

October 2011

MARITIME SECURITY

Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure

U.S. Government Accountability Office

GAO

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE OCT 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 59	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Why GAO Did This Study

Congressional interest in the security of offshore energy infrastructure has increased because of the lives lost and the substantial damages that resulted from the *Deepwater Horizon* incident in April 2010. The U.S. Coast Guard—a component of the Department of Homeland Security (DHS)—is the lead federal agency for maritime security, including the security of offshore energy infrastructure. The Coast Guard oversees two main types of offshore energy infrastructure—facilities on the Outer Continental Shelf (OCS) and deepwater ports. GAO was asked to examine (1) Coast Guard actions to ensure the security of OCS facilities and what additional actions, if any, are needed; (2) Coast Guard actions to ensure the security of deepwater ports and what additional actions, if any, are needed; and (3) what limitations in oversight authority, if any, the Coast Guard faces in ensuring the security of offshore energy infrastructure. GAO reviewed Coast Guard documents, such as inspection records, and relevant laws and regulations and interviewed Coast Guard inspectors and officials, including those at Coast Guard headquarters and the two Coast Guard districts that oversee all OCS facilities and deepwater ports that are subject to security requirements.

What GAO Recommends

GAO recommends that the Coast Guard develop policies or guidance to ensure that (1) annual security inspections are conducted at OCS facilities and (2) information entered into its database for both OCS facilities and deepwater ports is more useful for management. DHS and the Coast Guard concurred with these recommendations.

View [GAO-12-37](#) or key components. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

MARITIME SECURITY

Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure

What GAO Found

The Coast Guard has taken actions to address the security of OCS facilities (that is, facilities regulated for security pursuant to 33 C.F.R. part 106), but could improve its process for managing security inspections. For example, the Coast Guard developed a security plan for the Gulf of Mexico, in which all 57 OCS facilities are located, and it reviews security plans developed by the owners and operators of OCS facilities. It has also issued guidance, which states that Coast Guard personnel should conduct security inspections of OCS facilities annually, but has conducted about one-third of these inspections from 2008 through 2010. Further, the Coast Guard does not have procedures in place to ensure that its field units conduct these inspections. Consequently, the Coast Guard may not be meeting one of its stated goals of reducing the risk and mitigating the potential results of an act that could threaten the security of personnel, the OCS facility, the environment, and the public. The Coast Guard also faces challenges in summarizing inspection results. Specifically, its database for storing inspection data has limitations that make it difficult to determine if security inspections were conducted. For example, there is no data field to identify OCS facilities, which makes it difficult to readily analyze whether required inspections were conducted. By addressing some of these challenges, Coast Guard managers could more easily use the data as a management tool to inform decision making.

The Coast Guard has also taken actions to ensure the security of the four deepwater ports, but opportunities exist for improvement. The Coast Guard's actions to ensure the security of deepwater ports are similar to actions it has taken to ensure the security of OCS facilities. For example, Coast Guard security plans address security at deepwater ports, and the Coast Guard also reviews security plans developed by the owners and operators of the deepwater ports. However, Coast Guard guidance for deepwater ports does not call for annual security inspections, and it has conducted only one security inspection at a deepwater port from 2008 through 2010. Coast Guard officials said that the Coast Guard plans to begin annual security inspections of deepwater ports in recognition of the risk of a transportation security incident. However, limitations in the Coast Guard's inspection database and lack of guidance available to database users may complicate the Coast Guard's management and oversight of inspections at deepwater ports. For example, the data field for deepwater ports has been incorrectly applied to other types of infrastructure and some deepwater ports are recorded under multiple names. Unless the Coast Guard addresses these database limitations and issues updated guidance to database users, it will be difficult for the Coast Guard to verify that the deepwater ports are complying with applicable maritime security requirements.

The Coast Guard has limited authority regarding the security of mobile offshore drilling units (MODU) registered to foreign countries, such as the *Deepwater Horizon*. The Coast Guard is taking action, though, to gain a fuller understanding of the security risks associated with MODUs by conducting a study to help determine whether additional actions could better ensure the security of offshore energy infrastructure in the Gulf of Mexico, including MODUs.

Contents

Letter		1
	Background	9
	Coast Guard Could Further Ensure the Security of OCS Facilities by Improving Its Process for Managing Security Inspections	16
	Actions Are Needed to Further Ensure the Security of Deepwater Ports	26
	Coast Guard Has Limited Authority over the Security of MODUs Registered to Foreign Countries	33
	Conclusions	39
	Recommendations for Executive Action	40
	Agency Comments and Our Evaluation	40

Appendix I	Scope and Methodology	44
------------	-----------------------	----

Appendix II	Status of Action Items from National Level Exercise 2009	48
-------------	--	----

Appendix III	Comments from the Department of Homeland Security	50
--------------	---	----

Appendix IV	GAO Contact and Staff Acknowledgments	52
-------------	---------------------------------------	----

Related GAO Products		53
----------------------	--	----

Tables		
	Table 1: Security Inspections Required and Conducted of OCS Facilities, 2008 through 2010	20
	Table 2: Security Inspections Required and Conducted of OCS Facilities, by Type, 2008 through 2010	21
	Table 3: Status of Action Items Resulting from National Level Exercise 2009	48

Figures

Figure 1: OCS Facility in the Gulf of Mexico	9
Figure 2: Types of OCS Facilities and Deepwater Ports and the Applicable Security Related Regulations	13
Figure 3: Coast Guard Security Requirements Applicable to MODUs Operating in U.S. Federal Waters	34
Figure 4: Aftermath of the Explosion of the <i>Deepwater Horizon</i> Drilling Unit in the Gulf of Mexico, April 2010	38

Abbreviations

BOEMRE	Bureau of Ocean Energy Management, Regulation and Enforcement
BSEE	Bureau of Safety and Environmental Enforcement
DHS	Department of Homeland Security
ISPS Code	International Ship and Port Facility Security Code
LNG	Liquefied Natural Gas
LOOP	Louisiana Offshore Oil Port
MARSEC Level	Maritime Security Level
MISLE	Marine Information for Safety and Law Enforcement
MODU	mobile offshore drilling unit
MTSA	Maritime Transportation Security Act of 2002
NLE	National Level Exercise
NVIC	Navigation and Vessel Inspection Circular
OCS	Outer Continental Shelf
SAFE Port Act	Security and Accountability For Every Port Act of 2006
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

October 28, 2011

Congressional Requesters

The explosion of the *Deepwater Horizon* in April 2010 resulted in 11 deaths, serious injuries, and the largest oil spill in the history of the United States. The spill resulted in widespread and substantial environmental consequences and had an adverse impact on workers and businesses, with an estimated cost to compensate for these damages totaling billions of dollars. While the explosion was not the result of a breakdown in security procedures or a terrorist attack, other countries have experienced attacks by terrorists or other criminals on offshore energy infrastructure—facilities that produce, transport, or receive oil and natural gas. For example, attacks on oil facilities in the Niger River Delta in Africa have occurred in the last several years. Further, in 2004, a terrorist attack on an offshore oil terminal in Iraq using speedboats packed with explosives killed two U.S. Navy sailors and a U.S. Coast Guardsman. Domestically, offshore energy infrastructure may be an attractive target to terrorists given the importance of oil and natural gas to the nation's economy and security. In May 2011, the Department of Homeland Security (DHS) issued a press statement that intelligence information showed that throughout 2010 there was continuing interest by members of al Qaeda in targeting oil tankers and commercial oil infrastructure at sea. In addition, congressional interest in potential attacks on offshore energy infrastructure has increased because of the economic and environmental damages that resulted from the *Deepwater Horizon* incident.

The U.S. Coast Guard—a component of DHS—is the lead federal agency responsible for maritime security, including the security of offshore energy infrastructure. In this role, the Coast Guard seeks to mitigate many kinds of security challenges in the maritime environment. Doing so is a key part of its overall security mission and a starting point for identifying security gaps and taking actions to address them. Offshore energy infrastructure presents security challenges because some of this infrastructure is located many miles from shore.

The Maritime Transportation Security Act (MTSA) of 2002—enacted in the aftermath of the terrorist attacks of September 11, 2001—underscored the importance of deterring, preventing, or disrupting a

terrorist attack on key infrastructure in and around the nation's ports and waterways.¹ In accordance with MTSA, and its implementing regulations, the Coast Guard undertakes efforts to ensure maritime security by, among other things, reviewing and approving security plans produced by owners and operators of regulated vessels and facilities.² The Security and Accountability For Every (SAFE) Port Act of 2006 subsequently amended provisions of MTSA to, among other things and subject to the availability of appropriations, require verification of the effectiveness of facility security plans at least twice a year.³

There are two main types of offshore energy infrastructure that the Coast Guard oversees for security. The first type of offshore energy infrastructure includes facilities that operate on the outer continental shelf (OCS) and are generally described as facilities temporarily or permanently attached to the subsoil or seabed of the OCS that engage in exploration, development, or production of oil, natural gas, or mineral resources.⁴ There are about 3,900 such facilities, and if a facility of this type meets or exceeds any one of three thresholds for production or personnel—(1) producing greater than 100,000 barrels of oil a day, (2) producing more than 200 million cubic feet of natural gas per day, or (3) hosting more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more—it is subject to security

¹ See Pub. L. No. 107-295, 116 Stat. 2064 (2002).

² Maritime security regulations implementing provisions of MTSA relevant to this report are codified at parts 101 to 106 of title 33, Code of Federal Regulations.

³ See Pub. L. No. 109-347, § 103, 120 Stat. 1884, 1888 (2006) (codified at 46 U.S.C. § 70103(c)(4)(D)).

⁴ See 33 C.F.R. § 101.105. The OCS is a designation for all submerged lands extending seaward from generally 3 nautical miles off the coastline to at least 200 nautical miles, and of which the subsoil and seabed appertain to the U.S. and are subject to its jurisdiction and control. See 43 U.S.C. § 1331(a); 33 C.F.R. § 140.10.

requirements in accordance with 33 C.F.R. part 106.⁵ In this report, we discuss the 57 facilities regulated for security in accordance with part 106 because they met or exceeded these criteria at some point from 2008 through 2010. We refer to these facilities as “OCS facilities.”⁶ The second type of offshore energy infrastructure is called a deepwater port. Deepwater ports fall under a different set of regulations than OCS facilities.⁷ Deepwater ports are fixed or floating manmade structures used or intended for use as a port or terminal for the transportation, storage, or handling of oil or natural gas to any state and include the transportation of oil or natural gas from the United States’s OCS.⁸ There are currently four licensed deepwater ports⁹—two in the Gulf of Mexico and two in Massachusetts Bay. Unlike OCS facilities, which are involved in the production of oil or natural gas, deepwater ports enable tankers to offload oil or liquefied natural gas for transport to land by underwater pipelines.

In partnership with the Coast Guard, owners and operators of offshore energy infrastructure also play a key role in securing OCS facilities and deepwater ports. For example, working in conjunction with appropriate Coast Guard personnel, owners and operators are responsible for

⁵ See 33 C.F.R. § 106.105. Facilities meeting any of the threshold criteria are often referred to as MTSA-regulated facilities. Production means those activities which take place after the successful completion of any means for the removal of minerals, including, but not limited to, such removal, field operations, transfer of minerals to shore, operation monitoring, maintenance, and workover. See 33 C.F.R. § 140.10. According to the Coast Guard, the statement; “transfer of minerals to shore,” encompasses fixed facilities that operate as “transmission facilities.” Production quantities shall be calculated as the sum of all sources of production from wells on the primary and any attending platform(s), including the throughput of other pipelines transferring product across the same platform(s).

⁶ For those facilities that do not meet production or personnel thresholds under 33 C.F.R. part 106, the Coast Guard may conduct other oversight functions, such as safety inspections.

⁷ See 33 C.F.R. pts. 148-150.

⁸ See 33 C.F.R. § 148.5. Although deepwater ports are generally not regulated for security in accordance with MTSA, owners and operators generally carry out similar measures to those carried out for OCS facilities by, among other things, developing security plans comparable to those implemented by OCS facilities pursuant to part 106. See 33 C.F.R. § 150.15(x).

⁹ The term deepwater port is sometimes used to refer to shoreside ports that have deep drafts, which allow large ships to enter these ports. This report, however, uses “deepwater port” in accordance with its regulatory definition. See 33 C.F.R. § 148.5.

assessing risks and implementing security measures at their facilities. They may assess risks by identifying the vulnerabilities of their facilities to possible attack scenarios and, in so doing they identify ways to mitigate vulnerabilities in and around their facilities. Owners and operators also have security officers that are responsible for carrying out appropriate security measures.

Given the role that the Coast Guard plays in ensuring the security of OCS facilities and deepwater ports, we were asked to address the following three questions:

- What has the Coast Guard done to ensure the security of OCS facilities, and what additional actions, if any, are needed?
- What has the Coast Guard done to ensure the security of deepwater ports, and what additional actions, if any, are needed?
- What limitations in oversight authority, if any, does the Coast Guard face in ensuring the security of offshore energy infrastructure?

This report supplements our August 2011 testimony that focused on Coast Guard risk assessments of OCS facilities and deepwater ports.¹⁰ In this report, we focus on Coast Guard security inspections of OCS facilities and deepwater ports.

To address all three objectives in this report, we interviewed officials in Coast Guard headquarters in Washington, D.C., and district offices in New Orleans, Louisiana, and Boston, Massachusetts, about offshore

¹⁰ GAO, *Maritime Security: Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply*, [GAO-11-883T](#) (Washington D.C.: Aug. 24, 2011). In this testimony, we reported that the Coast Guard has taken actions to assess risks to such facilities, such as coordinating its risk assessment efforts with the intelligence community and with key stakeholders. We also reported that the Coast Guard faces challenges in data and scope that hinder its risk assessment efforts. For example, we reported that the Coast Guard did not assess the risks to 12 of 50 OCS facilities in 2011 which, pursuant to Coast Guard risk assessment guidance, should have been assessed. The Coast Guard generally agreed with our findings and has taken action to conduct the required risk assessments. Further, we determined that the Coast Guard's current set of policies and procedures do not call for an updated list of OCS facilities to be provided to analysts to assess the risks to such facilities annually. Doing so is important in that the number of OCS facilities could change each year. Coast Guard officials acknowledged that their policies and procedures do not include this requirement and agreed with our recommendation to revise their policies and procedures to add this requirement.

energy infrastructure security because officials in these offices are responsible for ensuring the security of OCS facilities or deepwater ports.¹¹ In addition, we reviewed relevant laws, regulations, and Coast Guard guidelines for ensuring the security of OCS facilities and deepwater ports. We also reviewed our previous work on Coast Guard efforts to assess security plans and to conduct security inspections of shoreside maritime facilities.¹²

To address the first question, we visited the Coast Guard's field unit in Morgan City, Louisiana, because Coast Guard officials at this location are responsible for inspecting the most OCS facilities of any unit in the Coast Guard. We also interviewed Coast Guard marine inspectors by telephone at Coast Guard field units located in Mobile, Alabama; Morgan City, Louisiana; New Orleans, Louisiana; Corpus Christi, Texas; Galveston, Texas; and Port Arthur, Texas. We selected these offices because they constitute all Coast Guard offices responsible for conducting security inspections of OCS facilities. We also visited an OCS facility in the Gulf of Mexico to observe security measures that had been implemented and to interview the facility security officer. We visited this facility because the local Coast Guard marine inspectors and the facility's security officer were able to accommodate our visit without interrupting operations. We also interviewed representatives from two companies that together operate 18 OCS facilities that are subject to annual security inspections. We selected these two companies because they own and operate the most OCS facilities in the Gulf of Mexico. We cannot generalize the results of our visit and interviews with these representatives to all owners and operators of OCS facilities; however, the information we obtained provided further insights into the Coast Guard's and owners' and operators' efforts to ensure the security of offshore energy infrastructure.

In addition, we interviewed relevant officials and analyzed information and data on the National Level Exercise (NLE) 2009—an exercise that tested, among other things, the Coast Guard's capabilities for preventing a hypothetical terrorist attack on offshore energy facilities in the Gulf of

¹¹ Currently, the Eighth Coast Guard District in New Orleans, Louisiana, and the First Coast Guard District in Boston, Massachusetts, are the only two districts that have OCS facilities or deepwater ports operating in their respective areas of responsibility.

¹² GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, [GAO-08-12](#) (Washington D.C.: Feb. 14, 2008).

Mexico. Regarding NLE 2009, we also reviewed data on “action items” resulting from the exercise to determine whether corrective actions had been implemented. We assessed the reliability of these data by interviewing Coast Guard officials who use the data and by reviewing relevant documentation, such as the after action report produced by the Coast Guard. We concluded that the data were sufficiently reliable for the purpose of assessing action items that have not been resolved. For those action items from NLE 2009 that had not been addressed, we followed up with Coast Guard and DHS officials responsible for tracking such action items to verify the status of the action items.

To further address the first question, we analyzed inspection data and reports for OCS facilities from 2008 through 2010 from the Coast Guard’s Marine Information for Safety and Law Enforcement (MISLE) database—the database that the Coast Guard uses to, among other things, record its inspection results. We also analyzed security inspection data for 2011 (through June 24, 2011), but did not report on these data because most of the annual security inspections of OCS facilities are typically not conducted until the fall. We assessed the reliability of these data by interviewing Coast Guard officials who use the data and by reviewing relevant documentation. As discussed later in this report, we identified some problems with the data and worked with Coast Guard officials to address these problems. Appendix I has a more detailed discussion on our scope and methodology in analyzing the MISLE database. Based on the steps we took to assess data reliability, we found the data to be sufficiently reliable for the purpose of determining the extent to which the Coast Guard conducted security inspections of OCS facilities. We also interviewed officials from the Department of the Interior’s Bureau of Safety and Environmental Enforcement (BSEE), formerly the Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), to determine what role, if any, BSEE plays in ensuring the security of OCS facilities.¹³ We also reviewed our *Standards for Internal Control in the*

¹³ BSEE is the federal agency responsible for enforcing safety, environment, and conservation compliance regarding offshore resources on the OCS. We are currently reviewing, among other things, the Department of the Interior’s recent reorganization of its bureaus which oversee offshore oil and natural gas activities and recent policy changes to the way in which it reviews drilling permits and its offshore inspection program. We are doing this work at the request of the Chairman of the Subcommittee on Oversight, Committee on Environment and Public Works, U.S. Senate. We expect to issue this related report in the winter 2012.

*Federal Government*¹⁴ and compared the standards for control activities with the Coast Guard's policies and procedures for conducting security inspections of OCS facilities and for recording inspection results in MISLE.

To address the second question, we reviewed Coast Guard documents on the security of deepwater ports and interviewed owners and operators of deepwater ports to discuss their role in the security of their facilities. We also visited a deepwater port in the Gulf of Mexico called the Louisiana Offshore Oil Port (LOOP) to observe security measures that had been implemented and to interview the facility security officer. We visited the LOOP because it is the only operational deepwater port in the Gulf of Mexico. While we cannot generalize our findings from this visit to all deepwater ports, the information we obtained provided us with valuable insights about the role of facility security officers and Coast Guard efforts to ensure the security of such facilities. We also interviewed Coast Guard officials responsible for inspecting deepwater ports in Morgan City, Louisiana, and Boston, Massachusetts. We selected these locations because these are the only Coast Guard units in which there are federally regulated deepwater ports. We analyzed inspection data from 2008 through 2010 for deepwater ports from the Coast Guard's MISLE database. We assessed the reliability of these data by interviewing Coast Guard officials who use the data and by reviewing relevant documentation to ensure its integrity. As discussed later in this report, we identified some problems with the data and worked with Coast Guard officials to address these problems. On the basis of the steps we took to assess data reliability, we found the data to be sufficiently reliable for the purpose of determining the extent to which the Coast Guard conducted security inspections of deepwater ports. We also reviewed Coast Guard policies and procedures for ensuring the security of deepwater ports. Further, we reviewed the *Standards for Internal Control*

¹⁴ GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget (OMB) issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in OMB Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

*in the Federal Government*¹⁵ and compared the standards for control activities with the Coast Guard's policies and procedures for recording inspection results in MISLE.

To address the third question, we reviewed relevant international requirements, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code and U.S. regulations for ensuring the security of OCS facilities, which may include mobile offshore drilling units (MODU). We also reviewed reports on the *Deepwater Horizon* incident, including the Coast Guard's report¹⁶ from the joint investigation it conducted with BSEE's predecessor, BOEMRE,¹⁷ and a report from the National Commission on the BP *Deepwater Horizon* Oil Spill and Offshore Drilling.¹⁸ We also discussed international agreements and U.S. regulations that apply to OCS facilities and MODUs with Coast Guard officials.

We conducted this performance audit from October 2010 through October 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

¹⁵ [GAO/AIMD-00-21.3.1](#).

¹⁶ U.S. Coast Guard, *Report of Investigation into the Circumstances Surrounding the Explosion, Fire, Sinking and Loss of Eleven Crew Members Aboard the Mobile Offshore Drilling Unit Deepwater Horizon in the Gulf of Mexico April 20 – 22, 2010, Volume I* (Washington, D.C.: September 2011).

¹⁷ On October 1, 2011, BOEMRE reorganized into two independent entities: the Bureau of Ocean Energy Management and BSEE. The Bureau of Ocean Energy Management is responsible for managing development of the nation's offshore resources in an environmentally and economically responsible way, and its activities include oversight of leasing, environmental studies, and economic analysis. BSEE is responsible for enforcing safety and environmental regulations.

¹⁸ National Commission on the BP *Deepwater Horizon* Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* (Washington D.C.: January 2011).

Background

OCS Facilities and Deepwater Ports Are Important and Vulnerable

The nation's economy and security are dependent, in part, on domestic offshore exploration and production of oil and natural gas. OCS facilities play a significant and growing role in domestic production. For example, oil production from offshore sources helped offset declines in land-based production in recent decades. The OCS is in an area of federal jurisdiction that contains an estimated 85 billion barrels of oil, more than all onshore resources and those in shallower state waters combined (see fig. 1 for a photograph of an OCS facility in the Gulf of Mexico).¹⁹ In addition, the LOOP is responsible for transporting to shore about 10 percent of imported oil to the United States.

Figure 1: OCS Facility in the Gulf of Mexico



Source: GAO.

¹⁹ This estimate comes from the National Commission on the BP *Deepwater Horizon* Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling* (Washington D.C.: January 2011).

Offshore production of oil and natural gas is critical in supporting businesses, the military, and individuals who rely on a steady supply of these resources. In addition, the leasing of offshore lands and the collection of royalties on the production of oil and natural gas results in billions of dollars in revenue for the federal government.

Because of their importance to the economy and national security, OCS facilities and deepwater ports are possible targets for al Qaeda and other groups with malevolent intent. For example, in May 2011, DHS issued a press statement that intelligence information showed that throughout 2010 there was continuing interest by members of al Qaeda in targeting oil tankers and commercial oil infrastructure at sea. In addition, other countries have experienced attacks by terrorists or criminals. For example, in 2006, Nigerian militants attacked energy facilities and abducted foreign oil workers in the oil-rich Niger delta. These attacks have continued in recent years and, in August 2011, the United Nations Security Council expressed concern about the attacks. Potential attack methods identified by the Coast Guard or owners and operators of offshore energy infrastructure include (1) crashing an aircraft into a facility; (2) using a submarine vessel, diver, or other means of attacking a facility underwater; (3) ramming a facility with a vessel; and (4) sabotage by an employee.²⁰

OCS facilities and deepwater ports may be at risk for an attack because they are located in open waters and generally are many miles away from Coast Guard assets and personnel. For example, owners and operators of OCS facilities expressed concern about recreational and fishing boats

²⁰ One technique used by owners and operators to reduce the risk of sabotage is to check the background of their employees and other staff who board or work on offshore infrastructure. Among other things, they use Transportation Worker Identification Credentials (TWIC) that are issued by the Transportation Security Administration (TSA)—an agency within DHS with primary responsibility for transportation security. Owners and operators can require employees and other staff to submit to a background investigation by TSA as one means of ensuring security. We have previously reported on problems with TWIC, such as internal controls in the enrollment and background checking processes are not designed to provide reasonable assurance that (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC-holders have maintained their eligibility. See GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, [GAO-11-657](#) (Washington D.C.: May 10, 2011).

and divers operating near or attempting to attach themselves to an OCS facility. Another risk is that many OCS facilities do not have personnel on-board the facility who can detect or report unauthorized incursions. According to Coast Guard officials, OCS facilities and deepwater ports are generally not considered to be high-risk targets. Rather, Coast Guard officials also noted that OCS facilities and deepwater ports are lower risk targets because of their remote location because an attack on them would not likely result in a significant disruption of maritime commerce. However, if an incident occurs, it would be difficult for the Coast Guard to respond quickly because deepwater ports and OCS facilities are generally isolated and located many miles from the closest Coast Guard unit.

Characteristics of OCS Facilities and Deepwater Ports Vary

Of the roughly 3,900 offshore facilities on the OCS, from January 1, 2008, through December 31, 2010, there were 57 facilities which, at some point during that period of time, met the production or personnel thresholds subjecting them to security requirements. OCS facilities generally consist of two different types of facilities: (1) fixed OCS facilities and (2) floating OCS facilities. For example, 41 of the OCS facilities are fixed OCS facilities that are permanently fixed to the sea floor. Of those, 34 are primarily involved in the transportation of large volumes of oil or natural gas and are called “transmission platforms.”²¹ These facilities, unlike facilities that produce oil and natural gas, may not be staffed, but instead may have automated operations or could be operated remotely from shore. The remaining 16 facilities are floating OCS facilities, which are buoyant facilities that are securely moored to the seabed.²² An example of such a facility is a floating offshore installation, which is a floating structure that is moored to the seafloor in a semipermanent manner, to be

²¹ According to a Coast Guard official, some of these facilities may also be involved in producing oil, but their primary function is as a transmission facility.

²² A floating OCS facility is a buoyant OCS facility securely and substantially moored so that it cannot be moved without a special effort and includes tension leg platforms and permanently moored semisubmersibles or shipshape hulls, but does not include mobile offshore drilling units or other vessels. However, for the purposes of this report, we include non-self-propelled MODUs that meet relevant production or personnel thresholds in the category of floating OCS facilities because such MODUs are also regulated for security under 33 C.F.R. part 106.

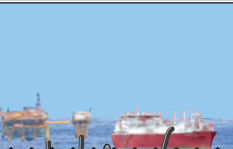
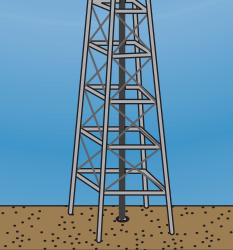
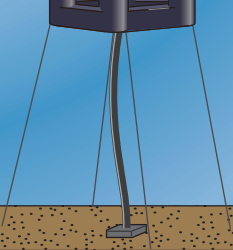
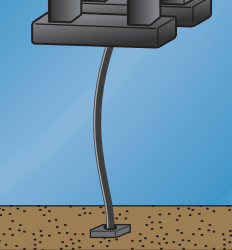
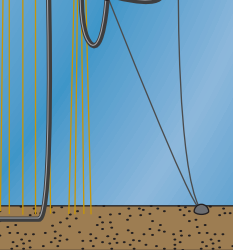
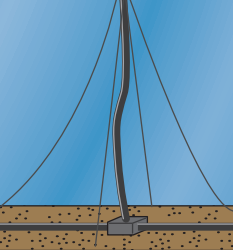
kept at that location for the primary purpose of producing oil and natural gas from wells drilled into the sea floor.²³

Further, we determined there were four deepwater ports in operation during the time period covered by our review. Deepwater ports can be one of two types: (1) oil deepwater ports and (2) liquefied natural gas (LNG) deepwater ports. The LOOP is an oil deepwater port that has two above the water fixed platforms in addition to buoys that float on the surface, while the remaining three deepwater ports involve an underwater buoy system that tankers use to offload LNG and have no above the water infrastructure.²⁴ When LNG tankers are not using these ports, the ports are not visible above the water. Figure 2 shows these facilities by type, number of each type from 2008 through 2010, and the applicable security regulation.

²³ Floating offshore installations include, but are not limited to, tension leg platforms, semisubmersible floating production systems, and spar platforms.

²⁴ According to the Coast Guard, on April 13, 2011, the LNG deepwater port in the Gulf of Mexico gave notice of its intent to be decommissioned in the near future.

Figure 2: Types of OCS Facilities and Deepwater Ports and the Applicable Security Related Regulations

Type of offshore energy infrastructure	Fixed OCS facility ^a	Floating OCS facility ^b		Oil deepwater port	LNG deepwater port
		Floating offshore installation	Mobile offshore drilling unit ^c		
Photograph					
Illustration showing underwater infrastructure					
Applicable security regulation	33 C.F.R. part 106	33 C.F.R. part 106	33 C.F.R. part 106	C.F.R. § 150.15(x)	C.F.R. § 150.15(x)
Number from 2008 through 2010 ^d	41	15	1	1	3

Sources: U.S. Coast Guard; BOEMRE; GDF Suez Energy North America; LOOP, LLC; and GAO.

^aA fixed OCS facility is a bottom-founded facility permanently attached to the seabed or subsoil of the OCS, including platforms, guyed towers and other structures. Fixed OCS facilities include (1) production platforms that produce oil and/or natural gas; and (2) transmission platforms, whose primary purpose is the pumping, maintenance, and/or inspection of transfer pipelines.

^bA floating OCS facility is a buoyant facility securely and substantially moored so that it cannot be moved without a special effort. This term includes tension leg platforms and permanently moored semisubmersibles or shipshape hulls, but does not include mobile offshore drilling units or other vessels.

^cA mobile offshore drilling unit (MODU) is a vessel, other than a public vessel of the United States, capable of engaging in drilling operations for exploration or exploitation of subsea resources. MODUs that are not self (or mechanically) propelled are regulated for security under 33 C.F.R. part 106 if they meet or exceed the relevant threshold criteria. For the purposes of this report, we refer to such MODUs subject to 33 C.F.R. part 106 as floating OCS facilities. Self-propelled MODUs are generally regulated for security as vessels pursuant to 33 C.F.R. part 104. We describe security regulations over MODUs in more detail later in figure 3.

^dThe number of OCS facilities may change each year based on whether a facility continues to meet or exceed the production or personnel thresholds, as determined by the Coast Guard. For example, there were 56 OCS facilities in 2008, 53 OCS facilities in 2009, and 51 OCS facilities in 2010.

All OCS facilities, as defined in this report, are located in the Gulf of Mexico. Among the four deepwater ports, the LOOP and one LNG deepwater port are located in the Gulf of Mexico and the other two LNG ports are located offshore in Massachusetts Bay near Boston. During the course of our review, the operator of the LNG deepwater port in the Gulf of Mexico notified the Coast Guard that it intended to decommission the

facility. As a result, the rest of this report's discussion of deepwater ports will focus on the remaining three deepwater ports.

Multiple Stakeholders Have Responsibility for Security

Coast Guard Is the Lead Federal Agency

As the lead federal agency for maritime security, the Coast Guard has broad responsibilities for ensuring the security of OCS facilities and deepwater ports. For example, staff at Coast Guard headquarters oversee and develop policies and procedures for field staff to follow when conducting security inspections of offshore energy infrastructure and to assist affected owners and operators so that they can comply with maritime security regulations.²⁵ Such policies and procedures offer guidance for (1) reviewing security plans produced by owners and operators of OCS facilities and (2) ensuring the security of OCS facilities. Among other things, Coast Guard marine inspectors in field units are to conduct security inspections of OCS facilities and deepwater ports by taking helicopter rides to facilities that can range up to 200 miles offshore. Once arriving, inspectors are to conduct on-site interviews with facility security officers and observe operations to verify whether required security measures are in place. As of August 2011, the Coast Guard had about 12 active marine inspectors who were qualified to conduct security inspections of OCS facilities. These inspectors work out of six field units near the Gulf of Mexico. After conducting security inspections of OCS facilities and deepwater ports, and in accordance with the guidance, inspectors are to record the results of these inspections in the MISLE database. Coast Guard marine inspectors are to record information such as any deficiencies that were identified and enforcement actions that were used to ensure compliance by the owners and operators. In addition to recording the results of offshore security inspections in MISLE, Coast Guard staff are to record other actions that are not related to offshore inspections, such as the results of search and rescue missions.

²⁵ See, e.g., Navigation and Vessel Inspection Circular (NVIC) 05-03, *Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 for Outer Continental Shelf Facilities* (December 15, 2003) and NVIC 03-05, *Guidance for Oversight of Post-Licensing Activities Associated with Development of Deepwater Ports* (May 16, 2005). We refer to NVIC 05-03 as "OCS facility guidance" and NVIC 03-05 as "deepwater port guidance."

Owners and Operators Partner
with the Coast Guard

Owners and operators of OCS facilities and deepwater ports have a shared responsibility with the Coast Guard to ensure the security of their offshore facilities and ports. For example, owners and operators of OCS facilities must carry out measures intended to improve the security in and around their facilities.²⁶ These measures include designating a company security officer and a facility security officer for each OCS facility the company operates. Company and facility security officers have responsibilities that include reporting security incidents to the National Response Center,²⁷ submitting facility security plans to the Coast Guard for approval, and ensuring their facilities comply with the security plans. Among other things, each facility security plan must address any vulnerabilities identified through a facility security assessment.²⁸ Although not subject to the same security requirements as OCS facilities, owners and operators of deepwater ports must develop security plans comparable to those required for OCS facilities and that address, among other things, risk identification and procedures for detecting and deterring terrorist or subversive activity.²⁹

²⁶ See, e.g., 33 C.F.R. §§ 106.200-.280. Corporate security officials told us that they also apply security measures to offshore facilities that do not meet the thresholds for production or personnel under 33 C.F.R. part 106.

²⁷ The primary function of the National Response Center is to serve as the sole national point of contact for reporting all oil, chemical, radiological, biological, and other discharges into the environment anywhere in the United States and its territories. In addition, the National Response Center serves as a conduit of information to and from law enforcement agencies. This includes reports of suspicious activity and actual security breaches.

²⁸ See 33 C.F.R. §§ 106.300-.310 (addressing facility security assessments), 106.400-.415 (addressing facility security plans).

²⁹ See 33 C.F.R. § 150.15(x).

Coast Guard Could Further Ensure the Security of OCS Facilities by Improving Its Process for Managing Security Inspections

Coast Guard Actions to Ensure Security

The Coast Guard has taken actions to ensure the security of OCS facilities in the Gulf of Mexico, within which all OCS facilities are presently located. For example, within a greater maritime security preparedness program, it established an Area Maritime Security Committee for the Gulf of Mexico in 2004. An Area Maritime Security Committee is responsible for, among other things, identifying critical infrastructure and operations, identifying risks, and providing advice to the Coast Guard for developing the Area Maritime Security Plan. The Gulf of Mexico Area Maritime Security Committee covers a broad area that crosses jurisdictional boundaries of multiple Coast Guard field units. Among other things, the Gulf of Mexico committee has representatives from stakeholders, such as federal law enforcement, state emergency responders, and owners and operators of OCS facilities. The committee has taken actions to enhance information sharing among stakeholders by holding annual meetings and offering training to OCS facility security officers on the command structure for responding to a transportation security incident. One of the functions of the committee is to contribute to the development of an Area Maritime Security Plan, which is discussed in more detail below.

The Coast Guard, in consultation with the Gulf of Mexico Area Maritime Security Committee and reliance on information in OCS facility security plans, has also developed an Area Maritime Security Plan specific to the

offshore environment in the Gulf of Mexico.³⁰ One of the primary objectives of the plan is to provide a framework for communication and coordination among stakeholders and law enforcement officials and to identify and reduce vulnerabilities to security threats in and near the marine transportation system in the Gulf of Mexico. For example, the plan specifies security measures to be taken at OCS facilities under certain security conditions. Furthermore, the plan discusses the broader security environment, including security measures at facilities and vessels that are not currently regulated with respect to security under part 106, which includes fixed transmission platforms or MODUs that do not exceed the production or personnel thresholds in part 106, and provides that the Coast Guard may consider requiring additional security measures for such facilities.

Additionally, the Coast Guard has conducted exercises and has taken corrective action, as appropriate, to strengthen its ability to prevent a terrorist attack on OCS facilities. In particular, in July 2009, the Coast Guard participated in a National Level Exercise (NLE)—a major exercise that involved multiple agencies, including DHS; the Department of Justice; the White House; and other federal, state, and local stakeholders—that tested the effectiveness of federal agencies in preventing a hypothetical attack on the nation's energy infrastructure, including OCS facilities.³¹ According to officials in the Coast Guard's Exercise Policy and Budget Division, the Coast Guard's role in this exercise was its most extensive involvement in an NLE to that date. As a result of the exercise, to address the lessons learned from the exercise, the Coast Guard developed 99 remedial action items that were assigned to Coast Guard units.³² According to Coast Guard data, 88 of these 99

³⁰ According to the Coast Guard, the Gulf of Mexico Area Maritime Security Plan is one of 43 Area Maritime Security Plans that were developed in 2004. The Coast Guard completed a formal 5-year review and approval process for these plans in August 2009. According to the Coast Guard, during this process the plans were updated to implement additional requirements of the SAFE Port Act regarding the inclusion of salvage response plans. Coast Guard policy requires that each plan be reviewed on an annual basis, and these plans are to be tested annually within an Area Maritime Security Training and Exercise Program exercise.

³¹ Additional exercises include a 2006 exercise to assess and validate information and procedures in the Gulf of Mexico Area Maritime Security Plan and a 2008 exercise scenario that involved a terrorist seizure of one or more offshore oil platforms.

³² These remedial action items are corrective actions that the Coast Guard tracks and analyzes as part of a continuous corrective action program.

action items have been resolved. For example, two field units that oversee the Gulf of Mexico clarified procedures for notifying relevant stakeholders of changes in risk levels.³³ Additionally, the Office of the Director of National Intelligence³⁴ has established a working group to examine the issue of information sharing with the private sector with the aim of finding a balance between sharing and securing sensitive information. Actions are being taken to address items that are not yet fully resolved. For more information about the status of action items from NLE 2009, see appendix II.

All OCS facilities that meet the production and personnel thresholds to be regulated for security are required to operate in accordance with facility security plans that the Coast Guard has approved. Coast Guard officials have reviewed and approved security plans produced by owners and operators of all OCS facilities. A Coast Guard port security specialist uses a detailed checklist to review the facility security plans to ensure that the plans satisfactorily address regulatory requirements.³⁵ For example, in reviewing a facility security plan, the port security specialist ensures that the plan includes provisions to provide security training to OCS facility personnel, including full-time and part-time contractors and temporary and permanent employees. Upon approval, a facility security plan remains valid for 5 years. Facility owners and operators must submit updated security plans to the Coast Guard at least every 5 years for

³³ Maritime Security (MARSEC) Levels advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. The Coast Guard uses the three-tiered system of MARSEC Levels, which is designed to easily communicate to Coast Guard assets and its maritime industry partners preplanned responses for credible threats. MARSEC Levels are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States. MARSEC Levels apply to vessels, Coast Guard-regulated facilities within the jurisdiction of the United States, and to Coast Guard operations.

³⁴ The Director of National Intelligence serves as the head of the Intelligence Community, overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. The goal of the Office of the Director of National Intelligence is to effectively integrate foreign, military, and domestic intelligence in defense of the homeland and of United States interests abroad.

³⁵ 33 C.F.R. § 106.405 lists the required components of a facility security plan, which are further described throughout part 106.

approval, and regulations also require owners and operators to review their plans annually and submit any amendments to the Coast Guard for approval. The Coast Guard also undertakes to assess the effectiveness of such facility plans by, for example, conducting security inspections, as discussed in the next section.³⁶

Procedures Are Needed to Ensure OCS Facility Inspections Are Conducted

Coast Guard OCS facility guidance³⁷ provides that Coast Guard personnel are to conduct security inspections of OCS facilities annually, but our analysis of inspections data shows that the Coast Guard has not conducted such inspections for most of these OCS facilities.³⁸ For example, the Coast Guard conducted about one-third of annual inspections of OCS facilities from 2008 through 2010 (see table 1).³⁹ In 2008 the Coast Guard inspected 7 of 56 OCS facilities, which was 13 percent of the annual inspections. More recently, in 2010, the Coast Guard inspected 23 of 51 OCS facilities (45 percent) that the Coast Guard should have inspected.

³⁶ See, e.g., 46 U.S.C. § 70103(c)(4)(D).

³⁷ We use the term OCS facility guidance to refer to the Coast Guard's NVIC 05-03, Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 for Outer Continental Shelf Facilities (December 15, 2003).

³⁸ The Coast Guard conducts annual security inspections for the purpose of ensuring compliance with applicable security requirements and verifying the effectiveness of facility security plans. Pursuant to 46 U.S.C. § 70103(c)(4)(D), as amended by the SAFE Port Act of 2006, the Secretary of Homeland Security, subject to the availability of appropriations, must verify the effectiveness of facility security plans periodically, but not less than two times per year, at least one of which must be an inspection of the facility conducted without notice. Coast Guard officials stated that in many cases, unannounced inspections can be logistically challenging because of the arrangements that are needed to fly out to OCS facilities. The 2003 OCS facility guidance (NVIC 05-03) provides for annual security inspections but does not specifically address the 2006 amendment to § 70103(c)(4)(D). This report, however, focuses on Coast Guard efforts to conduct annual inspections of facilities regulated under 33 C.F.R. part 106 pursuant to its existing guidance.

³⁹ We only present security inspection data from 2008 through 2010. We also analyzed security inspection data for 2011 (through June 24, 2011), but did not report on this information because most of the annual security inspections on OCS facilities are typically not conducted until the fall. From January through June 2011, the Coast Guard conducted four inspections of the OCS facilities.

Table 1: Security Inspections Required and Conducted of OCS Facilities, 2008 through 2010

Coast Guard field unit	2008		2009		2010	
	Inspections required	Inspections conducted	Inspections required	Inspections conducted	Inspections required	Inspections conducted
Corpus Christi	2	1	2	1	2	1
Galveston	5	2	4	3	4	4
Mobile	1	0	1	0	1	0
Morgan City	31	3	32	7	31	7
New Orleans	10	1	7	2	6	5
Port Arthur	7	0	7	7	7	6
Total (%)	56	7 (13%)	53	20 (38%)	51	23 (45%)

Source: GAO analysis of data provided by the U.S. Coast Guard.

Note: The number of OCS facilities fluctuates year-to-year based on whether a facility continues to meet or exceed the threshold criteria. For example, in 2009 there were 53 OCS facilities, but in 2010, 2 of the facilities became "deregulated." Once a facility (1) is below the production thresholds for a year or below the personnel threshold for 30 days; (2) has informed the Coast Guard; and (3) provided relevant documentation supporting that the facility is below the thresholds, the Coast Guard considers it no longer subject to 33 C.F.R. part 106 requirements and the facility will no longer be subject to security inspections.

Our analysis of Coast Guard inspections data shows that the Coast Guard generally inspected a greater percentage of floating OCS facilities than fixed OCS facilities (see table 2). For example, from 2008 through 2010, the Coast Guard conducted annual security inspections of 54 percent of floating OCS facilities, compared to 24 percent of fixed OCS facilities. During our interviews with Coast Guard marine inspectors and their supervisors, we learned that some field units did not know that they were responsible for conducting security inspections of fixed OCS facilities, approximately one-third of which are not staffed because operations are automated. For example, marine inspectors in the Coast Guard field unit that oversees more than half of the OCS facilities stated that they had only recently learned that they were responsible for conducting security inspections of fixed OCS facilities. These marine inspectors stated that they thought that security inspections of the fixed OCS facilities within their area of responsibility were carried out by another field unit and that they had only been conducting annual security inspections of the floating OCS facilities. Further, other Coast Guard officials stated that it is easier to arrange for security inspections of floating OCS facilities because marine inspectors visit those facilities more frequently for other types of inspections, such as hull or safety inspections, whereas for fixed OCS facilities, the Coast Guard conducts an initial safety inspection when they are first installed and then are only

required to visit the fixed OCS facilities once a year for annual security inspections.⁴⁰

Table 2: Security Inspections Required and Conducted of OCS Facilities, by Type, 2008 through 2010

Type	Inspections required	Inspections conducted	Percentage
Fixed OCS facility	119	28	24%
Floating OCS facility	41	22	54%

Source: GAO analysis of data provided by the U.S. Coast Guard.

The Coast Guard does not have procedures in place to help ensure that its field units conduct security inspections of OCS facilities annually in accordance with its guidance. *Standards for Internal Control in the Federal Government* state that internal controls should include control activities, such as policies, procedures, and mechanisms that help ensure management directives are carried out. However, the Coast Guard does not have such control activities in place. For example, the Coast Guard’s OCS facility guidance does not describe specific procedures for the way in which Coast Guard staff should track whether annual security inspections have been conducted. Further, Coast Guard district officials and most local field unit supervisors and marine inspectors we spoke with do not maintain any kind of tool, such as a spreadsheet or calendar, to remind them when annual security inspections of OCS facilities are due. Coast Guard officials from five of the six Coast Guard field units that conduct annual security inspections of OCS facilities told us that they do not maintain a spreadsheet or other management tool to track whether annual security inspections had been conducted. For example, at three of these locations, Coast Guard officials told us they rely on owners and operators to inform them when inspections were due rather than tracking themselves when annual inspections were due. As a result of the lack of procedures or control activities to manage the offshore security inspection program, the Coast Guard is not positioned to ensure OCS facility

⁴⁰ Per Coast Guard regulations, all fixed offshore facilities engaged in OCS activities are subject to inspection by BSEE, formerly the Minerals Management Service, on behalf of the Coast Guard. According to a mutually agreed upon arrangement between the two agencies, the Coast Guard will conduct the initial safety inspection on new fixed OCS facilities, after which BSEE handles subsequent safety inspections. However, for floating facilities the Coast Guard still carries out various inspections throughout the year, including hull inspections.

compliance with established maritime security requirements for most of the OCS facilities. Without conducting annual inspections of OCS facilities, the Coast Guard may not be meeting one of its stated goals of reducing the risk and mitigating the potential results of an act that could threaten the security of personnel, the OCS facility, the environment, and the public.

During the course of our review, Coast Guard officials stated that they are planning to update the OCS facility guidance, policies, and procedures—which have not been updated since 2003—for implementing security requirements for OCS facilities. In September 2011, in response to our findings, Coast Guard officials indicated that they may issue a separate policy letter to Coast Guard marine inspectors to address these weaknesses, but they noted that they were still considering how to best address the problem to achieve a higher level of compliance.

Inconsistent Documentation and Database Limitations

In addition to challenges in the Coast Guard's inspection efforts, inconsistent documentation of security inspections as well as limitations in the MISLE database—the database in which security inspection results are recorded—hinder the Coast Guard's ability to manage the offshore security inspection program or analyze inspection data needed for making management decisions about OCS facilities. During the course of our review, we found inconsistencies in how security inspection data were recorded in MISLE. For example, in most cases, marine inspectors select the "MTSA-related" inspection type to designate that an annual security inspection of an OCS facility was completed in accordance with 33 C.F.R. part 106. However, among the 50 security inspections of OCS facilities that were conducted from 2008 through 2010, marine inspectors did not select this inspection type for 5 records.⁴¹ Instead, the inspectors selected another inspection type (such as a safety inspection) and indicated in the narrative section that a security inspection was conducted. Without reviewing the narrative of each inspection report, Coast Guard management may not be able to determine if security inspections of OCS

⁴¹ For more information on how we addressed and corrected data issues pertaining to the inconsistencies in how security inspections were recorded in MISLE, see appendix I.

facilities were conducted.⁴² In July 2011, and in response in part to our review, the Coast Guard issued new MISLE guidance on documenting the annual security inspections of OCS facilities in MISLE and distributed this guidance to all of the relevant field units. Specifically, the guidance provides step by step instructions for entering information on annual security inspections into MISLE for both fixed and floating OCS facilities. If effectively implemented, this guidance should help to ensure that all future security inspections of OCS facilities are recorded consistently, which would enhance program management and oversight of these facilities.

In addition to the inconsistencies with how inspections are recorded in MISLE, we also identified limitations with the MISLE database in the following three areas:

- **No OCS facility data field:** There is no data field⁴³ in the MISLE database to identify a facility as an OCS facility, which makes it difficult to readily analyze and summarize information on this type of facility.⁴⁴ Coast Guard officials recognize that not having an OCS facility data field makes it difficult to readily summarize information and they created an alternative method using standardized language

⁴² Our prior work involving the MISLE database has also noted flaws that complicated the Coast Guard's ability to analyze inspection activities. For example, in February 2008 we reported that the Coast Guard was limited in its ability to accurately assess shoreside facility oversight activities because the MISLE database suffered from such problems as missing, duplicate, and inconsistent compliance activity data. We recommended that the Secretary of Homeland Security direct the Commandant of the Coast Guard to assess MISLE compliance data, including the completeness of the data, data entry, and consistency, and make any changes needed to more effectively use MISLE data. DHS agreed with this recommendation. In response to our findings in that report, the Coast Guard described steps taken to improve consistency and data entry time. In June 2011, DHS's Office of the Inspector General reviewed the Coast Guard's offshore vessel inspection program and similarly noted that improvements are needed to ensure the completeness and accuracy of vessel safety inspection data input into MISLE. See GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, [GAO-08-12](#) (Washington, D.C.: Feb. 14, 2008).

⁴³ A data field is a location in a data set where the same information (such as facility name) is entered for each case.

⁴⁴ For more information on how we identified OCS facilities in the MISLE data for our analysis, see appendix I.

in another data field.⁴⁵ However, this alternative method only applies to the fixed OCS facilities and there is no alternative method to identify floating OCS facilities in MISLE. Officials noted that it would be useful if there were a data field for both fixed and floating OCS facilities because this would allow the Coast Guard field units to generate a report each year that would help local officials see when security inspections are due for the OCS facilities within their area of responsibility.

- **Multiple entries for facilities:** In the MISLE data we reviewed and analyzed, we found that 14 of the 57 OCS facilities were listed multiple times under slightly different facility names and, as such, had multiple entries in the database. According to Coast Guard officials, because of the MISLE database's limited search functions, staff wishing to enter the results of an inspection or other activity might not be able to find the OCS facility in MISLE because the information they entered was not an exact match to how the facility was recorded in MISLE. Consequently, the staff may assume that the facility is not in MISLE and create a new entry to record their results. For example, Coast Guard staff might not be able to find the "Green Canyon 55" facility in MISLE because the facility name was entered into MISLE initially as "GC 55." As a result, data records in MISLE are listed under several names and identification numbers, which make it difficult to determine how many security inspections have been conducted of an OCS facility.⁴⁶ Coast Guard marine inspectors stated this issue can make it difficult to (1) locate previous inspection records, which the marine inspectors review prior to conducting an inspection and (2) compile a history of a facility's inspections.
- **OCS facilities may be considered either "facilities" or "vessels" in MISLE:** Infrastructure in the MISLE database is classified as either a "facility" or a "vessel," and information on these two types cannot be gathered simultaneously. While the fixed OCS facilities are considered "facilities" in the MISLE database, the floating OCS

⁴⁵ Using the alternative method, officials select the data field for shore-based facilities regulated under 33 C.F.R. part 105 and note that the fixed OCS facility is regulated under 33 C.F.R. part 106 in its facility description. According to officials, this method will help them to identify the OCS facilities regulated under 33 C.F.R. part 106 until other changes are made to the MISLE database.

⁴⁶ For more information on how we addressed and corrected data issues pertaining to multiple entries for the same OCS facility, see appendix I.

facilities are considered “vessels.”⁴⁷ This distinction exacerbates the potential for creating multiple entries in MISLE for the same OCS facility. For example, 13 of the 57 OCS facilities were listed in the MISLE database as both a “facility” and a “vessel” under different names and identification numbers. Further, officials at one location reported that they entered security inspection reports for the facilities within their area of responsibility into MISLE twice—once as a vessel and once as a facility. As a result, data analysts cannot gather information on both fixed and floating OCS facilities at the same time without first searching for and eliminating duplicate entries, which complicates data analyses.⁴⁸

The Coast Guard could benefit from enhancing and facilitating the use of performance information to make improved management decisions.⁴⁹ One way to enhance the use of performance information is to improve the usefulness of such information to better meet management’s decision-making needs. We reported previously that to be useful, performance information must meet users’ needs for completeness, accuracy, consistency, timeliness, validity, and ease of use.⁵⁰ However, due to the MISLE database limitations noted above, it is difficult for Coast Guard managers to determine if annual security inspections have been conducted. Coast Guard officials indicated that they are taking action to address not having an OCS data field and that they plan to create such a data field for both fixed and floating OCS facilities when they release an updated version of MISLE in early 2013. However, while the Coast Guard is in the process of updating MISLE, it remains unclear whether problems with (1) multiple facility names and (2) considering OCS facilities both vessels and facilities will be addressed in the updated MISLE version. Further, the new MISLE guidance on documenting security inspections for OCS facilities in MISLE that was issued in July 2011 does not

⁴⁷ According to Coast Guard officials, floating OCS facilities are considered “vessels” in MISLE based on their structural components. For example, floating OCS facilities, like vessels, have hulls and require hull inspections.

⁴⁸ For more information on how we addressed and corrected data issues pertaining to OCS facilities listed as both a fixed and floating OCS facility in MISLE, see appendix I.

⁴⁹ We have identified such practices in prior work. See GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, [GAO-05-927](#) (Washington, D.C.: Sept. 9, 2005).

⁵⁰ See GAO, *Results-Oriented Government: GPRHA Has Established a Solid Foundation for Achieving Greater Results*, [GAO-04-38](#) (Washington, D.C.: Mar. 10, 2004).

describe policies or procedures that would address the MISLE database limitations described above. Addressing such problems, either in the updated version of MISLE or through updated guidance that addresses these problems, could enhance the Coast Guard's ability to summarize data on OCS facilities and make informed decisions.

Actions Are Needed to Further Ensure the Security of Deepwater Ports

Coast Guard Actions to Ensure Security

The Coast Guard has taken actions to ensure the security of deepwater ports that are similar to actions it has taken to ensure the security of OCS facilities. For example, the three deepwater ports are located in areas that are covered by Area Maritime Security Plans—the LOOP is mentioned in the Gulf of Mexico Area Maritime Security Plan, and the two LNG deepwater ports in Massachusetts Bay are mentioned in the Boston Area Maritime Security Plan.⁵¹ Further, the Coast Guard has conducted some exercises that address the security of the LOOP, which was an attack target in a 2008 exercise as well as in NLE 2009.⁵² The Coast Guard has also reviewed and approved deepwater port operations manuals for the three deepwater ports that, among other things, must include deepwater port security plans that are comparable to the security plans required for OCS facilities pursuant to 33 C.F.R. part 106.⁵³ In addition, the Coast Guard has taken additional actions to ensure the security of deepwater

⁵¹ The most recent update to the Boston Area Maritime Security Plan occurred in March 2009, prior to one of the two LNG deepwater ports becoming operational. However, the anticipated time frame for the port becoming operational is mentioned in the plan. The ongoing and annual reviews and exercises of Area Maritime Security Plans support periodic plan refinements between the formal review and approvals, which occur on a 5-year cycle, to maintain currency. The next formal nationwide Area Maritime Security Plan review and approval cycle is scheduled to be completed in 2014.

⁵² According to the Coast Guard, Coast Guard exercises have not included the two LNG deepwater ports in the Massachusetts Bay because, due to the infrequency of shipments arriving at the deepwater port, other port facilities are considered to be higher risk. However, the deepwater port owners and operators have conducted exercises and drills as required by regulation.

⁵³ See 33 C.F.R. § 150.5(x).

ports. For example, the Coast Guard has established security zones around the two LNG deepwater ports in Massachusetts Bay.⁵⁴ In the context of a deepwater port, a security zone is a designated area for such time as deemed necessary to safeguard the port from destruction, loss, or injury from sabotage or other subversive acts.⁵⁵ In particular, the establishment of a security zone prohibits a person or vessel from entering the designated area without permission and authorizes the Coast Guard to take appropriate enforcement actions against such unauthorized persons or vessels.⁵⁶ Additionally, the Coast Guard has access to live video feeds from the two LNG deepwater ports in Massachusetts Bay.⁵⁷

Coast Guard Could Improve the Security of Deepwater Ports by Conducting Security Inspections

The Coast Guard has conducted only one security inspection of a deepwater port from 2008 through 2010. Following the LOOP's 2010 annual self-inspection—an inspection conducted by owners and operators that generally assesses maintenance and repair issues—Coast Guard marine inspectors conducted a security inspection at the LOOP in November 2010 and found deficiencies.⁵⁸ Specifically, Coast Guard marine inspectors determined that the facility security officer was not familiar with the facility security plan. Based on MISLE inspection records, this was the only security inspection conducted for a deepwater port from 2008 through 2010. However, according to Coast Guard officials, Coast Guard marine inspectors have observed security measures at the deepwater ports as part of their responsibilities for overseeing the vessels that connect to these ports. For example, as part of a vessel examination,

⁵⁴ According to the Coast Guard, it does not have authority to establish permanent security zones around OCS facilities or deepwater ports located beyond the territorial sea, which extends 12 nautical miles from the coast. The two LNG deepwater ports in Massachusetts Bay are located within the territorial sea, but the LOOP is further away from the coast.

⁵⁵ See 33 C.F.R. pt. 165, subpart D.

⁵⁶ See 33 C.F.R. § 165.33. Violation of Coast Guard-established security zones may subject the offending party to civil or criminal penalties as appropriate.

⁵⁷ The LOOP also has a private security patrol boat that monitors the area surrounding the deepwater port.

⁵⁸ See 33 C.F.R. §§ 150.100 (providing that a marine inspector may conduct an inspection of a deepwater port, with or without advance notice, at any time the Officer in Charge of Marine Inspection deems necessary); 150.105 (providing that the owner or operator of each manned deepwater port must ensure compliance with applicable requirements through regular inspections conducted annually).

the Coast Guard might observe whether physical security measures at the deepwater port prevent unauthorized access to the port and the vessel.⁵⁹ Additionally, Coast Guard officers can ask questions of the vessel crew about security practices to ensure that the vessel is complying with either U.S. or international security requirements, as applicable.

Because deepwater ports are subject to different regulations than OCS facilities, the Coast Guard has different sets of policies and procedures for these two types of facilities.⁶⁰ Unlike its requirement for OCS facilities, the Coast Guard's deepwater port guidance does not call for annual security inspections.⁶¹ According to Coast Guard officials, deepwater ports were specifically excluded from the regulatory definition of OCS facilities because of the different statutory and regulatory regimes governing these two types of offshore energy infrastructure and because the security risk factors at deepwater ports may be different from those at OCS facilities.⁶² For example, deepwater ports are not connected, directly

⁵⁹ The Coast Guard conducts inspections of U.S.-flagged vessels and examinations of foreign-flagged vessels pursuant to 33 C.F.R. part 104 to ensure compliance with applicable security requirements. See 33 C.F.R. § 104.115. All of the vessels that deliver LNG to the deepwater ports in Massachusetts Bay are foreign-flagged.

⁶⁰ Although deepwater ports are not considered to be "MTSA-regulated" (that is, do not meet the regulatory criteria of 33 C.F.R. parts 101-106), Coast Guard officials explained that MTSA nonetheless influenced the security requirements for deepwater ports. For example, deepwater ports must have a security plan comparable to security plans required under part 106 and must participate in the TWIC program.

⁶¹ We use the term deepwater port guidance to refer to the Coast Guard's NVIC 03-05, Guidance for Oversight of Post-Licensing Activities Associated with Development of Deepwater Ports (May 16, 2005). There are two types of inspections that apply to deepwater ports: Coast Guard biennial inspections and owner/operator self-inspections. Coast Guard guidance states that the Coast Guard should conduct an initial inspection prior to a port's initial operation and biennially thereafter. However, the scope of the biennial inspections is left to the discretion of the responsible Coast Guard field unit. By regulation, the owner or operator of each staffed deepwater port must ensure that the port is annually inspected to determine whether the facility is in compliance with regulatory requirements. See 33 C.F.R. § 150.105. However, according to the Coast Guard, the self-inspections typically focus on maintenance and repair issues. The LOOP, the only staffed deepwater port, has submitted self-inspection reports to the Coast Guard; however, none of its self-inspection reports from 2008 through 2010 specifically addressed security issues. Deepwater port inspection requirements are not security specific.

⁶² Whereas the Coast Guard promulgates regulations governing the security OCS facilities pursuant to MTSA, the Coast Guard promulgates regulations governing deepwater ports pursuant to the Deepwater Port Act of 1974, Pub. L. No. 93-627, 88 Stat. 2126 (1975), as amended. See 33 U.S.C. §§ 1501-24.

or via a pipeline network, to the source of oil or natural gas production. Therefore, the oil or natural gas that could be released as a result of an attack on a deepwater port would be limited to the volume contained in the tankers that connect to the deepwater port rather than the generally larger volumes contained in source wells that are connected to OCS facilities. As a result, according to Coast Guard officials, an attack on a deepwater port could have lesser consequences compared to an attack on an OCS facility that is directly connected to an oil or natural gas source.

While current Coast Guard deepwater port guidance does not require annual security inspections of deepwater ports, the Coast Guard is mandated by statute to verify the effectiveness of facility security plans for those facilities that could be involved in a transportation security incident.⁶³ While deepwater port operators are required to develop security plans as part of their operations manuals, which are to be approved by the Coast Guard, and the Coast Guard acknowledges that its mandate to verify the effectiveness of security plans applies to deepwater ports where an incident may meet the definition of a transportation security incident, the Coast Guard has not implemented procedures for conducting inspections to verify the effectiveness of the deepwater port security plans on annual basis. Officials at Coast Guard headquarters, however, recognize that an incident at the LOOP or either of the two LNG deepwater ports in Massachusetts Bay could be considered a transportation security incident.

We discussed the statutory requirement to assess the effectiveness of facility security plans and the general lack of security inspections at deepwater ports with Coast Guard officials who generally agreed with our observations. Based on this discussion, Coast Guard officials stated that by the end of 2011 they plan to (1) update applicable Coast Guard

⁶³ A transportation security incident is defined as a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. See 33 C.F.R. § 101.105. Subject to the availability of appropriations, the Coast Guard has responsibility for periodically verifying the effectiveness of the security plan at each facility that may be involved in a transportation security incident, but not less than two times per year, at least one of which should be an inspection of the facility that is conducted without notice to the facility. See 46 U.S.C. § 70103(c)(2)(A), (c)(4)(D). Although the Coast Guard does not consider deepwater ports to be OCS facilities for purposes of part 106 security regulation, the Coast Guard recognizes that a deepwater port may nonetheless be involved in a transportation security incident.

guidance to require annual security inspections of deepwater ports and (2) add new procedures for conducting such security inspections. In addition to this Coast Guard headquarters initiative, the Coast Guard field unit in Boston is planning to develop and implement a local security inspection program for the two LNG deepwater ports in Massachusetts Bay, and the Coast Guard field unit in Morgan City, Louisiana, plans to perform annual site safety and security inspections at the LOOP.

As the Coast Guard moves forward with updating its deepwater port guidance, one challenge it faces is the inherent differences between the LOOP and the two LNG deepwater ports. These differences may necessitate approaching security inspections of these facilities in different ways. For example, the LOOP and the two LNG deepwater ports in Massachusetts Bay differ in terms of their potential consequences, economic importance, and physical structure.

- **Potential consequences of an incident may be greater for the LOOP than for the LNG deepwater ports:** While the Coast Guard views the LOOP and the LNG deepwater ports as having the potential for a transportation security incident, an incident at the LOOP could have greater consequences than an incident at the LNG ports. In particular, an oil spill resulting from an attack on the LOOP could have greater environmental consequences than the release of LNG from an attack on one of the LNG deepwater ports because oil does not dissipate as quickly as LNG does, and it must be removed from the water. Additionally, there can be personnel stationed at the LOOP's offshore location; therefore, potential death and injury consequences could also be a consideration for the LOOP. In contrast, no staff are stationed at the LNG deepwater ports, except when a tanker is attached to the buoy and offloading LNG. Therefore, if an incident were to occur at an LNG deepwater port, such as an explosion, the potential for deaths or injuries could be limited to the crew aboard the LNG tanker.
- **The LOOP has greater importance to the economy than the LNG deepwater ports:** The LOOP is the only crude oil port in the United States that can receive oil transfers from the largest crude oil tankers. Additionally, about half of the oil consumed in the United States is imported and the LOOP accounts for approximately 10 percent of U.S. crude oil imports. In contrast, most of the natural gas consumed in the United States is produced domestically, and the two LNG deepwater ports import a relatively low volume of LNG compared to onshore LNG port facilities. As a result, an attack on the LOOP could

have greater economic impact than an attack on the LNG deepwater ports.

- **Due to the structural nature of the ports, security inspections of the LOOP may be more feasible than security inspections of the LNG deepwater ports:** In addition to the buoys that connect to oil tankers, the LOOP has a fixed platform structure above the water surface, similar to some of the OCS facilities, and the Coast Guard plans to conduct on-site inspections of the LOOP. In contrast, the structural nature of the two LNG deepwater ports may make these ports difficult to inspect. Specifically, the LNG deepwater ports are submerged buoy systems, meaning that buoys are submerged whenever they are not connected to an LNG tanker, and these buoys are connected by pipeline to shoreside facilities. As a result, when an LNG tanker is not connected to the port's buoy, there is no visible infrastructure above the water to inspect. Coast Guard officials in the Boston field unit, which oversees these deepwater ports, said that they could conduct an onshore security inspection that could include a review of the deepwater port security plan with the facility security officer to discuss how security measures are being implemented.

The differences between the LOOP and the two LNG deepwater ports described above could play a role in how the Coast Guard decides to conduct security inspections of these deepwater ports. For example, on-site inspections of the LOOP could be warranted because of its importance and the fact that a major part of the facility is above the water, while inspections of LNG deepwater ports could potentially be done, at least in part, at those ports' onshore facilities since these ports do not have infrastructure above the water, except when a tanker is offloading. As the Coast Guard updates its guidance for deepwater ports, the factors described above could be considered in determining how to carry out future security inspections of these deepwater ports.

Database and Guidance Limitations Could Hinder Inspections

When the Coast Guard begins annual security inspections of deepwater ports, limitations in the MISLE database may complicate Coast Guard management and oversight of such facilities. Similar to the problems we found with MISLE regarding OCS facilities, we also noted the following weaknesses in MISLE specific to deepwater ports:

- **Deepwater port data field incorrectly used for other types of infrastructure:** The MISLE database contains a data field for deepwater ports; however, this term is not defined in MISLE guidance

and has been incorrectly applied to facilities that do not meet the definition of a deepwater port in applicable federal regulations.⁶⁴ According to Coast Guard officials, staff sometimes select the deepwater port data field for shoreside ports that have deep drafts, which allow large ships to enter these ports. For example, the MISLE deepwater port data we reviewed identified 80 facilities as deepwater ports rather than just the 3 currently active and 1 soon to be decommissioned deepwater ports that meet the definition established by applicable federal regulations. Further, Coast Guard MISLE guidance does not define a deepwater port nor does it make reference to the applicable federal regulations or definitions. As a result, it is difficult to identify deepwater ports in MISLE for the purpose of summarizing data that may inform management decisions.

- **Multiple entries for deepwater ports:** We also found that some of the deepwater ports in MISLE were listed multiple times under slightly different names. For example, the LOOP appeared in MISLE under four different names. This situation may have occurred in part because the Coast Guard's MISLE guidance does not provide naming conventions for how deepwater ports are to be entered into MISLE. The existence of multiple names for the same deepwater port and the limited search function of MISLE make it difficult for Coast Guard marine inspectors and managers to locate previous inspection records.

Similar to what we found with MISLE regarding OCS facilities, limitations in the MISLE database, as well as no guidance on recording inspection results into MISLE, make it difficult for the Coast Guard to analyze security inspection results and other information on deepwater ports. As previously discussed, performance information must meet users' needs for completeness, accuracy, and consistency if it is to be useful. According to the *Standards for Internal Control in the Federal Government*, controls such as policies, procedures, and mechanisms help ensure management directives are carried out. One way to enforce management directives involves policies and procedures that ensure accurate and timely recording of transactions and events, such as

⁶⁴ 33 C.F.R. § 148.5 defines a deepwater port as a fixed or floating manmade structure located beyond state seaward boundaries that is used or intended for use as a port or terminal for the transportation, storage, or handling of oil or natural gas for transportation to any state and includes the transportation of oil or natural gas from the United States's OCS.

security inspections. However, the Coast Guard's MISLE guidance does not describe procedures related to information on deepwater ports and it is difficult to use the information currently in the database as a management tool. Correcting MISLE limitations and developing guidance related to deepwater ports, including information on how deepwater ports are named in MISLE and how the results of security inspections are to be entered into MISLE, would allow the Coast Guard to better manage security inspections and verify that the deepwater ports are complying with applicable maritime security requirements.

Coast Guard Has Limited Authority over the Security of MODUs Registered to Foreign Countries

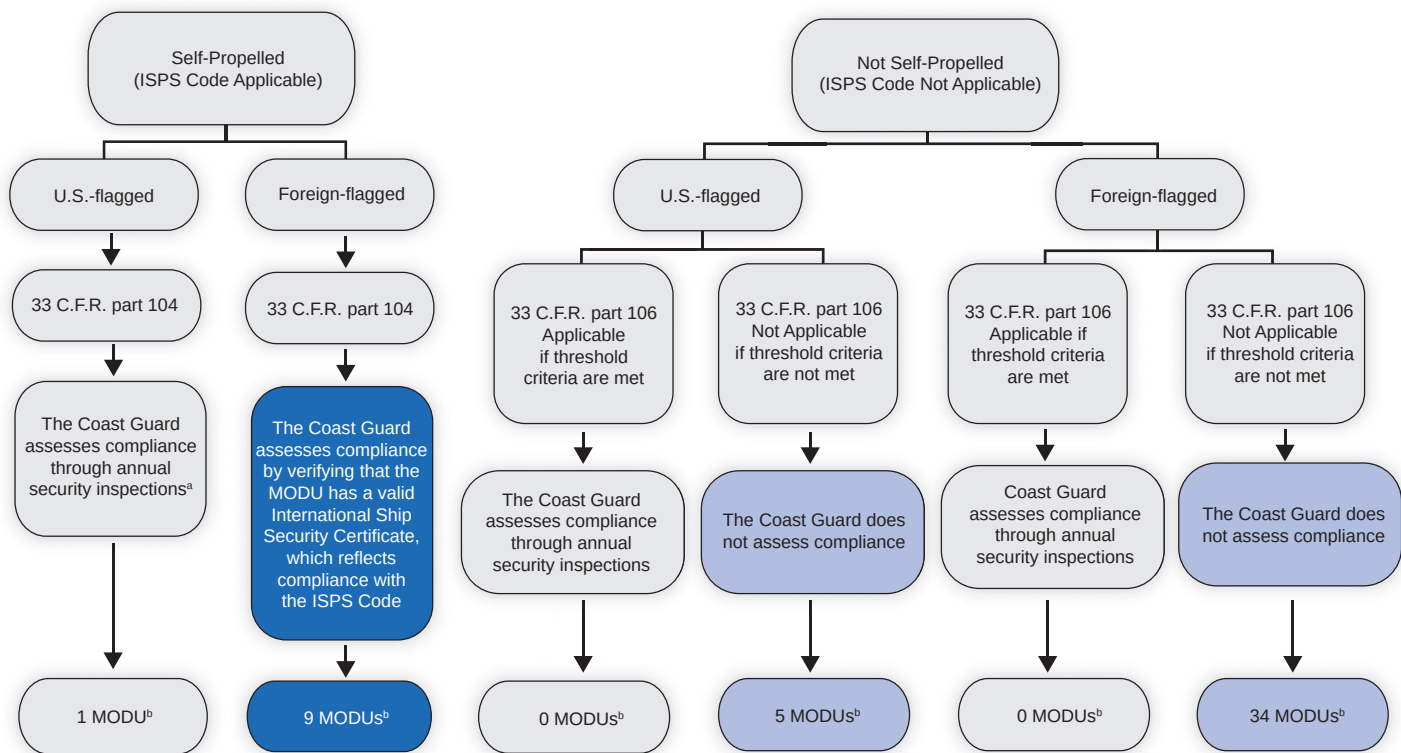
While the *Deepwater Horizon* incident was not the result of a breakdown in security procedures or the result of a terrorist attack, the loss of the *Deepwater Horizon* and the resulting oil spill have raised concerns about U.S. oversight over MODUs that are registered to foreign countries.⁶⁵ In this regard, various circumstances govern the extent to which the Coast Guard oversees the security of MODUs. In general, MODUs operating on the OCS implement security measures consistent with applicable security requirements—specifically, they implement requirements in accordance with U.S. security regulations and the International Maritime Organization's ISPS Code.⁶⁶ Depending on the particular characteristics and operations of the MODU—for example, its method of propulsion or its personnel levels—it may be subject to Coast Guard security regulations governing vessels (33 C.F.R. part 104) or OCS facilities (33 C.F.R. part 106). MODUs will fall under applicable Coast Guard regulations if (1) they are self-propelled—that is, they are capable of relocating themselves, as opposed to other types that require another vessel to tow them—in which case they are subject to the ISPS Code and 33 C.F.R. part 104, or (2) they meet production or personnel levels specified in 33 C.F.R. part 106. In the case of self-propelled, foreign-flagged MODUs, the Coast Guard will assess compliance with part 104 by reviewing a MODU's International Ship Security Certificate, which certifies compliance with the ISPS Code; in all other cases where MODUs are subject to Coast Guard security requirements, the Coast Guard assesses compliance with part

⁶⁵ The *Deepwater Horizon* was registered to the Republic of the Marshall Islands.

⁶⁶ The Coast Guard's security regulations—33 C.F.R. parts 101 through 106—are consistent with the ISPS Code. The International Maritime Organization is the international body responsible for improving maritime safety. It primarily regulates maritime safety and security through the International Convention for the Safety of Life at Sea, 1974.

104 or part 106 through annual security inspections.⁶⁷ Figure 3 illustrates the types of MODUs, the applicable security requirements, and the means by which the Coast Guard assesses compliance.

Figure 3: Coast Guard Security Requirements Applicable to MODUs Operating in U.S. Federal Waters



Source: GAO analysis of ISPS Code, 33 C.F.R. parts 104 and 106, and Coast Guard MISLE data, and U.S. Coast Guard.

^aA self-propelled, U.S.-flagged MODU must also comply with the ISPS Code and possess an International Ship Security Certificate if it is on an international voyage. 33 C.F.R. part 104 security regulations, which govern self-propelled, U.S.-flagged MODUs, are consistent with the ISPS Code.

^bThere are no MODUs operating in U.S. federal waters that meet the threshold criteria of 33 C.F.R. part 106. The numbers for other categories of MODUs shown above—those that are subject to 33 C.F.R. part 104 and those that do not meet the threshold criteria of 33 C.F.R. part 106—are the number of MODUs in each category that are, according to the Coast Guard, drilling in the Gulf of Mexico as of September 23, 2011.

⁶⁷ The *Deepwater Horizon* was self-propelled and foreign-flagged.

-
- **Self-propelled MODUs:** Among other things, the ISPS Code establishes an international framework, involving cooperation between contracting governments, government agencies, local administrations, and the shipping and port industries to detect and assess security threats and take preventive measures against security incidents affecting ships or port facilities in international trade, and to ensure confidence that adequate and proportionate maritime security measures are in place. MODUs that are self-propelled are considered vessels and are subject to the ISPS Code. In general, the country to which a vessel is registered (the flag state) enforces its own as well as applicable international requirements. Coast Guard regulations governing vessel security (33 C.F.R. part 104) are consistent with the requirements of the ISPS code. For example, a MODU may be registered to a foreign flag state, such as the Marshall Islands or Panama, and if self-propelled, the Coast Guard is able to ensure compliance with applicable U.S. security requirements by ensuring the MODU possesses a current International Ship Security Certificate issued by the flag state. Whereas the Coast Guard may physically inspect a U.S.-flagged MODU to ensure compliance with applicable security requirements, the Coast Guard's oversight of foreign-flagged MODUs is more limited.⁶⁸ For example, Coast Guard inspectors may board a self-propelled, foreign-flagged MODU to verify the issuance of an International Ship Security Certificate, observe security measures, and ask security related questions of personnel; however, absent consent from the flag state, the inspectors generally do not have authority to review the MODU's vessel security plan.
 - **MODUs that are not self-propelled:** In contrast, MODUs that are not self-propelled—those that require another vessel to move them from one location to another—are not subject to the ISPS Code, and countries in whose jurisdiction drilling occurs may individually determine how they choose to regulate such MODUs. In U.S. federal waters, both U.S.-flagged and foreign-flagged MODUs that are not self-propelled may be subject to the security requirements of 33 C.F.R. part 106, which govern OCS facilities, if they meet the applicable production or personnel thresholds. While some non-self-

⁶⁸ As a self-propelled, foreign-flagged MODU, the *Deepwater Horizon* was subject to the requirements of the ISPS Code. In July 2009, Coast Guard inspectors conducted a certificate of compliance examination on the *Deepwater Horizon* in which the inspectors reviewed all applicable licenses and other compliance documents, including those related to security; the inspectors found no deficiencies during this examination.

propelled MODUs could meet the personnel thresholds that would make them subject to part 106, most such MODUs do not meet the applicable production or personnel thresholds.⁶⁹ Since 2008, security regulations for OCS facilities have applied to one foreign-flagged MODU and no U.S.-flagged MODUs. Because most MODUs are not regulated for security under part 106, the owners and operators are not required to provide security plans to the Coast Guard and the Coast Guard does not conduct security inspections.

The Coast Guard may not be fully aware of the security measures implemented by self-propelled, foreign-flagged MODUs because of its limited oversight of such MODUs. The Coast Guard and BOEMRE conducted a joint investigation into the *Deepwater Horizon* incident, and the Coast Guard's report from the investigation emphasized the need to strengthen the system of Coast Guard oversight of foreign-flagged MODUs. The Coast Guard's report from the joint investigation stated that the Coast Guard's regulatory scheme for overseeing the safety of foreign-flagged MODUs is insufficient because it defers heavily to the flag state to ensure safety. The report noted that deferring to a flag state could work if the flag state conducts inspections comparable to those conducted by the Coast Guard on U.S.-flagged MODUs; however, the report found deficiencies in the way that the flag state for the *Deepwater Horizon* exercised its oversight responsibilities. The investigation also found that Coast Guard examinations of foreign-flagged vessels, which include foreign-flagged, self-propelled MODUs, are less stringent than for U.S.-flagged vessels, and the report stated that had the *Deepwater Horizon* been a U.S.-flagged MODU, the Coast Guard likely would have become aware of some of the deficiencies onboard. The joint investigation team recommended, among other things, that the Commandant of the Coast Guard develop more comprehensive inspection standards for foreign-flagged MODUs operating on the OCS. The Commandant concurred with this recommendation and has chartered an Outer Continental Shelf Activities Matrix Team, which has been tasked with providing recommendations on the establishment and implementation of an

⁶⁹ Currently, there are no MODUs subject to regulation under 33 C.F.R. part 106. For a MODU to be regulated under 33 C.F.R. part 106, it must exceed any one of three thresholds for production or personnel—(1) producing greater than 100,000 barrels of oil a day; (2) producing more than 200 million cubic feet of natural gas per day; or (3) hosting more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more. MODUs are involved with drilling rather than production, and therefore, they are only likely to be regulated under part 106 if they exceed the personnel threshold.

enhanced oversight regime for foreign-flagged MODUs on the U.S. OCS. While the investigation focused on issues that were not related to security, such as safety, these findings may have implications for security oversight because the Coast Guard also relies on the flag state to carry out responsibilities for assessing compliance with security requirements.

Further, in its report to the President, the National Commission on the BP *Deepwater Horizon* Oil Spill and Offshore Drilling reported that the risks involved with deepwater drilling are not yet completely addressed by reviews on where it is safe to drill, what could go wrong, or how to respond if something does go awry. While the report did not address the federal role in ensuring the security of offshore energy infrastructure, it did address risk management and challenges in responding to the consequences of an incident on a MODU operating in deepwater. In particular, the report noted that when a failure happens at such depths, regaining control is a formidable challenge. This potential for adverse consequences could be of greater concern as drilling technologies advance and more drilling occurs in deeper waters. For example, drilling in deeper water means that the Coast Guard or other response resources are generally going to be further away from the drilling sites. Figure 4 depicts the aftermath of the *Deepwater Horizon* explosion, which demonstrates the possible consequences of a successful terrorist attack or other security incident on offshore energy infrastructure.

Figure 4: Aftermath of the Explosion of the *Deepwater Horizon* Drilling Unit in the Gulf of Mexico, April 2010



Source: U.S. Coast Guard.

According to Coast Guard officials, it is likely that MODUs operating in deepwater would be subject to security requirements because the industry is increasingly using dynamically positioned MODUs that are able to maintain position without being anchored to the seabed, and as such MODUs are self-propelled, they would be subject to the ISPS Code and 33 C.F.R. part 104.⁷⁰ Additionally, the Coast Guard is aware of potential risks regarding MODUs and is conducting a study designed to help determine whether additional actions could better ensure the security of offshore energy infrastructure in the Gulf of Mexico, including MODUs. This study is expected to be completed in the fall of 2011. Gaining a fuller understanding of the security risks associated with MODUs could better inform Coast Guard decisions and potentially improve the security of these facilities. Further, the Coast Guard has implemented a new risk-based oversight policy for MODUs, including foreign-flagged MODUs, to address safety and environmental protection issues. This policy includes a targeting matrix to assist inspectors in determining whether a foreign-

⁷⁰ Deepwater is defined as water more than 1,000 feet deep.

flagged MODU may require increased oversight, based on inspection history or other related factors, through more frequent examinations by the Coast Guard. Additionally, the policy calls on Coast Guard field units to conduct random, unannounced examinations of a portion of all MODUs in their areas of responsibility. Although this policy does not directly address security, increased oversight resulting from this new policy could help mitigate some of the ways in which a MODU might be at risk of a terrorist attack.

Conclusions

The threat of terrorism and the significant damages resulting from the *Deepwater Horizon* incident point to the importance of the Coast Guard having robust policies and procedures in place to better ensure the security of OCS facilities and deepwater ports. Because the Coast Guard has not conducted annual security inspections of all OCS facilities in accordance with Coast Guard requirements, it could benefit from having procedures in place across its field units to ensure that such inspections are conducted. Because it is not complying with its established maritime security requirements, the Coast Guard may not be adequately meeting one of its stated goals of reducing the security risk and mitigating the potential results of an act that could threaten the security of personnel, the OCS facility, the environment, and the public. We also found limitations in the MISLE database which make it difficult for Coast Guard managers to determine if security inspections were conducted when reviewing the data, and current guidance does not describe policies and procedures that would fully address these limitations. By addressing some of these inconsistencies and other limitations, Coast Guard managers could more easily summarize data, identify issues related to OCS facilities, and use the data as a management tool to inform decision making.

Finally, we also found weaknesses in the MISLE database related to deepwater ports, such as not defining a deepwater port in MISLE guidance and the use of multiple names for such ports in the MISLE database. These weaknesses could inhibit the Coast Guard's ability to analyze information on security inspections of such ports. Although the Coast Guard has conducted only one security inspection of a deepwater port from 2008 through 2010, Coast Guard officials have recognized the importance of conducting annual security inspections of deepwater ports and are planning to update guidance to require such inspections and to address the way in which such inspections are to be conducted. Correcting MISLE limitations and developing guidance related to how deepwater ports are to be inspected and how the results of security

inspections are to be entered into MISLE could allow the Coast Guard to (1) ensure more consistency in how the results of inspections are recorded in MISLE, (2) better manage such security inspections, and (3) verify that the deepwater ports are complying with applicable maritime security requirements.

Recommendations for Executive Action

To strengthen the Coast Guard's efforts to ensure the security of OCS facilities and deepwater ports, we recommend that the Commandant of the Coast Guard take the following three actions:

- Develop policies and procedures to monitor and track annual security inspections for OCS facilities to better ensure that such inspections are consistently conducted.
- Make improvements to the MISLE database or MISLE guidance to better ensure that all OCS facilities, both fixed and floating, are accurately and consistently identified and that the results of security inspections are consistently recorded to allow for better data analyses and management of the security inspections process.
- Ensure that information on deepwater ports in MISLE can be used as a management tool for decision making. These actions should include (1) issuing guidance on how information on deepwater ports and their security inspections should be entered into MISLE; (2) defining deepwater ports in MISLE guidance; and (3) making any changes necessary in the database to ensure that deepwater ports regulated under 33 C.F.R. parts 148-150 can be identified within MISLE.

Agency Comments and Our Evaluation

On October 7, 2011, we provided a draft of this report to DHS and the Coast Guard for comment. On October 24, 2011, DHS provided written comments on the draft report, which are reproduced in full in appendix III. DHS and the Coast Guard concurred with the findings and recommendations in the report, and DHS stated that the Coast Guard is taking actions to implement our recommendations. The Coast Guard also provided technical comments, which we incorporated, as appropriate.

The Coast Guard concurred with our first recommendation that it develop policies and procedures to monitor and track annual security inspections for OCS facilities. Specifically, the Coast Guard stated that it is planning to update (1) its MISLE database to identify if a vessel or facility is regulated as an OCS facility under 33 C.F.R. part 106 and (2) its OCS facility policy guidance for field units to monitor and track annual security

inspections for OCS facilities to better ensure that such inspections are consistently conducted. These actions should improve the Coast Guard's ability to ensure that such inspections are consistently conducted on an annual basis, thereby addressing the intent of our recommendation.

The Coast Guard also concurred with our second recommendation to make improvements to the MISLE database or MISLE guidance to better ensure that all OCS facilities are accurately and consistently identified and that the results of security inspections are consistently recorded to allow for better data analyses and management of the security inspections process. Specifically, the Coast Guard stated that it developed guidance in 2011 to improve MISLE database quality. However, as we discuss in this report, the MISLE guidance issued in July 2011 does not describe policies or procedures that would address the MISLE database limitations we identified. In particular, we noted that within MISLE (1) there is no data field to identify OCS facilities, (2) there are multiple entries for some facilities, and (3) OCS facilities may be considered either "facilities" or "vessels." While the update to the MISLE database mentioned in relation to our first recommendation should address the need to identify OCS facilities in MISLE, the Coast Guard would need to issue additional guidance or further update MISLE to resolve the other two database limitations to fully address the intent of our recommendation.

Finally, the Coast Guard concurred with our third recommendation to ensure that information on deepwater ports in MISLE can be used as a management tool for decision making. The Coast Guard stated that it plans to modify MISLE to include facilities, such as deepwater ports, that do not fall under maritime security regulations in parts 101 to 106 of Title 33, Code of Federal Regulations, which implement provisions of MTSA. However, according to the Coast Guard, this modification will take a few years to complete. If, in addition to the MISLE modification, the Coast Guard issues accompanying guidance for how information on deepwater ports and their security inspections are to be entered into MISLE, these actions should, collectively, address the intent of our recommendation.

We are distributing this report to the Secretary of Homeland Security, the Commandant of the Coast Guard, and other relevant DHS officials. We are also sending copies of this report to interested congressional committees. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report or wish to discuss the matter further, please contact me at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink, appearing to read "Steve Caldwell", with a large checkmark at the end.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable Jay D. Rockefeller IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Fred Upton
Chairman
The Honorable Henry A. Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable John L. Mica
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Edward J. Markey
Ranking Member
Committee on Natural Resources
House of Representatives

The Honorable Michael T. McCaul
Chairman
Subcommittee on Oversight, Investigations, and Management
Committee on Homeland Security
House of Representatives

Appendix I: Scope and Methodology

This appendix describes in more detail our scope and methodology for analyzing the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database. We used this database to address the objectives on what the Coast Guard has done to ensure the security of Outer Continental Shelf (OCS) facilities and deepwater ports, and what additional actions, if any, are needed.

To determine the extent to which the Coast Guard conducted security inspections of OCS facilities, we analyzed security inspection data for OCS facilities recorded in the MISLE database for calendar years 2008 through 2010. We requested and obtained all MISLE inspection records for this time period for inspections conducted by the six field units responsible for conducting security inspections on all of the OCS facilities: Mobile, Alabama; Morgan City, Louisiana; New Orleans, Louisiana; Corpus Christi, Texas; Galveston, Texas; and Port Arthur, Texas. The MISLE data were provided in two spreadsheets: (1) a facility inspections spreadsheet that included fixed OCS facilities, among others and (2) a vessel inspections spreadsheet that included floating OCS facilities, among others. To assess the reliability of the MISLE data, we (1) performed electronic testing for errors in accuracy and completeness; (2) reviewed related documentation, such as MISLE user guides and data dictionaries; and (3) held meetings and exchanged correspondence with Coast Guard information systems officials and marine inspectors at the field units to discuss data entry, analysis procedures, and results. We analyzed the spreadsheets separately and, after taking the steps described below, manually merged them to summarize the results. We also obtained security inspection data for 2011 (through June 24, 2011), but did not report on this information because most annual security inspections of OCS facilities are typically not conducted until the fall.

Because MISLE does not have a data field for OCS facilities, we obtained a separate list from the Coast Guard that identified the 57 OCS facilities that had been regulated for security under 33 C.F.R. part 106 at any point from 2008 through 2010. We planned to use information contained in the list, including facility names, identification numbers, and the dates on which facilities were deregulated (that is, no longer subject to 33 C.F.R. part 106), to identify OCS facilities in the MISLE database. Prior to linking the Coast Guard list of OCS facilities to the MISLE data, we assessed the reliability of this list by interviewing Coast Guard officials responsible for maintaining the list, as well as marine inspectors at the field units who are to who conduct security inspections of the OCS facilities. In addition, to assess the completeness of the Coast Guard list, we used MISLE data to look for indicators that additional facilities were regulated for security

under 33 C.F.R. part 106 but were not included on the Coast Guard list. The indicators in the MISLE data that we considered included, for example, references made in the free-form, narrative portions of the MISLE data to “33 C.F.R. part 106” and “OCS” because these terms would likely be used to describe an OCS facility. When we found discrepancies, we brought these to the Coast Guard’s attention and worked with officials to correct them. After conducting these steps, we determined that the list was reliable for the purpose of identifying facilities that were regulated for security under 33 C.F.R. part 106 at some point from 2008 through 2010, which we refer to as OCS facilities, and that there were 57 such facilities during that time period.

During our interviews with Coast Guard officials and marine inspectors, we learned that the same OCS facility could be entered into MISLE multiple times under slightly different facility names and that there may be annual security inspection records for OCS facilities recorded under different facility names than those included in the Coast Guard list of OCS facilities. Failure to identify these facilities as the same facilities in the Coast Guard list could result in a possible undercount of annual security inspections at the 57 OCS facilities. To address this issue, we conducted searches for facilities in the MISLE database with matching, partially matching, or similar names and locations based on the Coast Guard list of 57 facilities to flag possible matches for OCS facilities in MISLE. Through these efforts, we identified alternative facility names for 14 of the OCS facilities on the Coast Guard list. For our analysis of the inspection records of the 57 OCS facilities, we combined the inspection records of the facilities identified in MISLE using the facility names provided by the Coast Guard with those of the 14 additional facility names we subsequently identified.

We also used the Coast Guard list of OCS facilities to determine the years for which the facilities were subject to the 33 C.F.R. part 106 requirements. According to the Coast Guard, an OCS facility that meets applicable production or personnel thresholds becomes regulated for security once its facility security plan is approved. A facility stays on the regulated list until the Coast Guard receives documentation from the facility that it no longer meets the thresholds to be regulated for security. In particular, once a facility has been below the production thresholds for 1 year or below the personnel thresholds for 30 days, the facility can inform the Coast Guard and provide supporting documentation. Upon reviewing this documentation, the Coast Guard may determine that the facility is no longer subject to the 33 C.F.R. part 106 requirements and it becomes “deregulated.” For our analysis, based on the date of

deregulation included in the Coast Guard list of OCS facilities, we only considered a facility to be subject to 33 C.F.R. part 106 for a particular year if it was regulated during the entire calendar year. For example, if a facility had its facility security plan approved prior to January 2008 and it was deregulated in October 2010, we considered that facility to be subject to security regulations in 2008 and 2009 only. We determined that there were 57 different facilities subject to 33 C.F.R. part 106 at some point from 2008 through 2010. In 2008, there were 56 OCS facilities. In 2009, 1 OCS facility became operational and 4 facilities were deregulated, for a total of 53 OCS facilities. In 2010, 2 facilities were deregulated for a total of 51 OCS facilities.

For our analysis of the MISLE inspection records of the 57 OCS facilities, we worked with Coast Guard officials to determine how marine inspectors documented annual security inspections of OCS facilities in MISLE because there was no guidance on documenting such inspections. This approach included identifying inspections in which marine inspectors selected a “MTSA-related” inspection type to designate that an annual security inspection was completed in accordance with 33 C.F.R. part 106, and we identified 52 security inspections from 2008 through 2010 in accordance with this approach. Further, at the advice of Coast Guard officials, we also searched the free-form, narrative portions of the MISLE data for indicators that a security inspection had been conducted. We used search terms such as “MTSA” and “security” in these searches and found 6 additional security inspections, for a total of 58 inspections. Prior to conducting our analysis of the data, we looked for duplicative security inspection records and errors and we removed 8 of these records, for a total of 50 annual security inspections. Specifically, 5 inspection records were removed because the same security inspection had been recorded twice in the MISLE database, including 1 of the 6 records that had been identified by reviewing the narrative. Of those 5 inspection records (1) 3 records had two inspections recorded on the same date under the same facility name and (2) 2 records had two inspections recorded on the same date under two different facility names for the same OCS facility. Further, 3 additional inspection records were removed because, based on the date of deregulation, the security inspection took place during a year that we determined the facility was not subject to regulation for security under 33 C.F.R. part 106. Therefore, out of the 50 annual security inspections we analyzed, 45 were identified in accordance with the Coast Guard’s suggested approach and 5 were identified solely through reviewing the inspection narratives.

We also analyzed MISLE data to determine the extent to which the Coast Guard had conducted security inspections of deepwater ports for calendar years 2008 through 2010. We requested and obtained all MISLE inspection records for 2008 through 2010 for deepwater ports as well as a MISLE-generated list of all facilities that were designated as deepwater ports in the database. To assess the reliability of the deepwater port data, we took similar steps with the data as those described above for OCS facilities. For example, we conducted searches in the MISLE database to identify deepwater ports with matching, partially matching, or similar names based on the names and locations of the deepwater ports. We also searched the narrative portions of the deepwater port inspection data for indicators that a security inspection had been conducted. Through these efforts, we identified one security inspection of a deepwater port from 2008 through 2010.

After conducting the above steps, we determined that the MISLE data were sufficiently reliable to determine the extent to which the Coast Guard conducted security inspections at OCS facilities and deepwater ports from 2008 through 2010. Our report discusses MISLE data problems in more detail, along with the steps the Coast Guard is taking to address some of the issues, and additional steps we believe are still needed.

We conducted this performance audit from October 2010 through October 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Status of Action Items from National Level Exercise 2009

This appendix provides additional information on action items developed in response to the National Level Exercise (NLE) 2009. In July 2009, the Coast Guard participated in NLE 2009, which focused on preventing a hypothetical attack on the nation's energy infrastructure, including offshore facilities in the Gulf of Mexico. In accordance with Coast Guard policy, the Coast Guard developed 111 remedial action items to address lessons learned in response to the exercise. According to Coast Guard data, as of May 31, 2011, 99 of these 111 action items were assigned to Coast Guard units and 12 of them were assigned to the Department of Homeland Security (DHS). According to those data, 88 of the 111 action items have been resolved and 23 are unresolved. For example, according to the data, the Coast Guard and DHS have not yet established a process for engaging the private sector to address the observation from the exercise that information sharing with private sector stakeholders occurred at multiple levels without clear synchronization. Among the 23 unresolved action items, 9 are pending resolution, meaning that the Coast Guard has taken steps to address an action item and is conducting a review to determine whether the steps are sufficient to change the action item's status to "resolved." According to Coast Guard data, among the 9 action items that are pending resolution, the latest anticipated resolution date is December 31, 2012.

Table 3: Status of Action Items Resulting from National Level Exercise 2009

Action office	Total	Resolved action items	Action items pending resolution	Action items not resolved
DHS	12	0	0	12
Coast Guard Commandant	34	26	6	2
Atlantic Area Command	4	4	0	0
District 8	24	21	3	0
Sector Corpus Christi	11	11	0	0
Sector Houston/Galveston	6	6	0	0
Sector New Orleans	20	20	0	0
Total	111	88	9	14

Source: GAO analysis of Coast Guard data maintained in the Coast Guard's Remedial Action Management Program database.

There is little information available on the status of action items assigned to DHS because, according to an official at DHS's Office of Operations Coordination and Planning, at the time the Coast Guard assigned these action items, DHS did not have a clear process for tracking DHS-internal action items. However, according to this DHS official, DHS is in the process of changing the way it tracks such action items. In particular, the

National Exercise Division within the Federal Emergency Management Agency is working to establish a DHS Exercise and Evaluation Program, which will include a process for the National Exercise Division to coordinate DHS internal action items.

Appendix III: Comments from the Department of Homeland Security



October 24, 2011

Stephen L. Caldwell
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-12-37, "MARITIME SECURITY: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note the report's acknowledgment that the United States Coast Guard has taken actions to address the security of Outer Continental Shelf (OCS) facilities and those of the deepwater ports. As the lead federal agency for maritime security, the Coast Guard remains committed to continuing its work with its interagency partners to meet the challenge of security in these facilities and ports for the safety of our Nation.

The draft report contained three recommendations directed to the Coast Guard, with which the Department concurs. Specifically, GAO recommended that the Commandant of the Coast Guard:

Recommendation 1: Develop policies and procedures to monitor and track annual security inspections for OCS facilities to better ensure that such inspections are consistently conducted.

Response: Concur. In 2008, Coast Guard District Eight requested the Marine Information for Safety and Law Enforcement (MISLE) database to include features to identify if a vessel or facility was regulated as an OCS facility under the *Maritime Transportation Security Act* (MTSA, 33 CFR 106). This feature has since been approved for addition to the MISLE database and will be incorporated into a future update of the database. Additionally, the Coast Guard is updating OCS facility policy guidance for field units and anticipates completion in calendar year (CY) 2012.

Recommendation 2: Make improvements to the MISLE database or MISLE guidance to better ensure that all OCS facilities, both fixed and floating, are accurately and consistently identified and that the results of security inspections are consistently recorded to allow for better data analyses and management of the security inspections process.

Response: Concur. The Coast Guard has developed a MISLE database process guide that has greatly improved database quality. This process guide was released in CY 2011.

Recommendation 3: Ensure that information on deepwater ports in MISLE can be used as a management tool for decision-making. These actions should include (1) issuing guidance on how information on deepwater ports and their security inspections should be entered into MISLE; (2) defining deepwater ports in MISLE guidance; and (3) making any changes necessary in the database to ensure that deepwater ports regulated under 33 C.F.R. parts 148-150 can be identified within MISLE.

Response: Concur. Deepwater ports have not traditionally been inspected under MTSA. However, in the permitting of deepwater ports, security plans are required to be developed. The modification of the MISLE database to include non-MTSA facilities is planned, but will require substantial lead time to complete. A request for a change to the database was approved in CY 2011.

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments were provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-9610 or caldwells@gao.gov

Acknowledgments

Key contributors to this report were Christopher Conrad, Assistant Director; Neil Asaba, Analyst-in-Charge; Alana Finley; Colleen McEneaney; and Erin O'Brien. Chuck Bausell contributed economic expertise, Pamela Davidson assisted with design and methodology, Thomas Lombardi provided legal support, Joshua Ormond provided assistance with graphics, and Jessica Orr provided assistance in report preparation.

Related GAO Products

Maritime Security: Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply. [GAO-11-883T](#). Washington, D.C.: August 24, 2011.

Maritime Security: Updating U.S. Counterpiracy Action Plan Gains Urgency as Piracy Escalates off the Horn of Africa. [GAO-11-449T](#). Washington, D.C.: March 15, 2011.

Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed By Seafarers, but Efforts Can Be Strengthened. [GAO-11-195](#). Washington, D.C.: January 14, 2011.

Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security. [GAO-11-207](#). Washington, D.C.: December 3, 2010.

Maritime Security: Actions Needed to Assess and Update Plan And Enhance Collaboration among Partners Involved in Countering Piracy off the Horn of Africa. [GAO-10-856](#). Washington, D.C.: September 24, 2010.

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. [GAO-10-940T](#). Washington, D.C.: July 21, 2010.

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. [GAO-10-400](#). Washington, D.C.: April 9, 2010.

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed. [GAO-09-337](#). Washington, D.C.: March 17, 2009.

Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented. [GAO-08-672](#). Washington, D.C.: June 20, 2008.

Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data. [GAO-08-12](#). Washington, D.C.: February 14, 2008.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. [GAO-08-141](#). Washington, D.C.: December 10, 2007.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

