June 2004

HOMELAND SECURITY

Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-682, a report to congressional requesters

Why GAO Did This Study

Established in March 2002, the Homeland Security Advisory System was designed to disseminate information on the risk of terrorist acts to federal agencies, states, localities, and the public. However, these entities have raised questions about the threat information they receive from the Department of Homeland Security (DHS) and the costs they incurred as a result of responding to heightened alerts. This report examines (1) the decision making process for changing the advisory system national threat level; (2) information sharing with federal agencies, states, and localities, including the applicability of risk communication principles; (3) protective measures federal agencies, states, and localities implemented during high (code-orange) alert periods; (4) costs federal agencies reported for those periods; and (5) state and local cost information collected by DHS.

What GAO Recommends

The Under Secretary for Information Analysis and Infrastructure Protection in DHS should (1) document communication protocols for sharing threat information and (2) incorporate risk communication principles into the Homeland Security Advisory System to assist in determining and documenting information to provide to federal agencies and states. We provided a draft copy of this report to DHS for comment. DHS generally concurred with the findings and recommendations in the report.

www.gao.gov/cgi-bin/getrpt? GAO-04 -682

To view the full product, including the scope and methodology, click on the link above. For more information, contact William Jenkins at (202) 512-8777 or jenkinswo@gao.gov.

What GAO Found

DHS assigns threat levels for the entire nation and assesses threat conditions for geographic regions and industrial sectors based on analyses of threat information and vulnerability of potential terrorist targets.

DHS has not yet officially documented its protocols for communicating threat level changes and related threat information to federal agencies and states. Such protocols could assist DHS to better manage these entities' expectations about the methods, timing, and content of information received from DHS. To ensure early, open, and comprehensive information dissemination and allow for informed decisionmaking, risk communication experts suggest that warnings should include (1) multiple communication methods, (2) timely notification, and (3) specific threat information and guidance on actions to take. Federal agencies and states responding to GAO's questionnaires sent to 28 federal agencies and 56 states and territories generally indicated that they did not receive specific threat information and guidance, which they believe hindered their ability to determine and implement protective measures.

The majority of federal agencies reported operating at heightened security levels regardless of the threat level, and thus, did not need to implement a substantial number of additional measures to respond to code-orange alerts. States reported that they varied in their actions during code-orange alerts.

The costs reported by federal agencies, states, and selected localities are imprecise and may be incomplete, but provide a general indication of costs that may have been incurred. Additional costs reported by federal agencies responding to GAO's questionnaire were generally less than 1 percent of the agencies' fiscal year 2003 homeland security funding. DHS collected information on costs incurred by states and localities for critical infrastructure protection during periods of code-orange alert. However, this information does not represent all additional costs incurred by these entities during the code-orange alert periods.

Homeland Security Advisory System

Source: Department of Homeland Security