March 2004

HOMELAND SECURITY

Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-538T, a testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Established in March 2002, the Homeland Security Advisory System was designed to disseminate information regarding the risk of terrorist acts to federal, state, and local government agencies, private industry, and the public. However, this system generated questions among these entities regarding whether they were receiving the necessary information to respond appropriately to heightened alerts.

GAO obtained information on how the Homeland Security Advisory System operates, including the process used to notify federal, state, and local government agencies, private industry, and the public of changes in the threat level. GAO also reviewed literature on risk communication to identify principles and factors to be considered when determining when, what, and how information should be disseminated about threat level changes. Additionally, GAO researched what type of information had been provided to federal, state, and local agencies, private industry, and the public regarding terrorist threats. GAO also identified protective measures that were suggested for these entities to implement during code-orange alerts. Last, GAO identified additional information requested by recipients of threat information.

www.gao.gov/cgi-bin/getrpt?GAO-04-538T.

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

What GAO Found

On the basis of intelligence information, the Secretary, Department of Homeland Security (DHS), in consultation with members of the Homeland Security Council, determines whether the national threat level should be elevated. After the Secretary makes this decision, DHS and others begin the process of notifying federal, state and local government agencies, private industry, and the general public through various means, such as conference calls, e-mails, telecommunication systems, and press releases.

Risk communication principles may provide useful guidance for disseminating terrorist threat information to the public. Public warning systems should, to the extent possible, include specific, consistent, accurate, and clear information on the threat at hand, including the nature of the threat, location, and threat time frames. Additionally, public warnings should include guidance on actions to be taken in response to the threat. The public's perception of the threat can also be affected by the content and method of public warnings. Without adequate threat information, the public may ignore the threat or engage in inappropriate actions, some of which may compromise rather than promote the public's safety.

Federal, state, and local governments, private industry, and the public typically received general information from DHS on why the national threat level was changed, but did not receive specific information such as threat locations or time frames. However, for the December 21, 2003, to January 9, 2004, code-orange alert period, DHS announced that the aviation industry and certain geographic locations were at particularly high risk.

DHS and others, such as the American Red Cross, provided federal, state, and local government agencies, private industries, and the public with suggested protective actions for responding to increases in the threat level from code yellow to code orange. For example, the American Red Cross suggested that private industries and the public report suspicions activity to proper authorities and review emergency plans during code-orange alerts.

To determine appropriate protective measures to implement for code-orange alerts, federal, state, and local government officials have requested more specific threat information. Federal agencies indicated that, particularly, region-, sector-, site-, or event-specific threat information, to the extent it is available, would be helpful. One state official said that receiving more specific information about likely threat targets would enable the state to concentrate its response rather than simply blanketing the state with increased general security measures. One local official also noted that specific information about the location of a threat should be provided to law enforcement agencies throughout the nation—not just to localities that are being threatened—thus allowing other local governments to determine whether there would be an indirect impact on them and to respond accordingly.