officer (FSO) and OCS facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical OCS facility and OCS facility-to-vessel interface operations;
(b) Deny access to the OCS facility, except to those responding to an emergency;
(c) Evacuate the OCS facility in case of security threats or breaches of security; and
(d) Report security incidents as required in Sec. 101.305 of this subchapter;

(e) Brief all OCS facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and
(f) Secure non-critical operations in order to focus response on critical operations.

Sec. 106.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.
(b) A single FSA may be performed and applied to more than one OCS facility to the extent they share physical characteristics, location, and operations.
(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Company Security Officer (CSO) reviews and accepts their work.
(d) Those involved in a FSA must be able to draw upon expert
assistance in the following areas, as appropriate:

1. Knowledge of current and anticipated security threats and patterns;
2. Recognition and detection of dangerous substances and devices;
3. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;
4. Recognition of techniques used to circumvent security measures;
5. Methods used to cause a security incident;
6. Effects of dangerous substances and devices on structures and essential services;
7. OCS facility security requirements;
8. OCS facility and vessel interface business practices;
9. Contingency planning, emergency preparedness and response;
10. Physical security requirements;
11. Radio and telecommunications systems, including computer systems and networks;
12. Marine or civil engineering; and
13. OCS facility and vessel operations.

Sec. 106.305 Facility Security Assessment (FSA) requirements.

(a) Background. The OCS facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

1. The general layout of the OCS facility, including:
   (i) The location of each access point to the OCS facility;
   (ii) The number, reliability, and security duties of OCS facility personnel;
   (iii) Security doors, barriers, and lighting;
   (iv) The location of restricted areas;
   (v) The emergency and stand-by equipment available to maintain essential services;
   (vi) The essential maintenance equipment and storage areas;
   (vii) Location of escape and evacuation routes and assembly stations; and
   (viii) Existing security and safety equipment for protection of personnel;
2. Response procedures for fire or other emergency conditions;
3. Procedures for monitoring OCS facility and vessel personnel;
4. Procedures for controlling keys and other access prevention systems;
5. Response capability for security incidents;
6. Threat assessments, including the purpose and methodology of the
assessment, for the OCS facility's location;

(7) Previous reports on security needs; and

(8) Any other existing security procedures and systems, equipment, communications, and OCS facility personnel.

(b) On-scene survey. The OCS facility owner or operator must ensure that an on-scene survey of each OCS facility is conducted. The on-scene survey examines and evaluates existing OCS facility protective measures, procedures, and operations to verify or collect the information required in paragraph (a) of this section.

(c) Analysis and recommendations. In conducting the FSA, the OCS owner or operator must ensure that the Company Security Officer (CSO) analyzes the OCS facility background information and the on-scene survey, and considering the requirements of this part, provides recommendations to establish and prioritize the security measures that should be included in the FSP. The analysis must consider:

(1) Each vulnerability found during the on-scene survey, including but not limited to:
   (i) Access to the OCS facility;
   (ii) Structural integrity of the OCS facility;
   (iii) Existing security measures and procedures, including identification systems;
   (iv) Existing security measures and procedures relating to essential services;
   (v) Measures to protect radio and telecommunication equipment, including computer systems and networks;
   (vi) Existing agreements with private security companies;
   (vii) Any conflicting policies between safety and security measures and procedures;
   (viii) Any conflicting OCS facility operations and security duty assignments;
   (ix) Any deficiencies identified during daily operations or training and drills; and
   (x) Any deficiencies identified following security incidents or alerts, the report of security concerns, the exercise of control measures, or audits.

(2) Possible security threats, including but not limited to:
   (i) Damage to or destruction of the OCS facility or of a vessel adjacent to the OCS facility;
   (ii) Smuggling dangerous substances and devices;
   (iii) Use of a vessel interfacing with the OCS facility to carry
those intending to cause a security incident and their equipment;

(iv) Use of a vessel interfacing with the OCS facility as a weapon
or as a means to cause damage or destruction; and

(v) Effects of a nuclear, biological, radiological, explosive, or
chemical attack to the OCS facility’s shoreside support system;

(3) Threat assessments by Government agencies;

(4) Vulnerabilities, including human factors, in the OCS facility’s
infrastructure, policies and procedures;

(5) Any particular aspects of the OCS facility, including the
vessels that interface with the OCS facility, which make it likely to be
the target of an attack;

(6) Likely consequences, in terms of loss of life, damage to
property, or economic disruption, of an attack on or at the OCS
facility; and

(7) Locations where access restrictions or prohibitions will be
applied for each MARSEC level.

(d) FSA Report. (1) The OCS facility owner or operator must ensure
that a written FSA report is prepared and included as a part of the FSP.
The report must contain:

(i) A summary of how the on-scene survey was conducted;

(ii) A description of existing security measures, including
inspection, control and monitoring equipment, personnel identification
documents and communication, alarm, lighting, access control, and
similar systems;

(iii) A description of each vulnerability found during the on-scene
survey;

(iv) A description of security measures that could be used to
address each vulnerability;

(v) A list of the key OCS facility operations that are important to
protect; and

(vi) A list of identified weaknesses, including human factors, in
the infrastructure, policies, and procedures of the OCS facility.

(2) A FSA report must describe the following elements within the OCS
facility:

(i) Physical security;

(ii) Structural integrity;

(iii) Personnel protection systems;

(iv) Procedural policies;

(v) Radio and telecommunication systems, including computer systems
and networks; and

(vi) Essential services.

[[Page 396]]
(3) The FSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:

(i) OCS facility personnel;
(ii) Visitors, vendors, repair technicians, vessel personnel, etc.;
(iii) OCS facility stores;
(iv) Any security communication and surveillance systems; and
(v) Any other security systems, if any.

(4) The FSA report must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;
(ii) Conflicts between personnel duties and security assignments;
(iii) The impact of watch-keeping duties and risk of fatigue on personnel alertness and performance;
(iv) Security training deficiencies; and
(v) Security equipment and systems, including communication systems.

(5) The FSA report must discuss and evaluate key OCS facility measures and operations, including--

(i) Ensuring performance of all security duties;
(ii) Controlling access to the OCS facility through the use of identification systems or otherwise;
(iii) Controlling the embarkation of OCS facility personnel and other persons and their effects (including personal effects and baggage, whether accompanied or unaccompanied);
(iv) Supervising the delivery of stores and industrial supplies;
(v) Monitoring restricted areas to ensure that only authorized persons have access;
(vi) Monitoring deck areas and areas surrounding the OCS facility; and
(vii) The ready availability of security communications, information, and equipment.

(e) The FSA, FSA report, and FSP must be protected from unauthorized access or disclosure.


Sec. 106.310 Submission requirements.

(a) A completed FSA report must be submitted with the Facility Security Plan (FSP) required in Sec. 106.410 of this part.

(b) An OCS facility owner or operator may generate and submit a
report that contains the FSA for more than one OCS facility subject to this part, to the extent that they share similarities in physical characteristics, location and operations.

(c) The FSA must be reviewed and validated, and the FSA report must be updated each time the FSP is submitted for reapproval or revisions.


Subpart D_Outer Continental Shelf (OCS) Facility Security Plan (FSP)

Sec. 106.400 General.

(a) The OCS facility owner or operator must ensure the FSO develops and implements a Facility Security Plan (FSP) for each OCS facility for which he or she is designated as FSO. The FSP:

(1) Must identify the FSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Facility Security Assessment (FSA);

(4) Must describe security measures for each MARSEC Level; and

(5) May cover more than one OCS facility to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the cognizant District Commander.

(b) The FSP must be submitted for approval to the cognizant District Commander in a written or electronic format in a manner prescribed by the cognizant District Commander.

(c) The FSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the FSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.

[[Page 397]]

Sec. 106.405 Format and content of the Facility Security Plan (FSP).

(a) An OCS facility owner or operator must ensure that the FSP consists of the individual sections listed in this paragraph (a). If the FSP does not follow the order as it appears in this paragraph, the OCS facility owner or operator must ensure that the FSP contains an index identifying the location of each of the following sections:
(1) Security organization of the OCS facility;
(2) Personnel training;
(3) Drills and exercises;
(4) Records and documentation;
(5) Response to change in MARSEC Level;
(6) Procedures for interfacing with vessels;
(7) Declaration of Security (DoS);
(8) Communications;
(9) Security systems and equipment maintenance;
(10) Security measures for access control;
(11) Security measures for restricted areas;
(12) Security measures for delivery of stores and industrial supplies;
(13) Security measures for monitoring;
(14) Security incident procedures;
(15) Audits and FSP amendments; and
(16) Facility Security Assessment (FSA) report.

(b) The OCS facility owner or operator must ensure that the FSP describes in detail how each of the requirements of subpart B of this part will be met.


Sec. 106.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each OCS facility currently in operation must either:

(1) Submit one copy of the Facility Security Plan (FSP) for review and approval to the cognizant District Commander and a letter certifying that the FSP meets the applicable requirements of this part; or

(2) If intending to operate under an Approved Security Program, submit a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Owners or operators of OCS facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) The cognizant District Commander will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;
(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or
(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.
(d) An FSP may be submitted and approved to cover more than one OCS facility where they share similarities in physical characteristics, location, and operations.
(e) Each OCS facility owner or operator that submits one FSP to cover two or more OCS facilities of similar design, location, and operation must address OCS facility-specific information that includes the physical and operational characteristics of each OCS facility.
(f) An FSP that is approved by the cognizant District Commander is valid for 5 years from the date of its approval. The cognizant District Commander will issue an approval letter, as indicated in Sec. 106.115 of this part.


Sec. 106.415 Amendment and audit.

(a) Amendments. (1) Amendments to a Facility Security Plan (FSP) that are approved by the cognizant District Commander may be initiated by:
   (i) The OCS facility owner or operator; or
   (ii) The cognizant District Commander, upon a determination that an amendment is needed to maintain the OCS facility's security. The cognizant District Commander will give the OCS facility owner or operator written notice and request that the OCS facility owner or operator propose amendments addressing any matters specified in the notice. The OCS facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the OCS facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the cognizant District Commander.

   (2) Proposed amendments must be sent to the cognizant District Commander. If initiated by the OCS facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant District Commander allows a shorter period. The cognizant District Commander will approve
or disapprove the proposed amendment in accordance with Sec. 106.410 of this subpart.

(3) Nothing in this section should be construed as limiting the OCS facility owner or operator from the timely implementation of such additional security measures not enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant District Commander by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If the owner or operator has changed, the Facility Security Officer (FSO) must amend the Facility Security Plan (FSP) to include the name and contact information of the new OCS facility owner(s) or operator(s) and submit the affected portion of the FSP for review and approval in accordance with Sec. 106.410 of this subpart.

(b) Audits. (1) The FSO must ensure an audit of the FSP is performed annually, beginning no later than one year from the initial date of approval and attach a letter to the FSP certifying that the FSP meets the applicable requirements of this part.

(2) If there is a change in ownership or operations of the OCS facility, or if there have been modifications to the OCS facility, the FSP must be audited including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the FSP as a result of modifications to the OCS facility may be limited to those sections of the FSP affected by the OCS facility modifications.

(4) Unless impracticable due to the size and nature of the company or the OCS facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods of conducting audits and inspections, and control and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require an amendment of either the Facility Security Assessment (FSA) or FSP, the FSO must submit, in accordance with Sec. 106.410 of this subpart, the amendments to the cognizant District Commander for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

[DLOG-2003-14759, 68 FR 39345, July 1, 2003, as amended at 68 FR 60559,
# INDEX

SUBCHAPTER H_MARITIME SECURITY

Editorial Note: This listing is provided for informational purposes only. It is compiled and kept up-to-date by the Coast Guard, Department of Homeland Security, and is updated as of July 1, 2004.

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
</tr>
<tr>
<td>Additional communication devices.................................101.310</td>
</tr>
<tr>
<td>Additional requirements passenger vessels and ferries............104.292</td>
</tr>
<tr>
<td>Alternatives.....................................................101.120</td>
</tr>
<tr>
<td>Alternative Security Programs..................104.140, 105.140, 106.135</td>
</tr>
<tr>
<td>Amendment and audit.....................................104.415, 106.415</td>
</tr>
<tr>
<td>Applicability.........................101.110, 103.100, 105.105, 106.105</td>
</tr>
<tr>
<td>Approved Alternative Security Programs...........................101.125</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Committee...........................103.300</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Committee Responsibilities........103.310</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Committee, composition of..........103.305</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Plan................................103.505</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Plan elements.......................103.505</td>
</tr>
<tr>
<td>Area Maritime Security (AMS) Plan review and approval............103.505</td>
</tr>
</tbody>
</table>

| **C** |
| Communications (vessel)..........................................104.245 |
| Communications (facility)........................................105.235 |
| Communications (OCS).............................................106.240 |
| Company Security Officer (CSO)...............................104.210, 106.205 |
| Company or vessel personnel with security duties...............104.220 |
| Compliance dates........................................104.115, 106.110 |
| Compliance documentation.........................................104.120 |
| Control and Compliance Measures...............................101.410 |

| **D** |
Declaration of Security (DoS)........101.505, 104.255, 105.245, 106.250
Definitions..................101.105, 103.105, 104.100, 105.100, 106.100
Department of Homeland Security alignment............101.205
Designation of the Federal Maritime Security Coordinator (FMSC)

103.200

Drill and exercise requirements........104.230, 105.220, 106.225

E

Enforcement......................................................101.400
Equivalents.....................................................104.135, 105.135, 106.130
Equivalent security measures.........................101.130
Exemptions.......................................................104.110, 105.110
Exercises........................................................103.515

[[Page 400]]

F

Facility Security Assessment (FSA).........................Subpart C
Facility Security Assessment (FSA) requirements........105.305, 106.305
Facility Security Officer (FSO).........................105.205, 106.210
Facility Security Plan (FSP).................................Subpart D
Facility Security Requirements............................Subpart B
Federal Maritime Security Coordinator (FMSC) Authority........103.205

G

General..........................................................104.400

I

Incorporation by reference.................................101.115

M

MARSEC Levels..................................................101.200
MARSEC Level coordination and implementation..........104.240
Maritime Security
Area Maritime Security.........................................103
Facilities........................................................105
Outer Continental Shelf (OCS)...............................106
Vessels...........................................................104
Maritime Security (MARSEC) Directives...101.405, 102, 104.145, 105.145, 106.140

Noncompliance...........................................104.125, 106.120

Outer Continental Shelf (OCS) Facility Security Assessment (FSA)
Subpart C
Outer Continental Shelf (OCS) Facility Security Plan (FSP).....Subpart D
Owner or operator................................................106.200

Penalties........................................................101.415
Personal identification.........................................101.515
Persons involved in the Area Maritime Security Assessment......103.410
Preparedness communications....................................101.300
Purpose..........................................................101.100

Recognized Security Organization (RSO), procedures for authorizing
101.500
Recordkeeping.............................................103.520, 104.235, 105.225, 106.230
Reporting........................................................101.305
Right to appeal..............................................101.420, 104.150, 106.145

Security incident procedures............................104.290, 105.280
Submission and approval.....................................104.410, 106.410
Submission requirements.....................................104.310, 106.310

Vessel Security Assessment (VSA)...............................Subpart C

Vessel Security Assessment (VSA)requirements..................104.305
Vessel Security Officer (VSO) ...........................................104.215
Vessel Security Plan (VSP) ...........................................Subpart D
VSP Submission and approval ........................................104.410

Waivers ..........................................................104.130, 105.130, 106.125

[[Page 402]]