United States General Accounting Office

GAO

Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, March 16, 2004

HOMELAND SECURITY

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

Statement of Randall A. Yim
Managing Director
Homeland Security and Justice Issues

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.

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to participate in this hearing examining the Homeland Security Advisory System. We last testified before this Subcommittee on February 3, 2004, describing the key characteristics of effective national strategies for homeland security and comparing and contrasting the extent to which seven national homeland security strategies contained such characteristics. Our purpose was to assist in continual improvement and refinement of these strategies. At that hearing, we emphasized that the true measure of the value of these strategies was both (a) the extent to which each strategy was useful as guidance for the relevant federal, state and local government agencies, private industry, not-for-profits, and the general public; and (b) the extent to which these strategies were actually used in the implementation of the major missions of homeland security; namely, prevention, vulnerability assessment and reduction, response, and recovery.

Similarly, our purpose in providing observations on the Homeland Security Advisory System in this testimony is to identify key characteristics of effective public warning systems, to explore principles to be considered and balanced when determining what information to disseminate, and to assist in the Department of Homeland Security's (DHS) continued refinement of the Homeland Security Advisory System. As with the national strategies, the true value of the Homeland Security Advisory System will be the extent to which it is useful as guidance for and actually used in the implementation of prevention, vulnerability reduction, and response and recovery measures by relevant parties, including the general public. Further, the Homeland Security Advisory System is not and should not be considered the only means by which the threat and response information is disseminated.

Specific threat and vulnerability information is received by federal agencies and used by the executive branch in determining when to raise or lower the terrorist threat advisory levels. Key issues for the Homeland Security Advisory System are to what extent, when, and with whom such information should be shared. This Subcommittee suggested that there is a link between information sharing and the ability of the recipients to act upon such information. Each change in the national threat level presents unique facts and circumstances, which influence what, when, and with whom threat information, should be shared. Principles of risk

communication[1] may provide useful guidance for information sharing, thus assisting in the refinement of the Homeland Security Advisory System. Risk communication principles can and should assist not only in prevention, but also in implementing action to reduce vulnerabilities and preparation for enhanced response and recovery should a terrorist attack occur. On the other hand, poor risk communication could lead to complacency and misallocation of valuable limited resources and could be disruptive and expensive for affected parties. Preservation of credibility and public confidence are also important considerations in the refinement of the current terrorist threat advisory system.

Today, my testimony will focus on

- how the Homeland Security Advisory System operates, including a description of the process used to determine the national threat level and the notification process DHS uses to disseminate threat level information to federal, state, and local government agencies, private industry, and the general public;
- what principles and factors experts suggest should be considered when determining information to be disseminated about threat level changes;
- what information DHS currently shares regarding threats;
- what protective measures DHS and others have suggested for federal, state, and local government agencies, private industry, and the public for code-orange alerts; and
- additional information requested and improvements to the advisory system suggested by recipients of threat information.

To address these objectives, we examined reports, guidance, and other documents from individuals and organizations with expertise in homeland security and disaster response, including the American Red Cross, the ANSER Institute for Homeland Security, ASIS International, the Center for Strategic and International Studies, the Congressional Research Service, the Council of State Governments, the Harvard Center for Risk Analysis, and the Partnership for Public Warning. We also extracted information

[1]According to the National Research Council, risk communication is the exchange of information among individuals and groups regarding the nature of risk, reactions to risk messages, and legal and institutional approaches to risk management.

from our correspondence,[2] which provides information collected during our ongoing review of the Homeland Security Advisory System and guidance and information used by federal, state, and local government agencies to determine protective measures to implement when the national threat level is raised to code-orange alert. We are conducting this review at the request of the House Select Committee on Homeland Security. We expect to complete the review and report the final results later this year. We conducted our work from July 2003 to March 2004 in accordance with generally accepted government auditing standards.

In brief, on the basis of intelligence analysis, the Secretary of Homeland Security, in consultation with members of the Homeland Security Council,[3] determines whether the national threat level should be elevated or lowered. Once the Secretary makes this decision, DHS and others begin the process of notifying federal, state and local government agencies, private industries, and the public through various means, such as conference calls. According to experts, risk communication principles may assist in determining the nature, timing, and extent of warnings regarding threats to public safety. Additionally, experts suggest that effective public warning systems should include specific, consistent, accurate, and clear information on threats. Until recently, DHS announcements of national threat level changes included general information on why the threat level was changed, but not specific information on threats. Experts also suggest that public warnings include guidance on appropriate actions to take in response to threats. DHS and various organizations, such as the American Red Cross, suggested protective measures federal, state, and local agencies, private industries, and the public could take in response to code-orange alerts. To help determine what measures to implement for code-orange alerts, federal, state, and local government officials indicated they would prefer more specific threat information.

[2]See U.S. General Accounting Office, *Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*, GAO-04-453R (Washington, D.C.: Feb. 26, 2004).

[3]Members of the Homeland Security Council include the President; the Vice President; the Secretaries of Defense, Health and Human Services, Homeland Security, Transportation, and the Treasury; the Attorney General; the Director of the Federal Emergency Management Agency; the Director of the Federal Bureau of Investigation; the Director of Central Intelligence; and the Assistant to the President for Homeland Security.

Background

Homeland Security Presidential Directive 3 (HSPD-3) established the Homeland Security Advisory System in March 2002. Through the creation of the Homeland Security Advisory System, HSPD-3 sought to produce a common vocabulary, context, and structure for an ongoing discussion about the nature of threats that confront the nation and the appropriate measures that should be taken in response to those threats. Additionally, HSPD-3 established the Homeland Security Advisory System as a mechanism to inform and facilitate decisions related to securing the homeland among various levels of government, the private sector, and the general public.

The Homeland Security Advisory System is comprised of five color-coded threat conditions, which represent levels of risk related to potential terror attack. As defined in HSPD-3, risk includes both the probability of an attack occurring and its potential gravity. Since its establishment in March 2002, the Homeland Security Advisory System national threat level has remained at elevated alert—code yellow—except for five periods during which the administration raised it to high alert—code orange. The periods of code-orange alert follow:

- September 10 to 24, 2002
- February 7 to 27, 2003
- March 17 to April 16, 2003
- May 20 to 30, 2003
- December 21, 2003, to January 9, 2004.

When HSPD-3 first established the Homeland Security Advisory System, it provided the Attorney General with responsibility for administering the Homeland Security Advisory System, including assigning threat conditions in consultation with members of the Homeland Security Council, except in exigent circumstances. The Attorney General could assign threat levels for the entire nation, for particular geographic areas, or for specific industrial sectors. In November 2002, Congress enacted the Homeland Security Act of 2002, P.L. 107-296, which established the Department of Homeland Security. Under the Homeland Security Act of 2002, the DHS Under Secretary for Information Analysis and Infrastructure Protection (IAIP) is responsible for administering the Homeland Security Advisory System. In February 2003, in accordance with the Homeland Security Act, the administration issued Homeland Security Presidential Directive 5 (HSPD-

5), which amended HSPD-3 by transferring authority for assigning threat conditions and conveying relevant information from the Attorney General to the Secretary of Homeland Security.

How the Homeland Security Advisory System Currently Operates

According to DHS officials, the intelligence community continuously gathers and analyzes information regarding potential terrorist activity. This includes information from such agencies as DHS,[4] the Central Intelligence Agency, the Federal Bureau of Investigation (FBI), and the Terrorist Threat Integration Center.[5] Analyses from these and other agencies are shared with DHS's IAIP, which is engaged in constant communication with intelligence agencies to assess potential homeland security threats.

DHS officials told us that when intelligence information provides sufficient indication of a planned terrorist attack, and is determined to be credible, IAIP recommends to the Secretary of Homeland Security that the national threat level should be raised. To decide whether to lower the national threat level, DHS officials told us that the department reviews threat information to determine whether time frames for threats have passed and whether protective measures in place for the code-orange alerts have been effective in mitigating the threats. DHS officials further told us that analysis of the threat information and determination of threat level changes are specific for each time period and situation and include a certain amount of subjectivity. They said no explicit criteria or other quantifiable factors are used to decide whether to raise or lower the national threat level.

After reviewing threat information and analyses, the Secretary of Homeland Security consults with the other members of the Homeland

[4]DHS's Homeland Security Operations Center and its IAIP Directorate monitor threats and conduct information assessments on a daily basis. The Center is comprised of representatives from DHS component entities, other federal agencies, and local law enforcement agencies.

[5]The Terrorist Threat Integration Center is responsible for analyzing and sharing terrorist-related information that is collected domestically and abroad. It is an interagency joint venture that is comprised of elements of DHS, the FBI's Counterterrorism Division, the Director of Central Intelligence Counterterrorist Center, the Department of Defense, and other agencies.

Security Council on whether the national threat level should be changed.[6] DHS officials told us that if the Homeland Security Council members could not agree on whether to change the national threat level, the President would make the decision. After the determination has been made to raise or lower the national threat level, DHS begins its notification process.

As discussed in our February correspondence,[7] DHS used the following methods, among others, to notify federal, state, and local agencies of changes in the national threat level,

- conference calls between the Secretary of Homeland Security and state governors and/or state homeland security officials;
- telephone calls from Federal Protective Service (a component of DHS) officials to federal agencies;
- e-mail or telephone communications from Homeland Security Operations Center (HSOC) representatives to the federal, state, or local agencies they represent;
- HSOC electronic systems, such as the Joint Regional Information Exchange System;
- FBI electronic systems, such as the National Law Enforcement Telecommunications System; and
- e-mail and/or telephone communications with federal agencies' chief of staff and public affairs offices.

As discussed in the Congressional Research Service's January 2004 report on the Homeland Security Advisory System,[8] DHS also provides information to chief executive officers of the nation's top businesses and industries through the Business Roundtable's Critical Emergency Operations Communications Link (CEO COM LINK), a secure

[6]Under HSPD-5, the Secretary can change the national threat level without consulting other Homeland Security Council members in exigent circumstances. However, DHS officials told us that this did not occur for any of the three most recent code-orange alerts.

[7]GAO-04-453R.

[8]See Congressional Research Service, *Homeland Security Advisory System: Possible Issues for Congressional Oversight* (Washington, D.C.: Jan. 29, 2004).

telecommunications system activated during national crises and threats. Chief executive officers are asked to dial into a secure conference call, and after each officer goes through a multistep authentication process to ensure security, DHS or other federal officials brief them on threats. DHS also calls other critical infrastructure and business associations to notify them of national threat level changes. DHS provides information on changes in the national threat level and related threat information to the public through press conferences, press releases, and other announcements or statements released on Web sites or media sources.

DHS officials told us that they have not yet formally documented protocols for notifying federal, state, and local government agencies and the private sector of national threat level changes. They told us that they are working to document their protocols. However, they could not provide us with a specific time frame as to when DHS expects to complete this effort. For an entity to control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events.[9] As we have previously reported, to establish channels that facilitate open and effective communication, agencies should clearly set out procedures, such as communication protocols, that they will consistently follow when doing their work.[10] Communications protocols would, among other things, help foster clear understanding and transparency regarding federal agencies' priorities and operations. Moreover, protocols can help ensure that agencies interact with federal, state, local, and other entities using clearly defined and consistently applied policies and procedures.

[9]See U.S. General Accounting Office, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00.21.3.1 (Washington, D.C.: November 1999).

[10]See U.S. General Accounting Office, *Office of Compliance: Status of Management Control Efforts to Improve Effectiveness*, GAO-04-400 (Washington, D.C.: Feb. 3, 2004).

Risk Communication Principles May Provide Useful Guidance for Refinement of the Homeland Security Advisory System

Risk communication principles have been used in a variety of public warning contexts, from alerting the public about severe weather or providing traffic advisories to less commonplace warnings of infectious disease outbreaks or potential dangers from hazardous materials or toxic contamination.[11] These principles can be considered when determining the nature, timing, and extent of warnings regarding threats to public safety. In general, risk communication principles seek to maximize public safety by ensuring that the public has sufficient information to determine actions to take to prevent or to respond to emergencies. Appropriately warning the public of threats can help save lives and reduce the costs of disasters. In providing such warnings, experts say that citizens should be given an accurate portrayal of risk, without overstating the threat or providing false assurances of security. According to David Ropeik of the Harvard Center for Risk Analysis and Dr. Paul Slovic of Decision Research, understanding and respecting the ways people make risk judgments can help governments assist citizens in keeping their sense of risk in perspective. In turn, this helps citizens make wiser, healthier decisions and focuses social concern on the relatively greater risks.[12]

Differences between warnings about terrorist threats and relatively more familiar warnings about infectious disease must also be recognized in effective risk communication principles. For example, specific terrorist threat warnings may allow terrorists to alter tactics or targets in response or increase general anxiety for those clearly not at risk. Moreover, government agencies may not always have specific information on terrorist threats or may not be able to publicly share specific information in threat warnings.

Experts have identified the following as important principles for individuals when making risk management decisions:

[11]Public warning systems in the weather and health sectors provide information to citizens that allow them to determine their actions to respond to threats. For example, for severe storms, the National Weather Service and the mass media attempt to alert the public in advance when they might pose a hazard to public safety. Similarly, the Centers for Disease Control and Prevention developed a nationwide reporting system that seeks to detect emerging epidemics and then to warn the public about the nature of the health threat.

[12]David Ropeik and Paul Slovic, "Risk Communication: A Neglected Tool in Protecting Public Health," *Risk in Perspective, vol.* 11, no. 2 (Harvard Center for Risk Communication, Cambridge, Mass. 2003)

- Specific information on the potential threat including, to the greatest extent possible,

  - the nature of the threat,
  - when and where it is likely to occur, and
  - over what time period, and

- Guidance on actions to be taken.

  Additionally, experts have noted that such information should be consistent, accurate, clear, and provided repeatedly.

  Inadequately adhering to these principles can compromise public safety and erode public confidence. For example, at a March 5, 2004, hearing before the House Committee on Government Reform,[13] it was noted that the residents of the District of Columbia received incomplete and inconsistent information regarding appropriate protective measures to take in response to high concentrations of lead in drinking water. Specifically, the District of Columbia Water and Sewer Authority initially recommended that residents flush water lines for 1 to 2 minutes prior to using water for drinking or cooking. Later, District residents received different instructions to flush water lines for 10 minutes.

  Similarly, in his testimony before this Subcommittee in November 2001,[14] Dr. Kenneth Shine, the president of the Institute of Medicine, the National Academies, provided an example of how the public may take inappropriate actions due to inadequate information associated with the anthrax incidents. He said that better and earlier information on the extent to which Americans were at risk of harm from anthrax might have prevented the premature exhaustion of the supply of Ciprofloxacin[15] and might have prevented the nearly 20 percent of those who took the antibiotic unnecessarily from possibly experiencing harmful side effects.

[13]Chairman Tom Davis, "Public Confidence Down the Drain: The Federal Role in Ensuring Safe Drinking Water in the District of Columbia" (opening statement presented at a hearing before the House Committee on Government Reform, Washington, D.C.: Mar. 5, 2004).

[14]Dr. Kenneth Shine, "For a Hearing on Risk Communication: National Security and Public Health" (testimony presented to the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, Washington, D.C.: Nov. 29, 2001).

[15]Ciprofloxacin is an antibiotic that was used to treat persons believed to be exposed to anthrax.

David Ropeik and Dr. George Gray, both at the Harvard Center for Risk Analysis, also cited the risk of inadequate information to the public with regard to anthrax. They said that if the government does not manage the public's perception of the risk of terrorism, the public may be more apt to take actions that may cause them harm.[16]

Moreover, as we testified in July 2003, Severe Acute Respiratory Syndrome, better known as SARS, was able to spread worldwide due to delayed warnings about the appearance of the disease.[17] However, the outbreak was subsequently controlled because, according to health officials, rapid and frequent communications of crucial information about the disease—such as the level of outbreak worldwide and recommended infectious disease control measures—were vital to efforts to contain its spread.

Some experts caution government officials about providing too much threat information and highlight the need to balance the possible consequences of providing threat information that is either too specific or too general. For example, according to the Senior Advisor for Public Health Risk Communication at the Department of Health and Human Services, providing too much information to the public regarding terrorist threats could result in public panic and disorganization, while providing too little information could result in public denial, apathy, and inaction. She suggests that those informing the public must balance the information they provide so that the public's fear will translate into concern and, in turn, result in the implementation of self-protective measures by citizens. She also suggests that such balance can be achieved by emphasizing to the public that there is a response plan in place; avoiding over-reassurance; acknowledging that there is uncertainty about the threat; giving people things to do; acknowledging the shared misery; and addressing "what if" questions.

Other experts assert that it is not the amount of information that causes the public to respond inappropriately to warnings of threats, but rather, it

[16]George M. Gray and David P. Ropeik, *Dealing with the Dangers of Fear: The Role of Risk Communication*, Health Affairs. vol. 21, no. 6 (2002) 1-2.

[17]See U.S. General Accounting Office, *Severe Acute Respiratory Syndrome: Established Infectious Disease Control Measures Helped Contain Spread, but a Large-Scale Resurgence May Pose Challenges*, GAO-03-1058T (Washington, D.C.: July 30, 2003). SARS is believed to have originated in Guangdong Province, China, in mid-November 2002.

is the adequacy of the information provided that will determine the public's response. For instance, in a report prepared for the Federal Emergency Management Agency (FEMA),[18] public warnings experts John Sorensen and Dennis Mileti and the Partnership for Public Warning[19] assert that the public rarely, if ever, is given too much information in an official warning. [20] Furthermore, they noted that even though mass panic is commonly expected by civil authorities, it almost never occurs.[21]

Decisions regarding who should receive threat information, as well as the nature, timing, and extent of information to be shared, should be related to the willingness and ability of the recipients to use such information.

Mr. Ropeik and Dr. Slovic identified several key factors relevant to a recipient's risk perception and management:

- Dread—-the more horrific a threat, the more people fear it.
- Control—the more control individuals have over a situation, the smaller they perceive the risk; (e.g., driving one's own car versus traveling in a commercial airliner that is piloted by a stranger).
- Is the risk natural or is it human-made?—a man-made source of risk, such as radiation from cellular telephones, evokes greater fear among people than does radiation from natural sources such as the sun.
- Choice—risks that are chosen evoke less fear than those that are imposed on us.

[18]Dennis S. Mileti and John H. Sorensen, *Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment*, a report prepared for the Federal Emergency Management Agency, August 1990, 3-2.

[19]The Partnership for Public Warning is a public/private not-for-profit institute that works to promote and enhance efficient, effective, and integrated dissemination of public warnings and related information so as to save lives, reduce disaster losses, and speed recovery.

[20]Partnership for Public Warning, *Developing a Unified All-Hazard Public Warning System* (Emmitsburg, Md: Nov. 25, 2002) 8.

[21]Mr. Sorensen and Mr. Mileti reported that, according to research, panic occurs only in situations in which there is closed physical space, in which there is an immediate and clear threat of death, and in which escape routes will not accommodate all those in danger in the minutes before death comes to those left behind.

- Children—threats to children are perceived as worse than those to adults, even when the risks are from the same source, such as asbestos.
- Is the risk new?—emerging threats generate more anxiety among individuals than those that are known.
- Awareness—greater awareness of risks likely heightens concern
- Can it happen to me? —risks seem greater if one believes he or she or someone close may be a victim.
- The risk-benefit tradeoff—a perceived benefit from a behavior or choice makes the associated risk seem smaller.
- Trust—greater trust in those communicating the risk and responsible for action lessens anxiety.

Many of the principles and factors described above appear to be relevant to sharing information about terrorist threats, and consideration of the relevance of these factors may be useful in future refinements of the Homeland Security Advisory System. Further, it is important to recognize that this Advisory System is not and should not be considered the only means by which threat and response information is disseminated.

In certain contexts, risk communication principles have been codified—incorporated in legislation. For example, legislation, such as the Emergency Planning and Community Right-To-Know Act of 1986, recognizes the importance of providing information to the public regarding hazardous materials in their community. [22] Section 313 of the act generally requires facilities that manufacture, process, or otherwise use toxic chemicals to report the amounts of various toxic chemicals that they release to the environment and requires the Environmental Protection Agency (EPA) to make this information available to the public. Fire departments and other emergency responders have access to this information to help develop response plans before they arrive at the scene of a chemical accident or at a fire at a facility using hazardous chemicals. [23]

[22]P.L. 99-499, Title III, Subtitle A (Oct. 17, 1986).

[23]See U.S. General Accounting Office, *Environmental Information: Agencywide Policies and Procedures Are Needed for EPA's Information Dissemination*, GAO/RCED-98-245 (Washington, D.C.: Sept. 24, 1998).

In addition, occupational safety and health requirements mandate that materials safety data sheets accompany hazardous materials to provide information and warnings about potential dangers and appropriate protective or response measures.[24]

The Safe Drinking Water Act and its amendments require public water systems to provide information to the public that would allow them to respond to violations of the National Primary Drinking Water Regulations—standards that protect public health by limiting the levels of contaminants in drinking water. Included in these notifications should be a description of the violation, any potential adverse health effects, what the system is doing to correct the problem, and whether consumers should use an alternate source of water.[25]

Why Is It Important for the Homeland Security Advisory System to Incorporate Risk Communication Principles?

While federal agencies, state and local governments, the private sector and the general public routinely make risk management decisions (even though they may not think of them as such), threats of terrorism within the United States remain relatively unfamiliar. As noted by David Ropeik and Dr. Paul Slovic, greater recognition of the underpinnings of the fear of terrorism, and respect for the social and psychological dynamics of response, can assist policy makers in incorporating such realities as well as fact-based analysis into risk communication principles. As Ropeik and Slovic explain, understanding the reasons people perceive risk as they do, policy makers can communicate with various audiences about these issues in terms and language relevant to people's concerns, and as a result risk communication or warnings are likely to be more successful in helping people make more informed choices about the risks they face.[26]

Finally, implementation of risk communication principles could prevent complacency or inaction in the face of elevated threat warnings of the Homeland Security Advisory System. For example, it is assumed that when warnings are not followed by the occurrence of the hazard, the public will ignore future warnings. However, the Dr. Baruch Fischhoff, professor in the Department of Social and Decision Sciences at Carnegie Mellon University, and the Partnership for Public Warnings suggested

[24]See 29 C.F.R. 1910.1200(g).

[25]See 42 U.S.C. 300g-3(c)(2)(C); 40 C.F.R. 141.205.

[26]Ropeik and Slovic "Risk Communication" 3.

otherwise. They said that it is not the number of perceived false alarms that will cause the public to ignore future warnings and develop a sense of complacency about the hazard; rather, it is the lack of information provided to the public regarding the perceived false alarm that will cause the warning system to lose its credibility. The Partnership for Public Warning suggests that the real concern is educating the public about the uncertainty of the threat so that they can comprehend that false alarms arise from inherent uncertainty rather than from poor professional practice.[27] Similarly, Dr. Fischhoff, citing the color-coded levels of the Homeland Security Advisory System, suggested that the public needs to be educated regarding the philosophy underlying each threat level to help the public understand why false alarms are inevitable, thus minimizing cumulative apathy among the public.[28]

Information Currently Shared by DHS

Until recently, DHS's announcements of increases in the national threat level to code orange have included general information on why the threat level was raised and general suggestions for protective measures the public could take during code-orange alert periods. However, these announcements generally did not include information on locations of potential threats and threat time frames. For example, on the occasion of the third code-orange alert, March 17 to April 16, 2003, the Secretary of Homeland Security made the decision to raise the threat level based on intelligence indicating the possibility of terrorist attacks due to a military campaign in Iraq. Similarly, for the code-orange alert from May 20 to 30, 2003, the Secretary provided general information on why the national threat was raised. For example, the Secretary announced that the threat level was changed based on the U.S. intelligence community's belief that, in the wake of terrorist bombings in Saudi Arabia and Morocco, Al-Qaida had entered an operational period, which may include attacks in the United States.

During the most recent code-orange alert period, December 21, 2003, to January 9, 2004, there was heightened concern about the use of aircraft for potential terrorist attacks, and several geographic locations were also

[27]Partnership for Public Warning, "Developing a Unified All-Hazard Public Warning System" 8.

[28]Baruch Fischhoff, "Assessing and Communicating the Risks of Terrorism," in Science and Technology in a Vulnerable World, 51-64 (Washington, DC: American Association for the Advancement of Science, 2003).

reported to be at particularly high risk. DHS provided specific recommendations for protective measures to industry sectors and for geographic areas in response to specific threat information. When the national threat level was lowered to yellow on January 9, 2004, DHS recommended that some sectors, such as the aviation industry, and certain geographic locations continue on a heightened alert status. According to the Deputy Secretary, this was the first time since the creation of the Homeland Security Advisory System that DHS lowered the national threat level but recommended maintaining targeted protections for a particular industry sector or geographic location.

In addition, DHS officials said that the department issues threat advisories and information bulletins for specific threats that do not require changes in the national threat level. Threat advisories contain information about incidents or threats targeting critical national infrastructures or key assets, such as pipelines. Information bulletins communicate information of a less urgent nature to nongovernmental entities and those responsible for the nation's critical infrastructures. The threat advisories and bulletins we reviewed also include advice on protective measures for law enforcement agencies.

Agencies and Organizations Have Suggested Actions for Federal, State, and Local Agencies, the Private Sector, and the Public

Various agencies and organizations such as DHS, the American Red Cross, and ASIS International have suggested general protective measures for federal, state, and local government agencies, private industries, and the public to consider for each Homeland Security Advisory System threat level, including code orange. Federal, state and local agencies, private industries, and the public may use measures suggested by these agencies and organizations, as well as others, to determine actions to take when the national threat level is raised to code orange.

For example, HSPD-3, the presidential directive that established the Homeland Security Advisory System, suggested general protective measures for each threat level for federal agencies. At code orange, the directive suggests that federal agencies consider coordinating necessary security efforts with federal, state, and local law enforcement agencies; taking additional precautions at public events; preparing to execute contingency procedures; and restricting facility access to essential personnel only.

For state and local government agencies, DHS requested that they implement protective measures during code-orange alerts, although compliance with the Homeland Security Advisory System is voluntary for

state and local governments. For example, during the two most recent code-orange alerts (May 20 to 30, 2003, and December 21, 2003, to January 9, 2004), DHS suggested state governors and local government officials review security measures their agencies had in place and deploy additional measures to mitigate terrorist attacks. In addition, some states have developed their own protective measures for state and local government agencies for Homeland Security Advisory System threat levels. For example, at code-orange alert, the state of Washington's military department suggests that, among other measures, state and local agencies disseminate the orange advisory and share pertinent information with state and local agencies and officials; place all emergency management and specialized response teams on full alert status; and suspend public tours of critical infrastructure facilities.

For private industries, ASIS International, an international organization for security professionals, developed draft guidelines as a tool for private businesses and industries to consider when determining possible actions to be implemented at each Homeland Security Advisory System threat level.[29] At code-orange alert, ASIS International suggests that private industries consider, among other measures, preparing for possible evacuation, closing, and securing facilities; increasing security patrols; conducting heightened screening and inspection of mail and deliveries; and discontinuing tours and other non-essential site visits. In addition, the American Red Cross recommends that businesses be alert to suspicious activity and report it to proper authorities; review emergency plans; and determine the need to restrict access to businesses.

FEMA, an entity of DHS, and the American Red Cross suggest general actions citizens should consider taking during periods of code-orange alert. For example, in its guide, *Are You Ready? A Guide to Citizen Preparedness*,[30] FEMA recommends that citizens review preparedness measures (including evacuation and sheltering) for potential terrorist actions, including chemical, biological, and radiological attacks; avoid high profile or symbolic locations; and exercise caution when traveling. Likewise, the American Red Cross suggests that individuals and families

[29]ASIS International, *Threat Advisory System Response (TASR) Draft Guideline: Guideline for Preparations Relative to the Department of Homeland Security Advisory System* (November 24, 2003).

[30]Federal Emergency Management Agency, *Are You Ready?: A Guide to Citizen Preparedness* (Washington, D.C.: September 2002).

be alert to suspicious activity and report it to proper authorities; review personal and family disaster and communication plans; and have shelter-in-place materials so that individuals and families can remain where they are located when incidents occur. Moreover, in public announcements of national threat level increases, the Secretary of Homeland Security recommended that citizens continue with their plans but be alert and report any suspicious activity to law enforcement agencies. In addition, according to the Deputy Secretary of Homeland Security, the department has launched a public information campaign to increase citizen and community preparedness. As part of the campaign, DHS developed the Ready.gov Web site in early 2003, which recommends actions individuals and families can take, such as creating family emergency plans and assembling emergency kits.

Additional Information Requested and Improvements to the Advisory System Suggested by Relevant Parties

As noted in our February correspondence,[31] some federal agencies for which we collected information indicated that without specific information on threats, they cannot effectively focus resources on protective measures to respond to possible threats. Likewise, Governor Mitt Romney of Massachusetts testified in June 2003[32] that state and local officials need specific information if they are to match their response to an increased threat level appropriate to the increased risk.

Federal, state, and local government officials reported that receiving information with greater specificity about threats, if available, would have been helpful in determining additional actions to take in response to code-orange alerts. For example, 14 of 15 federal agencies that provided us with information indicated that information on region-, sector-, site-, or event-specific threats, if available, would have been helpful. Additionally, all of the 15 federal agencies that provided us with information noted that information on threat time frames, if available, would have assisted them in determining appropriate actions to take in responding to the code-orange alerts. Fourteen federal agencies also indicated that receiving information on recommended measures for preventing incidents would

[31]GAO-04-453R.

[32]Governor Mitt Romney, "First Responders: How States, Localities and the Federal Government Can Strengthen Their Partnership to Make America Safer" (testimony presented to the House Select Committee on Homeland Security, Washington, D.C.: July 17, 2003).

have been helpful in determining appropriate protective measures to implement or enhance for each code-orange alert period.

Similarly, one state official noted that receiving more specific information about the type of threat—against bridges and dams, for example—would enable the state to concentrate its response in those areas, a more effective approach 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. Additionally, according to a national survey on the public's priorities regarding receipt of terror-related information, the public wants honest and accurate information about terror-related situations, even if that information worries them.[33]

DHS officials told us that the Homeland Security Advisory System is constantly evolving based on their ongoing review of the system. DHS officials told us they adjust the system based on feedback from federal, state and local government and private sector officials; tests of the system; and experience with previous periods of code-orange alert. For example, during the most recent code-orange alert, there was heightened concern about the use of aircraft for potential terrorist attacks, and several geographic locations were also reported to be at particularly high risk. In a recent testimony, the Deputy Secretary of Homeland Security noted that DHS provided specific recommendations for protective measures to industry sectors and for geographic areas in response to specific threat information.

Concluding Observations

Specific terrorist threats present unique factors that will necessarily influence what information can and should be shared, when it should be disseminated, and to whom. Other factors to be considered include (a) the extent to which relevant parties can actually act upon such information, not only to prevent attacks, but also to identify and reduce vulnerabilities and enhance their response and recovery should an attack occur; (b) the

[33]Baruch Fischhoff, Roxana M. Gonzalez, Deborah A. Small, and Jennifer S. Lerner, "Evaluating the Success of Terror Risk Communications," Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, vol. 1, no. 4 (2003).

danger of mis-allocation of limited valuable resources through sharing of incorrect or vague information; (c) the disruption incurred as a result; and (d) the erosion of public confidence and credibility through ineffective risk communication. Risk communication principles used in areas such as hazardous materials management, disease prevention, or law enforcement, may provide useful guidance as DHS continues to refine the Homeland Security Advisory System.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the Subcommittee may have at this time.

GAO Contacts and Staff Acknowledgments

For further information about this testimony, please contact Randall A. Yim at (202) 512-8777. Other key contributors to this statement were David P. Alexander, Fredrick D. Berry, Nancy A. Briggs, Kristy N. Brown, Philip D. Caramia, Christine F. Davis, Katherine M. Davis, Michele Fejfar, Rebecca Gambler, William O. Jenkins, Debra B. Sebastian, Gladys Toro, Jonathan R. Tumin, and Kathryn G. Young.