GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-91, a report to Congressional Requesters

December 2005

RISK MANAGEMENT

Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure

Why GAO Did This Study

Congress and the President have called for various homeland security efforts to be based on risk management—a systematic process for assessing threats and taking appropriate steps to deal with them. GAO examined how three Department of Homeland Security components were carrying out this charge:

- the Coast Guard, which has overall responsibility for security in the nation's ports;
- the Office for Domestic Preparedness (ODP), which awards grants for port security projects; and
- the Information Analysis and Infrastructure Protection Directorate (IAIP), which has responsibility for developing ways to assess risks across all types of critical infrastructure.

GAO's work focused on identifying the progress each DHS component has made on risk management and the challenges each faces in moving further.

What GAO Recommends

This report contains many recommendations aimed at helping the three components face their next risk management challenges. DHS, including the Coast Guard, ODP, and IAIP, generally concurred with the report and its recommendations. DHS said that all three components have actions under way to address many of the recommendations in this report.

www.gao.gov/cgi-bin/getrpt?GAO-06-91.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Margaret Wrightson at (415) 904-2200 or wrightsonm@gao.gov.

What GAO Found

The three DHS components GAO studied varied considerably in their progress in developing a sound risk management framework for homeland security responsibilities. The varied progress reflects, among other things, each component's organizational maturity and the complexity of its task (see table below). The Coast Guard, which is furthest along, is the component of longest standing, being created in 1915, while IAIP came into being with the creation of the Department of Homeland Security in 2003. IAIP, which has made the least progress, is not only a new component but also has the most complex task—addressing not just ports but all types of infrastructure. The Coast Guard and ODP have a relatively robust methodology in place for assessing risks at ports; IAIP is still developing its methodology and has had several setbacks in completing the task. All three components, however, have much left to do. In particular, each component is limited in its ability to compare and prioritize risks. The Coast Guard and ODP can do so within a port but not between ports; IAIP has not demonstrated that it can do so either within or between all infrastructure sectors.

Each component faces many challenges in making further progress. Success will depend partly on continuing to improve various technical and management processes that are part of risk management. For example, obtaining better quality data from intelligence agencies would help DHS components estimate the relative likelihood of various types of threats—a key element of assessing risks. In the longer term, progress will depend increasingly on how well risk management is coordinated across agencies, because current approaches in many ways are neither consistent nor comparable. Also, weaving risk-based data into the annual budget cycle of program review will be important. Supplying the necessary guidance and coordination is what the Department of Homeland Security was set up to do and, as the Secretary of Homeland Security has stated, what it now needs increasingly to address. This is a key issue for the department as it seeks to identify relative risks and take appropriate actions related to the nation's homeland security activities.

Progress in Risk Management Is Affected by Organizational Maturity and Complexity of Risk Management Task

DHS component and degree of progress	Organizational characteristics	Complexity of risk management task
Coast Guard: furthest along in developing a risk management framework	Long-standing component; risk management activity began before September 11 attacks	Difficult: must be able to prioritize risks not only within ports but among them
Office for Domestic Preparedness: not as far along, but recent steps are good	Relatively new component transferred from Department of Justice to Department of Homeland Security in 2003	Difficult: for grant purposes, must be able to prioritize risks not only within ports but among them
Information Analysis and Infrastructure Protection Directorate: least far along	New component established with creation of Department of Homeland Security	Extremely difficult: must be able to prioritize risks not only among ports but among all sectors of the nation's critical infrastructure

Source: GAO.

United States Government Accountability Office