

## 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](mailto: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.