United States General Accounting Office

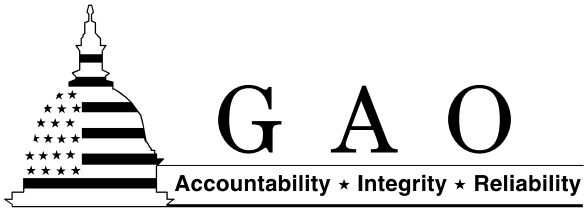
GAO

Report to Congressional Requesters

June 2004

HOMELAND SECURITY

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



GAO-04-682

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

Contents

Figure

Abbreviations

CDC	Centers for Disease Control
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
IAIP	Information Analysis and Infrastructure Protection
ODP	Office of Domestic Preparedness
OMB	Office of Management and Budget
SHSGP	State Homeland Security Grant Program
UASI	Urban Areas Security Initiative

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

June 25, 2004

The Honorable Christopher Cox
Chairman
The Honorable Jim Turner
Ranking Minority Member
Select Committee on Homeland Security
House of Representatives

The Honorable Joseph R. Biden, Jr.
United States Senate

The Homeland Security Advisory System was established in March 2002 to disseminate information regarding the risk of terrorist acts to federal agencies, states and localities, and the public utilizing five color-coded threat levels. Implementation of this system generated questions among government agencies regarding whether they were receiving the information necessary to respond appropriately when the national threat level was raised and about the costs resulting from additional protective measures implemented during periods of heightened alert.

You asked us to review several aspects about how the Department of Homeland Security (DHS) was operating the Homeland Security Advisory System including federal, state, and local responses to heightened alerts. This report discusses (1) the decision-making process for changing the national threat level; (2) guidance and other information provided to federal agencies, states, and localities, including the applicability of risk communication[1] principles to information sharing;[2] (3) protective measures federal agencies, states, and localities implemented during high—code-orange—alert periods; (4) additional costs federal agencies reported for implementing such measures; and (5) information DHS collected on costs states and localities reported for periods of code-orange alert. In addition, this report provides information on other threat advisory systems used by federal agencies, states, localities, and other countries. (See app. I.)

[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.

[2]See U.S. General Accounting Office, *Homeland Security: Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System*, GAO-04-538T (Washington, D.C.: Mar. 16, 2004).

To respond to your request, we met with and obtained information from DHS officials on the decision-making process for changing the national threat level; guidance and threat information the department provides to federal agencies, states, and localities; and information on protective measures and costs that the department collected from states and localities. We also examined literature on risk communication principles to identify the applicability of such principles to the Homeland Security Advisory System. In addition, we sent questionnaires to 28 federal agencies and the homeland security or emergency management offices in 50 states, the District of Columbia, American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands, regarding the notification and information these entities received, the protective measures they took, and the costs they reported for the three code-orange alert periods from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004. Although some federal agencies and states did not respond to every question in our questionnaires, we received responses from 26 federal agencies, which account for about 99 percent of total fiscal year 2003 nondefense homeland security funding as reported to the Office of Management and Budget (OMB),[3] and 43 states,[4] for a 77 percent response rate. We selected the 28 federal agencies because they reported receiving homeland security funding for fiscal year 2003 to OMB and are Chief Financial Officers Act agencies.[5] For this review, we analyzed information from the District of Columbia, American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands along with information from states, and we refer to all of these throughout the report as states.

[3]Office of Management and Budget, *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: September 2003).

[4]One state for which we received a questionnaire response indicated that it did not follow the Homeland Security Advisory System. We analyzed questionnaire responses for the other 42 states that indicated they followed the Homeland Security Advisory System.

[5]P.L. 101-576 (Nov. 15, 1990). Three of the federal agencies to which we sent a questionnaire are Chief Financial Officers Act agencies but did not report receiving homeland security funding in fiscal year 2003 to the Office of Management and Budget. We sent our questionnaire to these three federal agencies to include all Chief Financial Officers Act agencies in our review, and thus these 28 federal agencies accounted for about 91 percent of total nondefense gross federal obligations for fiscal year 2003.

To obtain information on localities' experiences during code-orange alerts, we conducted site visits with officials from 12 localities (8 cities and 4 counties).[6] We selected the 12 localities to visit based on the following criteria: (1) their receipt of grants from DHS; (2) their geographic location and topography (e.g., inland, border, or seaport); and (3) the type of locality (e.g., metropolitan and nonmetropolitan areas).[7] We also sent a questionnaire to 8 additional localities,[8] selecting them based on population and geographic location. We received questionnaire responses from 4 of these localities.[9] We used information obtained from the 16 localities we visited or from which we received questionnaire responses only as anecdotal examples, as information from these localities cannot be generalized across all localities in the United States.

DHS has not documented the policies and procedures it has used for assessing intelligence information, determining whether to raise or lower the threat level, and notifying federal agencies, states, and localities about changes in threat levels. Thus, the information provided about the operations of the Homeland Security Advisory System is principally based on interviews with DHS officials and questionnaire responses. We conducted our work from July 2003 to May 2004 in accordance with generally accepted government auditing standards. For more detailed information on our scope and methodology, see appendix II.

[6]The 12 localities are Atlanta and Fulton County, Georgia; Denver, Colorado Springs, and Douglas County, Colorado; Norfolk, Virginia; Portland and Wasco County, Oregon; Chicago and Cook County, Illinois; and Boston and Fitchburg, Massachusetts.

[7]We selected the 12 localities based on a mix of these criteria. For example, 5 of the localities we selected received urban areas grants from DHS, while 7 did not. Nine of the localities we visited were in metropolitan areas, while 3 were not.

[8]The 8 localities are Helena, Montana; Mankato, Minnesota; Rock Springs, Wyoming; San Jose, California; Miami/Dade County, Florida; Seattle, Washington; Jamestown, North Dakota; and New York City, New York.

[9]One of the localities from which we received a questionnaire response indicated that it did not follow the Homeland Security Advisory System. We analyzed questionnaire responses for the other 3 localities that indicated following the Homeland Security Advisory System.

Results in Brief

In administering the Homeland Security Advisory System, DHS assigns national threat levels and assesses threat conditions for specific geographic locations and industrial sectors. The national threat level is assigned by the Secretary of Homeland Security, in consultation with members of the Homeland Security Council,[10] based on analysis of intelligence information and assessment of the vulnerability of potential terrorist targets. DHS also uses analysis of threat information and assessments of the vulnerability of terrorist targets to determine whether specific industrial sectors or geographic regions should operate at heightened levels of security. DHS may encourage sectors or geographic regions to operate at heightened levels of security, without publicly announcing a threat.

DHS has not yet officially documented communication protocols for providing threat information and guidance to federal agencies and states. According to DHS officials, it has been difficult to develop protocols for notifying federal agencies and states of changes in the national threat level that provide sufficient flexibility for sharing information in a variety of situations. Communication protocols can assist DHS in better managing the expectations of federal agencies and states regarding the guidance and threat information they receive from the department. Risk communication experts suggest that threat warnings should include the following principles to ensure early, open, and comprehensive information dissemination and to allow for informed decisionmaking: (1) communication through multiple methods, (2) timely notification, and (3) specific threat information and guidance on actions to take. These principles have primarily been used in public warning contexts, but they are also applicable for communicating terrorist threat information to federal agencies and states through the Homeland Security Advisory System. DHS used multiple methods to communicate threat information to federal agencies and states when the national threat level was raised to code-orange. However, many federal agencies and states responding to our questionnaires reported first learning about changes in the national threat level from media sources. As a result, some of these states indicated that their ability to provide credible information to state and local agencies and the public was hampered. Moreover, federal agencies and states

[10]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.

responding to our questionnaires indicated that they generally did not receive specific threat information and guidance, which they believed hindered their ability to determine whether they were at risk as well as their ability to determine and implement appropriate protective measures.

The majority of federal agencies responding to our questions regarding protective measures reported that they regularly operate at high levels of security and did not have to implement a substantial number of additional measures to respond to code-orange alerts. For the most part, these federal agencies reported that their most common response to code-orange alert periods was to enhance existing protective measures, for example, an increase in the frequency of facility security patrols. To a lesser extent, federal agencies reported they maintained the use of existing protective measures without enhancement, for example, continuing the use of intrusion detection systems during code-orange alerts. However, based on responses to our questionnaire, states varied in the extent to which they enhanced or maintained protective measures already in place, or implemented measures solely in response to the three code-orange alert periods. States indicated that various factors, such as specific threat information received by the state, influenced the extent to which they implemented protective measures. While federal agencies and states responding to our questionnaires reported benefiting by implementing various protective measures during code-orange alerts, they also indicated that taking such actions adversely affected their operations, and they identified several operational challenges. For example, while these federal agencies and states reported that protective measures taken during code-orange alerts promoted employees' sense of security, they also said that the lack of federal governmentwide coordination, such as multiple government agencies providing conflicting information to states regarding protective measures, limited their ability to effectively coordinate and, therefore, implement measures.

Code-orange alert cost data provided by federal agencies responding to our questionnaire are not precise, may not include all additional costs incurred by agencies, and, in some cases, we have concerns about the reliability of the cost data source within particular agencies. Despite these limitations, we believe the cost data to be sufficiently reliable as indicators of general ranges of cost and overall trends. However, the data should not be used to determine the cumulative costs incurred across all federal agencies. The total additional costs reported by federal agencies responding to our questionnaire for the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods were less than 1 percent of these agencies' fiscal year 2003 homeland security funding, as reported by agencies to OMB.[11] On the basis of cost information reported by these federal agencies for the three code-orange alert periods in our review, we calculated additional average daily costs ranging from about $190 to about $3.7 million. Independent federal agencies typically reported the least amount of additional costs, while larger cabinet level agencies with responsibility for protecting critical national infrastructure reported the most additional costs. The majority of federal agencies responding to our questionnaire experienced a decline in additional average daily costs between the March 17 to April 16, 2003, and the December 21, 2003, to January 9, 2004, code-orange alert periods, which some of these agencies attributed to continued enhancement of standard levels of security. Some federal agencies responding to our questionnaire reported that they did not incur any additional costs during code-orange alert periods, because they did not implement any additional protective measures or they redirected already existing resources to implement additional code-orange alert measures rather than employ additional resources.[12] Although some federal agencies reported not incurring additional costs directly as a result of implementing protective measures for code-orange alerts, actions taken such as redirecting resources from normal operations may have resulted in indirect costs.

[11]We calculated the additional code-orange alert costs for the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods as a percentage of agencies' fiscal year 2003 homeland security funding because these are the only two code-orange alert periods in our review that occurred during fiscal year 2003.

[12]Typically, there are indirect costs associated with redirection of resources from one agency function to another. Federal agencies responding to our questionnaire were not able to quantify such indirect costs. However, they provided examples of redirection of resources that may have caused them to incur such costs.

DHS collected information on critical infrastructure protection costs states and localities reported incurring during the March 17 to April 16, 2003, May 20 to 30, 2003, and December 21, 2003, to January 9, 2004, code-orange alert periods through its State Homeland Security Grant Program – Part II and the Urban Areas Security Initiative – Part II. However, this cost information does not represent all additional costs incurred by states and their localities during code-orange alert periods. The U.S. Conference of Mayors also collected and reported estimates of costs localities incurred in response to code-orange alerts. Additionally, a Director with the Center for Strategic and International Studies estimated and reported costs incurred by federal agencies during code-orange alerts. However, because of limitations in the scope and methodologies used in these estimates, the cost information reported may not be adequate for making generalizations regarding additional costs federal agencies, states and localities incurred in response to code-orange alerts.

In this report, we make specific recommendations to the Secretary of Homeland Security regarding documentation of communication protocols to assist DHS in better managing federal agencies' and states' expectations regarding the methods, timing, and content of threat information and guidance provided to these entities and to ensure that DHS follows clear and consistent policies and procedures when interacting with these entities through the Homeland Security Advisory System. We also make a recommendation to the Secretary to incorporate risk communication principles into the Homeland Security Advisory System, including information on the nature, location, and time periods of threats and guidance on protective measures to take.

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 American citizens.

The Homeland Security Advisory System is comprised of five color-coded threat conditions as described below, which represent levels of risk related to potential terror attack.

- Code-red or severe alert—severe risk of terrorist attacks.
- Code-orange or high alert—high risk of terrorist attacks.
- Code-yellow or elevated alert—significant risk of terrorist attacks.
- Code-blue or guarded alert—general risk of terrorist attacks.
- Code-green or low alert—low risk of terrorist attacks.

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; and
- December 21, 2003, to January 9, 2004.

The Homeland Security Advisory System is binding on the executive branch. HSPD-3 directs all federal departments, agencies, and offices, other than military facilities,[13] to conform their existing threat advisory systems to the Homeland Security Advisory System. These agencies are responsible for ensuring their systems are consistently implemented in accordance

[13]The Homeland Security Advisory System does not directly apply to the armed forces, including their military facilities. Rather, the Department of Defense's Force Protection Condition system rates threats and sets specific measures for military facilities.

with national threat levels as defined by the Homeland Security Advisory System. Additionally, federal departments and agency heads are responsible for developing protective measures and other antiterrorism or self-protection and continuity plans in response to the various threat levels and operating and maintaining these plans. While HSPD-3 encourages other levels of government and the private sector to conform to the system, their compliance is voluntary.

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. As such, the Attorney General could assign threat levels for the entire nation, for particular geographic areas, or for specific industrial sectors. Upon its issuance, HSPD-3 also assigned responsibility to the Attorney General for establishing a process and a system for conveying relevant threat information expeditiously to federal, state, and local government officials, law enforcement authorities, and the private sector.

In November 2002, Congress passed 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. As such, the Under Secretary for IAIP is primarily responsible for issuing public threat advisories and providing specific warning information to state and local governments and to the private sector.[14] The act also charges the Under Secretary for IAIP with providing advice about appropriate protective actions and countermeasures.[15]

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. HSPD-5 directs the Secretary of

[14]DHS components and offices collaborate and share responsibility for notifying federal agencies, states, localities, the private sector, and the public of changes in the national threat level.

[15]P.L. 107-296, Sec. 201(d)(7).

Homeland Security to consult with the Attorney General and other federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, when determining the threat level, except in exigent circumstances.

Threat Information and Vulnerability of Potential Targets Inform National and Sector- or Location-Specific Threat Level Decisions

In implementing the Homeland Security Advisory System, DHS assigns national threat levels and assesses the threat condition of specific geographic locations and industrial sectors. While the national threat level has been raised and lowered for five periods, DHS officials told us that the department has not yet assigned a threat level for an industrial sector or geographic location.[16] However, DHS officials said that the department has encouraged specific sectors and regions to operate at heightened levels of security. According to DHS officials, decisions to change the national threat level and to encourage specific sectors and regions to operate at heightened levels of security involve both analysis and sharing of threat information, as well as an assessment of the vulnerability of national critical infrastructure assets that are potential targets of terrorist threats.

DHS officials told us they use the criteria in HSPD-3 in determining whether to raise the national threat level or whether to suggest that certain regions or sectors operate at heightened security levels. These criteria include:

- the credibility of threat information;
- whether threat information is corroborated;
- the degree to which the threat is specific and/or imminent; and
- the gravity of the potential consequences of the threat.

In determining whether these criteria are met and whether to raise the national threat level, DHS considers intelligence information and the vulnerability of potential targets, among other things. DHS officials told us that they use a flexible, "all relevant factors" approach to decide whether to raise or lower the national threat level or whether to suggest that certain regions or sectors operate at heightened security levels. They said that

[16]According to HSPD-3, threat levels may be assigned for the entire nation, or they may be set for a particular geographic area or industrial sector.

analysis of available threat information and determination of national threat levels and regional and sector threat conditions are specific for each time period and situation. According to these officials, given the nature of the data available for analysis, the process and analyses used to determine whether to raise or lower the national threat level or suggest that specific regions or sectors heighten their protective measures are inherently judgmental and subjective.

DHS officials said that the intelligence community continuously gathers and analyzes information regarding potential terrorist activity. This includes information from such agencies as DHS,[17] the Central Intelligence Agency, the Federal Bureau of Investigation (FBI), and the Terrorist Threat Integration Center,[18] as well as from state and local law enforcement officials. DHS officials also noted that 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 also considers the vulnerability of potential targets when determining the national threat level. For example, DHS officials explained that they hold discussions with state and local officials to determine whether potential targets specified by threat information require additional security to prevent a terrorist attack or minimize the potential gravity of an attack. According to these officials, if the target is determined to be vulnerable, then DHS will consider raising the threat level. Last, DHS determines whether there is a nationwide threat of terrorist attack or if the threat is limited to a specific geographic location or a specific industrial sector. DHS officials said that, in general, upon assessment of the above criteria, if there appears to be a threat of terrorist attack nationwide, then IAIP recommends to the Secretary of Homeland Security that the national threat level should be raised. The Secretary of Homeland Security then consults with the other members of the Homeland Security Council on whether the

[17]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.

[18]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.

national threat level should be changed.[19] 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. DHS officials also told us that when deciding whether to lower the national threat level, they consider whether the time period in which the potential threat was to occur has passed and whether protective measures in place for the code-orange alerts have been effective in mitigating the threats.

DHS officials told us that if a credible threat against specific industrial sectors or geographic locations exists, DHS may suggest that these sectors or locations operate at a heightened level of security, rather than raising the national threat level. For example, for the third code-orange alert period in our review from December 31, 2003, to January 9, 2004, threat information raised concerns of potential terrorist activity for specific industrial sectors and geographic locations. In response, DHS officials said that they encouraged those responsible for securing chemical and nuclear power plants, transit systems, and aircraft, as well as certain cities, to maintain a heightened level of security, even after the national threat level was lowered to code-yellow. However, DHS officials noted that they did not assign a threat level to these sectors and regions at that time. DHS officials further indicated that these sectors and locations were not operating at code-orange alert levels. Rather, they operated at heightened levels of security. According to DHS officials, when encouraging specific sectors or regions to continue to operate at heightened levels of security, DHS may suggest that these sectors or regions (1) implement security measures that are in addition to those implemented during a code-orange alert period, (2) continue the measures implemented during the code-orange alert period, or (3) continue selected measures implemented during a code-orange alert period.

DHS officials told us that not all threats to specific regions or sectors are communicated to the public or to officials in all regions or sectors. Rather, if intelligence information suggests a targeted threat to specific regions or industrial sectors, DHS officials said that they inform officials in the specific regions or sectors that are responsible for implementing protective measures to mitigate the terrorist threat. To inform these officials, DHS issues threat advisories or information bulletins. The threat advisories we

[19]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 code-orange alert periods in our review.

reviewed contained actionable information about threats targeting critical national networks, infrastructures, or key assets such as transit systems. These products may suggest a change in readiness posture, protective actions, or response that should be implemented in a timely manner. If the threat is less urgent, DHS may issue information bulletins, which communicate risk and vulnerabilities of potential targets. In a February 2004 testimony, the Deputy Secretary of Homeland Security said that because threat advisories and information bulletins are derived from intelligence, they are generally communicated on a need-to-know basis to a targeted audience.[20] The threat advisories and bulletins we reviewed also included advice on protective measures to be implemented by law enforcement agencies or the owners and operators of national critical infrastructure assets in response to the specific threat.

Risk Communication Principles Can Be Useful in Communicating Threat Information and Guidance to Federal Agencies and States

DHS officials told us that they have not yet officially documented protocols for communicating information about changes in the national threat level to federal agencies and states. To ensure early and comprehensive information sharing and allow for informed decision making, risk communication experts suggest that threat warnings should include the following principles: (1) communication through multiple methods, (2) timely notification, and (3) specific information on the nature, location, and timing of threats as well as guidance on actions to take in response to threats. These principles can be applied to threat information shared with federal agencies and states through the Homeland Security Advisory System. DHS used multiple methods to notify federal agencies and states of changes in the national threat level. However, many federal agencies and states responding to our questionnaires indicated that they heard about threat level changes from media sources before being notified by DHS. Federal agencies and states also reported that they did not receive specific threat information and guidance for the three code-orange alert periods from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004.

[20]DHS also issues threat advisories and information bulletins that provide general information to the public about indicators of possible terrorist attacks.

DHS Has Not Documented Communication Protocols Regarding Threat Level Changes Including the Methods, Timing, and Content of Guidance and Threat Information to Be Shared

Documentation of communication protocols can assist DHS in better managing the expectations of federal agencies and states regarding the methods, timing, and content of guidance and threat information they receive when the national threat level is raised to code-orange. DHS officials told us that they have not yet officially documented protocols for notifying federal agencies and states of changes in the national threat level, but are working to do so. They noted that it is has been difficult to develop protocols that provide sufficient flexibility for sharing information in a variety of situations. Thus, while attempts have been made to officially document protocols for notifying federal agencies and states of national threat level changes, DHS officials said that they have not made much progress in doing so and could not provide a specific target date for completing this effort. Without documented communication protocols, recipients of threat level notifications are uncertain as to how, when, and from what entity, such as which DHS agency, they will be notified of threat level changes and the content and extent of guidance and threat information they may receive. Communication protocols would, among other things, help foster clear understanding and transparency regarding DHS's priorities and operations.[21] Moreover, protocols could help ensure that DHS interacts with federal, state, local, and other entities using clearly defined and consistently applied policies and procedures.

Risk Communication Experts Suggest Warnings Should Be Communicated via Multiple Methods, Be Timely, and Include Specific Threat Information and Guidance on Protective Measures

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. Risk communication experts have identified the following as important principles for communicating risks to individuals and groups:

- Threat information should be consistent, accurate, clear, and provided repeatedly through multiple methods.
- Threat information should be provided in a timely fashion.
- To the greatest extent possible, threat information should be specific about the potential threat, including:

[21]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).

- the nature of the threat,
- when and where it is likely to occur, and
- guidance on protective measures to take to prevent or respond to the threat.

These risk communication principles have been used in a variety of 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.[22] However, warnings about terrorist threats differ from these relatively more familiar warnings.[23] For example, specific terrorist threat warnings to the public may allow terrorists to alter tactics or targets in response to the issuance of warnings. Warnings of terrorist threats may also increase general anxiety for populations 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. Yet, despite these differences, the purpose of warnings, regardless of the threat, is to provide information to citizens and groups that allows them to make informed decisions about actions to take to prevent and respond to threats. Thus, risk communication principles should be applicable to communicating terrorist threat information to federal agencies, states, and localities through the Homeland Security Advisory System.

DHS Used Multiple Methods to Notify Federal Agencies and States of Threat Level Changes

According to risk communication principles, threat information should be provided through multiple methods to ensure that dissemination of the information is comprehensive and that people receive the information regardless of their level of access to information. In addition, HSPD-3 states that the Homeland Security Advisory System should provide a

[22]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 CDC developed a nationwide reporting system that seeks to detect emerging epidemics and then to warn the public about the nature of the health threat.

[23]DHS officials told us that they are currently studying the impact that public announcement of changes in the national threat level may have on terrorist planning, targeting decisions, and attack execution.

comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities. One means of disseminating threat information is through notifications to federal agencies and states of changes in the national threat level. DHS officials told us that with each increase in the national threat level, they apply lessons learned from previous alerts to improve their notification and information sharing processes regarding threat level changes. Based on federal agencies' and states' responses to our questionnaires, it appears that DHS is making progress in expanding the scope of its notification process, which is consistent with HSPD-3. As shown in table 1, more federal agencies reported receiving direct notification from DHS for the third code-orange alert period than for the other two code-orange alert periods in our review. Similarly, more federal agencies reported receiving notification from DHS via multiple methods for the third code-orange alert period than for the other two code-orange alert periods.

Table 1: Number of Federal Agencies and States Responding to Our Questionnaires that Reported Receiving Direct Notification from DHS and Reported Being Notified through Multiple Methods for the Three Code-Orange Alert Periods

	Number of federal agencies n = 25[a]			Number of states n = 41[b]		
DHS notification	March 17 to April 16, 2003	May 20 to 30, 2003	December 21, 2003, to January 9, 2004	March 17 to April 16, 2003	May 20 to 30, 2003	December 21, 2003, to January 9, 2004
Reported receiving direct notification from DHS	17	19	20	35	33	39
Reported receiving notification from DHS by more than one method	8	10	14	25	24	31

Source: GAO analysis of questionnaire data.

[a]In the questionnaire we sent to DHS, we did not include questions on how DHS was notified of changes in the national threat level. Thus, this agency is not included in our analysis of code-orange alert notifications.

[b]One state responding to our questionnaire did not provide responses on how it was notified of changes in the national threat level. Additionally, 1 state reported that it did not follow the Homeland Security Advisory System. Thus, these 2 states are not included in our analysis of code-orange alert notifications.

DHS used the following methods, among others, to notify entities of changes in the national threat level, according to federal agencies' and states' responses to our questionnaires and discussions with DHS and local government officials:

- Conference calls between the Secretary of Homeland Security and state governors and/or state homeland security officials.
- Telephone calls from Federal Protective Service[24] (FPS) officials to federal agencies.
- E-mail, telephone, or electronic communications from Homeland Security Operations Center (HSOC) representatives to the federal, state, or local agencies they represent.
- FBI electronic systems, such as the National Law Enforcement Telecommunications System.
- E-mail and/or telephone communications with federal agencies' chief of staff and public affairs offices.
- E-mail and/or telephone communications to local government associations such as the National Governors Association and the U.S. Conference of Mayors.

Federal Agencies and States Reported Hearing about Threat Level Changes from Media Sources before Receiving Notification from DHS

Risk communication experts suggest that threat information should be provided in a timely fashion to prevent unofficial sources, such as the media, from reporting information before official sources, including government agencies, do so. These principles suggest that lack of early and open information sharing from official entities can undermine these entities' credibility. HSPD-3, as amended by HSPD-5, states that the Secretary of Homeland Security should establish a process and a system for conveying relevant information regarding terrorist threats expeditiously. In addition, for an entity to control its operations, it must have relevant, reliable, and timely communications relating to internal and external events.

Many federal agencies and some states responding to our questionnaires expressed concerns that they learned about national threat level changes

[24]The Federal Protective Service became part of DHS upon creation of the department in March 2003. Its overall mission is to provide law enforcement and security services to over one million tenants and daily visitors to all federally owned and leased facilities nationwide. FPS protection services focus directly on the interior security of the nation's facilities and the reduction of crimes and potential threats in federal facilities throughout the nation.

from media sources before being notified by DHS. Specifically, 16 of 24 federal agencies[25] indicated that they learned about threat level changes via media sources prior to being notified by DHS for at least one of the three code-orange alert periods. Likewise, 15 of 40 states[26] reported learning about national threat level changes via media sources prior to being notified by DHS for at least one of the three code-orange alert periods. This raises questions about whether DHS is always conveying information regarding threat level changes to government entities expeditiously, as required by HSPD-3.

Moreover, some states reported that their ability to provide credible information to state and local agencies and the public was hindered because they did not receive notification from DHS before the media reported on the threat level changes. For example, 6 states noted that when media sources reported national threat level changes before state and local emergency response officials were directly notified by DHS, these officials did not have sufficient time to prepare their response to the threat level change, including how they would respond to requests from the public for additional information on the threat level change. One other state reported that it would prefer to first learn about changes in the national threat level from DHS so that it has sufficient time to notify state agencies and localities of the change and so that these entities can prepare their responses before the public is notified of the change. Additionally, 8 localities from which we obtained information indicated that they first learned of threat level changes from media sources, and 4 of these localities would prefer to be notified of threat level changes prior to the public. Officials from some of these localities told us that after media sources reported the change, their agencies received requests for detailed information on the change from the public and other entities. They noted that their agencies appeared ineffective to the public and other entities because, without notification of the national threat level change before it

[25]We did not ask DHS questions about how it first learned about changes in the national threat level. One other federal agency did not respond to our questions on how federal agencies first learned about changes in the national threat level. Thus, these 2 federal agencies are not included in our analysis of how federal agencies first learned about national threat level changes.

[26]Two states did not provide responses to our questions on how states first learned about changes in the national threat level. Additionally, 1 state reported that it does not follow the Homeland Security Advisory System. Thus, these 3 states are not included in our analysis of how states first learned about national threat level changes.

was reported by media sources, they did not have time to prepare informed responses.

DHS officials told us that they attempt to notify federal agencies and states of threat level changes before the media report on the changes. However, they noted that DHS has not established target time periods in which to notify these entities of the threat level changes. Furthermore, DHS officials indicated they were aware that the media sometimes reported threat level changes before DHS notified federal and state officials, and in the case of the second code-orange alert period in our review, before the decision to raise the threat level was even made. DHS officials told us that they send notifications/advisories to the media to inform them of impending press conferences and that the media may speculate about announcements of threat level changes that may be made at the press conferences. DHS officials indicated that the department is trying to determine the best approach for managing expectations created by this situation.

Federal Agencies and States Reported that They Generally Did Not Receive Specific Guidance and Threat Information for Code-Orange Alert Periods, Hindering Their Response to the Alerts

Risk communication experts said that without specific information on the nature, location, and timing of threats and guidance on actions to take, citizens may not be able to determine whether they are at risk and make informed decisions about actions to take in response to threats, and thus may take inappropriate actions. According to HSPD-3, the Homeland Security Advisory System was established to inform and facilitate decisions appropriate to different levels of government regarding terrorist threats and measures to take in response to threats. However, federal agencies and states responding to our questionnaires generally indicated that they did not receive guidance and specific information on threats on the three occasions included in our review when the national threat level was raised to code-orange. These entities reported that insufficient information on the nature, location, and timing of threats and insufficient guidance on recommended measures hindered their ability to determine whether they were at risk as well as their ability to determine and implement protective measures.[27]

As shown in table 2, federal agencies and states responding to our questionnaires indicated that they generally did not receive specific

[27]Please see appendix III for information on guidance and information and intelligence federal agencies and states reported using from sources other than DHS to determine protective measures to take for the three code-orange alert periods.

information on threats with notification of increases in the national threat level for the three code-orange alert periods included in our review. Yet, as table 2 suggests, a greater number of federal agencies and states reported receiving more specific threat information for the third code-orange alert period than for the other two code-orange alert periods.

Table 2: Number of Federal Agencies and States That Reported Receiving Types of Information with Notification from DHS for the Three Code-Orange Alert Periods

	Number of federal agencies n = 25[a]			Number of states n = 42[b]		
Type of information	March 17 to April 16, 2003	May 20 to 30, 2003	December 21, 2003, to January 9, 2004	March 17 to April 16, 2003	May 20 to 30, 2003	December 21, 2003, to January 9, 2004
General information on threats	10	11	12	35	34	37
Information on region- or sector-specific threats	6	6	9	9	11	22
Information on site- or event-specific threats	4	4	8	8	7	15
Information on timing of threats	4	4	8	6	7	17
Recommended measures for preventing incidents	6	4	7	20	18	23
Recommended measures for responding to incidents	4	4	6	8	7	10

Source: GAO analysis of questionnaire data.

[a]In the questionnaire we sent to DHS, we did not include questions on how DHS was notified of changes in the national threat level. Thus, this agency is not included in our analysis of code-orange alert notifications.

[b]One state reported that it did not follow the Homeland Security Advisory System. Thus, this state is not included in our analysis of code-orange alert notifications.

As shown in tables 3 and 4, federal agencies and states responding to our questionnaires indicated that guidance and specific information on threats, if available, would have assisted them in determining their levels of risk and measures to take for the December 21, 2003, to January 9, 2004, code-orange alert period. Results for the other two code-orange alert periods are consistent with those reported in tables 3 and 4 for the third code-orange alert period.

Table 3: Number of Federal Agencies That Indicated Specific Types of Information That Would Have Been Helpful to Determine Measures to Take for the Code-Orange Alert Period from December 21, 2003, to January 9, 2004

Type of information	Number of federal agencies n = 25[a]
Timing of threats	24
Region- or sector-specific threats	23
Site- or event-specific threats	23
Recommended measures for preventing incidents	21
Recommended measures for responding to incidents	19

Source: GAO analysis of questionnaire data.

[a]In the questionnaire we sent to DHS, we did not ask DHS to indicate what other types of information would have been helpful to determine measures to take for the three code-orange alert periods. Thus, this agency is not included in our analysis of guidance and information preferred by federal agencies.

Table 4: Number of States That Indicated Specific Types of Information That Would Have Been Helpful to Determine Measures to Take for the Code-Orange Alert Period from December 21, 2003, to January 9, 2004

Type of information	Number of states n = 41[a]
Region- or sector-specific threats	34
Site- or event-specific threats	34
Timing of threats	32
Recommended measures for responding to incidents	29
Recommended measures for preventing incidents	27

Source: GAO analysis of questionnaire data.

[a]One of the states responding to our questionnaire did not provide responses on the types of information that would have been helpful to it in determining measures to take for the three code-orange alert periods. Additionally, 1 state reported that it did not follow the Homeland Security Advisory System. Thus, these 2 states are not included in our analysis of guidance and information preferred by states.

Furthermore, 13 localities reported to us that information on site-, area-, or event-specific threats would have been beneficial to them in responding to the code-orange alert periods. Six of the localities from which we obtained information reported that information on region- or sector-specific threats would have assisted them in determining their level of risk and measures to take in response to the three code-orange alerts in our review.

When federal agencies and states perceive that they have not received sufficient guidance and threat information, these entities may not be able to determine whether they are at risk from possible threats or what measures to take in response to the threats. For example, 1 federal agency reported that DHS never notified the agency as to whether Washington, D.C., would remain at heightened security levels after the national threat level was lowered to code-yellow on January 9, 2004, which resulted in the agency maintaining code-orange alert measures for an additional week and incurring additional costs for doing so. Another federal agency reported that to respond to the code-orange alerts, it implemented measures at all facilities regardless of the specific location or risk involved, which spread resources across all facilities rather than focusing the measures on mitigating specific threats. Officials from 1 state and 1 locality noted that without specific threat information, these entities did not understand the true nature of the threat and what impact the threat may have on them.

Federal agencies and states responding to our questionnaire also indicated that without guidance and specific threat information, they may not be able to effectively and efficiently target or enhance protective measures to respond to the code-orange alerts. Eighteen of the 25 federal agencies and 32 of the 41 states providing responses to the questions on operational challenges in our questionnaires reported that lack of sufficient threat information was a challenge they faced during the three code-orange alert periods. Moreover, in responding to our questionnaires, 16 federal agencies and 12 states noted that insufficient information on threats makes it difficult for these entities to focus resources on specific measures to respond to threats.

At a February 2004 hearing, the Deputy Secretary of Homeland Security said that the department's communications of national threat level changes are intended to provide specific information regarding the intelligence supporting the change in the threat level, and that protective measures are developed and communicated, along with the threat information, prior to a public announcement of the decision. DHS officials told us that they provide specific threat information, when available, to federal agencies, states, and localities at risk and with the authority to respond to threats. For example, the Deputy Secretary said that threat information that was shared by DHS regarding changes in the national threat level was primarily intended for security professionals at all levels of government and the private sector. Moreover, to provide more specific threat information and respond to sector- and location-specific security needs, DHS officials told us they have adjusted the system based on feedback from federal, state,

local and private sector officials; tests of the system; and experience with previous periods of code-orange alert. For example, for the most recent code-orange alert from December 21, 2003, to January 9, 2004, the Deputy Secretary noted in his February 2004 testimony that DHS provided specific recommendations for protective measures to industrial sectors and for geographic areas in response to specific threat information.

Federal Agencies Reported Implementing Few New Protective Measures for Code-Orange Alerts because They Always Operate at High Security Levels, While States Varied Their Responses

The majority of federal agencies responding to our questionnaire indicated that they maintain high security levels regardless of the national threat level and, as a result, they did not need to implement a substantial number of new or additional protective measures to respond to the three periods of code-orange alert from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004. For the most part, these federal agencies reported enhancing existing protective measures to respond to the three code-orange alerts. To a lesser extent, federal agencies continued the use of existing measures, without enhancement, during the code-orange alert periods. On the other hand, states differed in the extent to which they enhanced or maintained existing measures or implemented additional protective measures solely in response to the code-orange alerts. Federal agencies and states reported benefits, such as a heightened sense of security among employees, from enhancing or implementing protective measures for the code-orange alert periods. However, federal agencies and states also indicated that taking such measures negatively affected their operations, for example, by redirecting resources from normal operations to code-orange alert duties.

Federal Agencies Reported that High Security Postures Reduced the Need to Implement Additional Measures Solely in Response to Code-Orange Alerts

More than half of the federal agencies responding to our questionnaire indicated that they operate at high security levels, regardless of the national threat level. Thus, they did not need to implement a significant number of new or additional protective measures to respond to code-orange alerts. For example, in response to the third code-orange alert period in our review—December 21, 2003 to January 9, 2004—10 of 24[28] federal agencies indicated that they most commonly enhanced existing protective measures, such as increasing facility security patrols. During the same code-orange alert period, 8 federal agencies reported most often continuing protective measures at their pre-code-orange alert levels, for example, relying on continuing activation of monitoring systems and intrusion detection devices. For the remaining 6 federal agencies, there were slight differences among the number of protective measures they enhanced during the third code-orange alert period, those they maintained at pre-code orange alert levels, and those they implemented solely in response to the code-orange alert. For one of these agencies,

- three of the protective measures in place for the third code-orange alert period were maintained at their pre-code-orange alert levels,
- three of the protective measures were enhanced beyond their pre-code-orange alert levels, and
- four protective measures were implemented solely for the code-orange alert period.

Results for the other two code-orange alert periods in our review are similar to those reported for the third code-orange alert period. For more information on protective measures federal agencies most commonly reported having in place for the three code-orange alert periods and their testing of such measures, see appendix IV.

[28]One federal agency responding to our questionnaire reported that it did not implement protective measures because it is located in a privately owned building and is not responsible for its own security. Another federal agency did not provide a response to questions related to the protective measures taken during code-orange alerts due to security concerns. Thus, these 2 agencies are not included in our analysis of protective measures.

States Differed in the Extent to Which They Implemented Additional Protective Measures for Code-Orange Alerts

Overall, states differed in the extent to which they implemented additional protective measures for the three code-orange alert periods in our review. Based on our analysis of questionnaire responses from the 40 states[29] that provided information on protective measures for the third code-orange alert period in our review,

- 16 states most often enhanced protective measures that were already in place prior to the code-orange alert period;
- 6 states most often implemented new protective measures for the code-orange alert;
- 5 states most often maintained protective measures that were already in place at their pre-code-orange alert levels; and
- 13 states employed a varied response, enhancing measures, continuing existing measures, and/or implementing new measures in roughly equal proportion.

Results for the other two code-orange alert periods in our review are similar to those reported for the third code-orange alert period.

Various reasons influenced the extent to which states responding to our questionnaire enhanced, maintained, or implemented new protective measures. For example, some states reported that they already operated at heightened security levels and, therefore, did not need to implement additional protective measures in response to the code-orange alerts in our review; rather they enhanced measures already in place. Other states indicated that the extent to which they implemented protective measures for the code-orange alert periods in our review depended on specific threat information. For example, 1 state indicated that it did not enhance existing protective measures or implement new protective measures for the code-orange alert periods in our review because there were no specific threats to the state that required it to do so. Other states indicated that the extent to which they implemented protective measures for code-orange alert periods depended on the required level of security for their critical infrastructure

[29]Of the 43 states responding to our questionnaire, 1 reported that it did not follow the Homeland Security Advisory System and 2 did not provide responses to questions related to protective measures taken during code-orange alerts. Thus, these 3 states are not included in our analysis of protective measures.

sites. For example, 1 state reported that it implemented new protective measures for its nuclear power plants during code-orange alert periods, but for some other critical infrastructure assets, it enhanced security measures already in place. Some states also indicated that resource constraints determined the extent to which they enhanced or implemented new protective measures for code-orange alert periods. For example, 2 states indicated that they had to implement a substantial number of new protective measures for the three code-orange alert periods in our review because they could not afford to always operate at a high level of security. For more detailed information on protective measures that states most commonly reported having in place for code-orange alert periods and testing of these measures, see appendix IV.

Additionally, 4 localities from which we obtained information reported that they did not enhance or implement a substantial number of protective measures to respond to the code-orange alerts because they did not receive specific threat information indicating that the localities were at risk. For example, 1 locality reported that because it did not receive specific threat information on possible targets, the locality did not take any measures to respond to the code-orange alerts. Additionally, another locality noted that its emergency response staff was not able to implement additional measures in response to the code-orange alerts because the staff was too busy with regular duties such as responding to 911 calls.

Federal Agencies and States Reported that Protective Measures for Code-Orange Alerts Were Beneficial, but also Presented Operational Challenges and Affected Normal Operations

Federal agencies and states responding to our questionnaires indicated that they benefited in various ways from the protective measures they enhanced or implemented during the code-orange alert periods, but also noted that they faced operational challenges in responding to the three code-orange alert periods in our review. For example, federal agencies and states reported that protective measures increased employees' sense of security, promoted staff awareness, and provided visible deterrents to possible threats. However, federal agencies and states responding to our questionnaires also reported that their operations were negatively affected during code-orange alerts as a result of protective measures they enhanced or implemented. For example, 10 federal agencies and 13 states reported that they had to redirect resources from normal operations to enhance or implement protective measures for code-orange alerts. One locality also reported that its operations were negatively affected by the redirection of personnel, which resulted in delays of maintenance activities and preventative exercises as well as postponement of training. Additionally, 15 federal agencies noted delays for visitors and employees. Some of these

federal agencies and states reported that maintaining a code-orange alert level of security for more than a few days at a time significantly drained their security resources—an effect federal agencies and states have identified as "code-orange alert fatigue."

Federal agencies and states also indicated that the lack of federal governmentwide coordination hindered their ability to respond to threats. Without coordination of information and intelligence sharing during code-orange alert periods, federal agencies and states responding to our questionnaires noted that they may not receive threat information needed to help them determine and implement their responses to code-orange alerts. For example, 1 federal agency reported that it received different requests from several federal agencies to deploy personnel to different locations. This federal agency noted that improved federal governmentwide coordination might result in more efficient assignment of resources. Similarly, 1 locality noted that because different government agencies notified different local agencies of changes in the national threat level, first responders and local officials could not effectively and efficiently coordinate and implement protective resources. On the other hand, 1 state official raised concerns about whether federal agencies were fully informed of the information DHS provided to states and had the information needed to implement appropriate local security measures. This official noted that persons from the Transportation Security Administration, the Coast Guard, and the U.S. Army Corps of Engineers called his state's homeland security office for advisories and bulletins DHS had provided to the state. Because of these information requests, this official noted that the state was concerned that officials from these federal agencies did not receive information needed to implement security measures, especially at airports. In commenting on a draft of this report, DHS officials stated that the department is working to address this problem.

Six states also indicated that insufficient information from DHS on national critical infrastructure assets made it difficult to effectively protect these assets during the code-orange alert periods. Three of these states indicated that DHS asked them to protect specific national critical infrastructure sites, some of which were no longer operational or others that were closed, such as shopping malls. Officials in one state indicated that DHS did not coordinate with the state when it initially developed this list of national critical infrastructure assets. DHS officials told us that the department developed a list of national critical infrastructure assets to assist states in determining protective measures to implement at their national critical

infrastructure sites. According to the Deputy Director of the Protective Security Division of IAIP, DHS initially developed a list of 145 national critical infrastructure assets, including nuclear power plants, chemical facilities, and transportation systems, to ensure their security during Operation Liberty Shield.[30] This official told us that DHS identified national critical infrastructure assets for the list based on intelligence information indicating possible assets at risk, the vulnerabilities of these assets, and possible consequences of an attack on assets, including health, safety, and economic impacts. DHS did not coordinate with states and localities in developing the national critical infrastructure assets list for Operation Liberty Shield because planning and timing of military operations for the war in Iraq and for Operation Liberty Shield were given the highest classification levels and discussed only at the federal level. The Deputy Director said that since Operation Liberty Shield, DHS has continually expanded and revised its national critical infrastructure assets list based on ongoing analysis of threat information and input from states. In reviewing a draft of this report, DHS officials told us that its Protective Security Division has given all states and territories opportunities to suggest assets to be included in the National Asset Database as well as to verify and validate information DHS maintains on such assets. To enhance standard security levels at national critical infrastructure sites, this DHS official said that the department is working with states to develop plans for protecting the immediate areas surrounding national critical infrastructure assets and reducing vulnerabilities in those areas. In particular, the Deputy Director told us that DHS provided guidance and information to states and local law enforcement agencies to develop protection plans for areas around national critical infrastructure assets.

DHS Efforts to Gather Information on Protective Measures Taken by States and Localities

The majority of states responding to our questionnaire indicated that, for all three code-orange alert periods in our review, DHS requested some information on protective measures taken by states in response to the heightened threat levels. However, as shown in table 5, most states reported that DHS did not request information on the effectiveness of these security measures.

[30]Operation Liberty Shield was a comprehensive plan to increase protection for U.S. citizens and critical infrastructure assets during the war with Iraq in March and April 2003. For example, this plan included increased security measures at U.S. borders and enhanced protection for the transportation system.

Table 5: Number of States That Indicated DHS Requested Information on Protective Measures Taken by the State in Response to the Three Code-Orange Alert Periods

	Number of states n = 40[a]		
Type of information	**March 17 to April 16, 2003**	**May 20 to 30, 2003**	**December 21, 2003, to January 9, 2004**
Security actions taken in response to the elevated threat	28	22	33
Security actions taken at specific critical infrastructure sites	24	18	31
Effectiveness of state or government security actions taken	7	7	8

Source: GAO analysis of questionnaire data.

[a]Of the 43 states responding to our questionnaire, 1 reported that it did not follow the Homeland Security Advisory System and 2 did not provide responses to the question regarding the extent to which DHS requested information on protective measures taken by states in response to increased threat levels. Therefore, these 3 states are not included in our analysis of states from which DHS requested information on protective measures.

An Office of State and Local Government Coordination official said that DHS maintains close contact with states and localities during code-orange alert periods and fosters information sharing about actions taken to increase security. For example, this official noted that DHS co-sponsored a February 2003 workshop with the FBI to encourage state-level implementation of the Homeland Security Advisory System and provide a forum for information exchange among state and local homeland security representatives. More recently, on April 19, 2004, DHS launched a new Web site (www.llis.gov) to provide a nationwide network of lessons learned and best practices for homeland security officials and emergency responders. For the most recent code-orange alert from December 21, 2003 to January 9, 2004, DHS officials noted that they contacted states to inquire about protective measures that were put in place. According to DHS officials, they made such inquiries to (1) monitor the extent to which states implemented protective measures that DHS recommended, (2) apprise the White House of actions taken in response to code-orange alerts, and (3) enhance DHS officials' understanding of protective measures for which states may seek reimbursement.

Costs Reported by Federal Agencies, though Limited, Suggest a Decline in Additional Costs

Sixteen of 26 federal agencies responding to our questionnaire reported additional costs for at least one of the code-orange alert periods in our review. We examined the cost information provided by these agencies for obvious errors and inconsistencies and examined agencies' responses to the questionnaire regarding the development of the cost information. In doing so, we found that these federal agencies' cost data were generated from various sources, such as financial accounting systems, credit card logs, and security contracts. Additionally, this cost information is not precise, nor do the costs likely represent all additional costs incurred during code-orange alert periods. In some cases, we have concerns about the reliability of the data sources used to develop the costs reported to us. For example, 6 of the 16 federal agencies reported that they extracted some of the code-orange alert cost data from their agencies' financial accounting systems. However, as reported in the fiscal year 2005 President's Budget, 5 of these agencies' financial management performance had serious flaws as of December 31, 2003. Despite these limitations, we believe the cost data to be sufficiently reliable as indicators of general ranges of cost and overall trends. However, the data should not be used to determine the cumulative costs incurred across all federal agencies.

Based on the information provided by federal agencies, total additional costs reported by federal agencies responding to our questionnaire for the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods were less than 1 percent of these agencies' fiscal year 2003 homeland security funding, as reported to OMB. On the basis of this cost information, we determined additional average daily costs ranged from about $190 to about $3.7 million across all three code-orange alert periods in our review. Based on information reported by these agencies, the additional average daily costs incurred across code-orange alert periods have declined over time.

Some of these federal agencies attribute this decline to continued enhancement of standard levels of security. Some federal agencies reported that they did not have any additional costs during code-orange alert periods, as they either did not implement any additional protective measures or they redirected already existing resources to implement additional code-orange alert measures rather than employ additional resources. Although federal agencies may not have reported additional costs directly as a result of implementing protective measures for code-orange alerts, actions taken such as redirecting resources from normal operations would have resulted in indirect costs.

Additional Costs Reported by Federal Agencies for the First and Second Alert Periods in Our Review Were Less than 1 Percent of Agencies' 2003 Homeland Security Funding

Sixteen of 26 federal agencies responding to our questionnaire reported additional costs for the first code-orange alert period in our review—March 17 to April 16, 2003. Fifteen of these agencies also reported additional costs for the second code-orange alert period in our review—May 20 to 30, 2003. For 13 of the 15 federal agencies that reported additional costs for both the first and second code-orange alert periods in our review, we calculated that the additional costs reported by these agencies were less than 1 percent of these agencies' fiscal year 2003 homeland security funding. This calculation is based on OMB's *2003 Report to Congress on Combating Terrorism*, which presented information federal agencies reported to OMB on the amount of homeland security funding authorized to federal agencies in fiscal year 2003.

For the 16 federal agencies responding to our questionnaire that reported additional costs during the first code-orange alert period in our review, we calculated average daily additional costs, which ranged from about $190 to about $848,000.[31] A cabinet level agency with security responsibilities limited to protecting its facilities and employees reported the least additional costs for this code-orange alert period, while another cabinet level agency that, in addition to securing its facilities, is responsible for the protection of national critical infrastructure assets reported the most additional costs. For the 15 federal agencies that reported additional costs for the second and third—December 21, 2003, to January 9, 2004—code-orange alert periods in our review, we calculated additional average daily costs that ranged from about $240 to about $3.7 million and from about $190 to about $1 million, respectively.[32] The agency that reported the least additional costs for the second and third code-orange alert periods in our review was an independent agency, while the agencies that reported the most additional costs for these code-orange alert periods were generally cabinet agencies that are responsible for the protection of national critical infrastructure assets. Most of the additional costs federal agencies reported were personnel costs, such as overtime wages or costs for additional security personnel. Appendix V provides additional information regarding cost information submitted by federal agencies.

[31]Five federal agencies reported that they did not incur any additional costs during the March 17 to April 16, 2003, code-orange alert period.

[32]Six federal agencies reported that they did not incur any additional costs during the May 20 to 30, 2003, and December 21, 2003, to January 9, 2004, code-orange alert periods. One of these 6 agencies did incur additional costs for the March 17 to April 16, 2003, code-orange alert period.

Federal Agencies' Additional Average Daily Costs for Code-Orange Alerts Declined

Based on the cost information provided by federal agencies, we determined that there was a decline in the additional average daily costs incurred by these federal agencies over the three code-orange alert periods in our review. Of the 15 federal agencies that reported additional costs for the first and third code-orange alert periods, 11 federal agencies experienced an overall decline in the additional average daily costs across the code-orange alert periods. Five of these 11 federal agencies indicated that their additional costs declined across the three code-orange alert periods in our review because they were consistently enhancing their baseline levels of security, which, in turn, required fewer additional protective measures during subsequent code-orange alert periods. Three agencies indicated that the decline in additional average daily costs was due to a reduction in the number of protective measures they had in place. One of these agencies explained that rather than implementing general protective measures with the receipt of specific threat information for the third code-orange alert in our review, it was able to determine the most appropriate protective measures to put in place.

Some Federal Agencies Reported No Additional Costs Due to Redirection of Existing Resources and Lack of Additional Measures

Six federal agencies reported that they did not have additional costs for at least two of the code-orange alert periods in our review. Four of these agencies indicated that they did not have additional costs because they redirected already existing resources to implement additional protective measures for the code-orange alert periods rather than employ additional resources. For example, 2 agencies said that they were able to increase the frequency of their facility patrols without hiring additional guards or requiring guards to work overtime by closing one of the facility's entrances during code-orange alert. Therefore, the guards who would normally secure that entrance were assigned to conduct additional roaming facility patrols. Furthermore, 2 of the 4 agencies indicated that they planned their protective measures with the specific intent that the agency would not incur any additional security-related costs during code-orange alert periods. The remaining 2 agencies reported that they did not have any additional costs because they did not implement additional protective measures for the code-orange alert periods. One agency explained that it did not implement any protective measures during code-yellow or code-orange alert periods because it is located in a privately owned building and is not responsible for the security of its facility, nor does this agency have field offices for which it is responsible.

Although these federal agencies reported that they did not directly incur additional costs to implement protective measures for code-orange alert periods, the consequences of implementing such protective measures may have resulted in indirect costs for these agencies. Some federal agencies responding to our questionnaire indicated they could not quantify these indirect costs. However, federal agencies provided examples of redirection of resources that may have caused them to incur such costs. For example, 13 federal agencies noted that in order to implement code-orange alert measures, they had to redirect existing resources from normal operations. Furthermore, one agency indicated that redirecting resources in response to code-orange alerts prevented the agency from performing mission-related activities, such as deterrence of criminal activity other than terrorism. Additionally, 16 federal agencies said that as a result of implementing measures for code-orange alerts, there were delays for employees and visitors entering facilities, which may have resulted in loss of productivity among employees and a delay in provision of services. Seven federal agencies indicated that as part of their response to code-orange alerts, they postponed or cancelled agency-sponsored activities such as training for staff development.

Cost Data Collected by DHS and Data Reported by Others Cannot be Generalized

DHS has collected limited information on costs incurred by states and localities during code-orange alert periods through its State Homeland Security Grant Program – Part II and the Urban Areas Security Initiative – Part II. States must submit information to DHS to be reimbursed for costs incurred as a result of actions taken to increase critical infrastructure protection during code-orange alerts. However, this cost information does not represent all costs incurred by states and their localities during code-orange alert periods. Therefore, it cannot be used to assess the financial impact of code-orange alerts on states and localities. The U.S. Conference of Mayors also collected information and reported estimates of costs localities incurred in response to code-orange alerts. Moreover, a Director with the Center for Strategic and International Studies estimated and reported[33] costs incurred by federal agencies during code-orange alerts. However, because of limitations in the scope and methodologies used in these estimates, the cost information they reported may not be adequate for making generalizations regarding additional costs states and localities incurred in response to code-orange alerts.

[33]According to a Center for Strategic and International Studies press release, the estimate cited by its Director is solely the view of the Director and not that of the Center.

DHS Collected Limited Information on Costs Incurred by States and Localities during Code-Orange Alert Periods through Its Grant Programs

DHS issued an information bulletin to states on March 21, 2003, advising them to capture additional costs incurred by the state and its localities during the March 17 to April 16, 2003, code-orange alert period for the protection of critical infrastructure, in the event that funds became available to reimburse states and localities for these additional costs. Through the fiscal year 2003 State Homeland Security Grant Program – Part II (SHSGP II), DHS made a total of $200 million available to states and local communities to mitigate costs of critical infrastructure protection[34] during the period of hostilities with Iraq and future periods of heightened threat.[35] According to SHSGP II guidelines, SHSGP II funds can be used for

- public safety agency overtime costs,
- contract security personnel costs, and
- state-ordered National Guard deployments required to augment security at critical infrastructure.[36]

Additionally, at least 50 percent of a state's award must be allocated to local communities.

Through the fiscal year 2003 Urban Areas Security Initiative – Part II (UASI II), DHS made approximately $125 million available to reimburse select urban areas for costs incurred during the February 7 to February 27, 2003; March 17, 2003, to April 16, 2003; and May 20 to 30, 2003, code-orange alert periods. Specifically, UASI guidelines allowed for the reimbursement of costs associated with overtime and critical infrastructure protection.[37] On

[34]The SHSGP II guidelines define critical infrastructure as any system or asset that if attacked would result in catastrophic loss of life and/or catastrophic economic loss. Some examples of critical infrastructure are public water systems serving large population centers and nuclear power plants.

[35]SHSGP II also made $1.3 billion available for first responder preparedness to supplement funding received by first responders through the fiscal year 2003 State Homeland Security Grant Program.

[36]For the December 21, 2003, to January 9, 2004, code-orange alert period, DHS informed states that SHSGP II funds could also be used to reimburse costs incurred by states and localities for staffing their emergency operations centers for this, as well as previous, code-orange alert periods.

[37]Only 25 percent of UASI II funding can be used by localities to reimburse additional costs incurred during code-orange alert periods.

January 23, 2004, DHS issued a memorandum to state officials indicating that SHSGP II and UASI II funding could also be used to reimburse states and localities for additional costs incurred for protection of critical infrastructure for the December 21, 2003, to January 9, 2004, code-orange alert period.

For the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods, DHS required states to submit budget detail worksheets, including the name of the state agency or local jurisdiction that incurred the additional critical infrastructure protection costs and the amount the agency or locality requested for reimbursement. For the December 21, 2003, to January 9, 2004, code-orange alert period, DHS provided a more detailed template for the budget detail worksheet, which asked states to identify the critical infrastructure site protected and the amount of costs incurred and personnel deployed for each of the following categories:

- National Guard deployment,
- public safety overtime,
- contract security personnel, and
- emergency operations center overtime.

Additionally, for all three code-orange alert periods in our review, DHS asked states to distinguish between state-level and local-level costs. Through SHSGP II and UASI II, states were awarded a specified amount from which they could draw down over a period of 2 years to reimburse them for additional costs incurred during code-orange alert periods. According to the grant guidelines, DHS must approve the budget detail worksheet before states and localities can obligate, expend, or draw down these grant funds. DHS, in monitoring these grant programs, takes steps to validate critical infrastructure protection costs. Additionally, amounts that states and localities expend in excess of $300,000 are subject to an external audit which, when completed, provides assurance regarding the reliability of the cost data.[38]

[38]According to SHSGP II and UASI II program guidelines, recipients that expend $300,000 or more of federal funds during their fiscal year are required to submit a statewide financial and compliance audit report. The audit must be performed in accordance with the U.S. General Accounting Office's Government Auditing Standards and OMB Circular A-133.

Based on the following, it is unlikely that the cost information submitted by states to DHS represents all additional costs incurred by states and localities during code-orange alert periods:

- States have up to 2 years from the time when the grant is awarded to submit requests for reimbursement of additional code-orange alert costs.

- Some states are still in the process of validating proposed costs incurred by the state and its localities. For example, one state estimated that its state agencies and localities incurred an additional $3.7 million for the March 17 to April 16, 2003, code-orange alert period. However, the state could only validate additional code-orange alert costs of about $1.3 million, and thus could only report this amount as eligible for DHS reimbursement.

- The cost information submitted by states does not include additional costs for training or the purchase of equipment and materials during code-orange alert periods.

Additionally, DHS officials told us that not all states and localities that incurred additional costs have requested reimbursement; therefore, not all states and localities have submitted information to DHS on additional code-orange alert costs. Since the cost information does not include all costs incurred by states and localities for code-orange alerts, it should not be used to reach conclusions about the financial impact of these alerts on states and localities.

According to the cost information collected by DHS, as of April 14, 2004, 40 states provided cost information to DHS in order to draw down funds to reimburse additional costs incurred during the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods. Based on this cost information, the reported state share of additional code-orange alert costs ranged from about $7,900 to about $8 million for both the first and second code-orange alert periods, which lasted a total of 40 days. The locality share of additional costs incurred during these two code-orange alert periods ranged from about $2,800 to about $28 million.

As of April 14, 2004, 33 states provided information on additional costs incurred during the December 21, 2003, to January 9, 2004, code-orange alert period to DHS. Based on this information, additional costs incurred by state agencies for this code-orange alert period, which lasted 19 days,

ranged from about $2,000 to about $7 million. Additional costs incurred by localities during this code-orange alert period ranged from about $3,000 to about $4 million. In general, the states that have numerous critical infrastructure sites, as identified by DHS, were the ones that reported the most additional code-orange alert costs collectively for the state and its localities. Additionally, DHS officials noted that overtime costs for law enforcement or security personnel appear to be the primary expense incurred by states and localities.

You also requested that we determine the extent to which DHS analyzes available cost data related to code-orange alerts and the role that OMB plays in providing guidance to DHS on capturing such costs. Though not required to do so, DHS has not analyzed the cost data collected to identify trends or assess the financial impact code-orange alerts have on states and localities. DHS has not tallied individual or overall state and local costs for any of the increased threat alert periods. However, as cost information submitted by states for reimbursement through SHSGP II and UASI II does not include all costs incurred by states and localities during code-orange alert periods, such analysis may not be appropriate using these data. According to an OMB representative, OMB has not provided specific guidance to DHS in capturing and totaling additional costs that states and localities incurred during periods of heightened national threat levels, nor is it required to do so. However, the representative noted that OMB is concerned about the funds that the federal government expends on these programs and activities.

Publicly Reported Cost Information May be Insufficient for Assessing Financial Impact of Code-Orange Alerts

Prior to this report, the U.S. Conference of Mayors and a Director with the Center for Strategic and International Studies have been the only organization or official to attempt to report estimates of costs incurred by various governmental entities in response to code-orange alerts. However, despite their efforts, the information reported by the U.S. Conference of Mayors and a Director at the Center for Strategic and International Studies Homeland Security Initiatives, may not be adequate to draw conclusions regarding the extent to which responding to code-orange alerts imposes a financial burden on governmental entities.

On March 27, 2003, the Conference of Mayors published a report[39] that estimated localities within the United States were spending $69.5 million per week in response to the March 17 to April 16, 2003, code-orange alert period. However, the U.S. Conference of Mayors' estimate may not provide an adequate basis for drawing conclusions regarding the financial impact of code-orange alerts on localities due to several factors such as:

- lack of guidance to localities for developing their estimates,
- low response rate,
- limited scope, and
- the absence of independent verification or confirmation of amounts reported to the Conference of Mayors.

For example, the Conference of Mayors surveyed its membership asking them to report, "What are you spending extra per week?" However, according to a Conference of Mayors' official, members were not provided guidance on how to develop their costs. Thus, localities could have used different methodologies potentially resulting in the inclusion of certain costs in one locality's estimate that may not be included in another locality's estimate. Additionally, only 145 cities out of the U.S. Conference of Mayors total membership of 1,185 responded to the survey, representing a 12 percent response rate. The scope for this study was also somewhat limited in that the U.S. Conference of Mayors issued its report and estimates prior to the conclusion of the March 17 to April 16, 2003, code-orange alert period. Thus, the estimate may not represent all costs incurred during that time period. Finally, the U.S. Conference of Mayors' staff did not take any additional steps to verify the validity of the estimates provided in response to its survey nor did they request that localities provide information to assist them in corroborating the localities' responses.

Similarly, a December 21, 2003, news release[40] from the Center for Strategic and International Studies cited remarks by one of its directors who

[39]U.S. Conference of Mayors, "Survey On Cities' Direct Homeland Security Cost Increases Related to War/High Threat Alert," Mar. 27, 2003.

[40]Center for Strategic and International Studies, *Orange Threat Alert: Cost, Burden of Raising Level Signals Serious Concern by Administration* (Washington, D.C.: Dec. 21, 2003).

independently estimated that it costs the nation $1 billion a week to implement protective measures in response to a code-orange alert. According to the official that generated this estimate, it was an informal calculation based primarily on the funds appropriated by Congress to federal agencies for Operation Liberty Shield. The director divided the total amount of federal appropriations related to Operation Liberty Shield by the number of weeks that Operation Liberty Shield lasted. However, appropriated funds are not accurate representations of expenditures or costs incurred by federal agencies. Additionally, Operational Liberty Shield was a comprehensive national plan to increase protection for America's citizens and the nation's infrastructure during the war with Iraq. Thus, federal agencies may have taken additional protective measures in relation to the war that are not normally associated with code-orange alerts. As a result, this estimate may not be an accurate reflection of costs incurred by federal agencies in relation to other code-orange alerts.

Conclusions

DHS's implementation of the Homeland Security Advisory System is evolving, and the responses to our questionnaires from federal agencies and states suggest that DHS has made progress in providing more specific information to federal agencies and states and localities regarding the specific threats and risks they may face. However, DHS has not yet officially documented its protocols for communicating changes in the national threat level, as well as guidance and threat information, to federal agencies and states. The responses we received to our questionnaires indicated continuing confusion on the part of federal agencies and states and localities regarding the process and methods that DHS uses to communicate changes in the national threat level or recommendations for heightened security measures in specific regions or sectors. Without clearly defined and consistently applied communication policies and procedures, DHS may have difficulty managing the communication expectations of federal agencies and states and effectively communicating the methods, timing, and content of guidance and information—including information on protective measures and potential threats—the department provides to federal agencies and states. We believe that risk communication principles are applicable to the Homeland Security Advisory System and should be applied in DHS communications with federal agencies, states, and localities. Risk communication experts suggest that warnings should include the following principles to provide for early, open, and comprehensive information dissemination and for informed decision making: (1) communication through multiple methods, (2) timely notification, and (3) specific information about the nature, location, and

timing of the threat and guidance on actions to take. To the extent that DHS does not communicate specific threat information and guidance on actions to take, federal agencies, states, and localities may not be able to effectively determine their levels of risk, the appropriate protective measures to implement in response to threats, and how to effectively and efficiently focus their limited resources on implementing those appropriate protective measures. Finally, it is important to note that although periods of code-orange alert do result in some additional costs for many federal agencies, states, and localities, the available cost data have many limitations, are not precise or complete, and thus, any conclusions based on these data must reflect those limitations.

Recommendations for Executive Action

We recommend that the Secretary of Homeland Security direct the Under Secretary for Information Analysis and Infrastructure Protection to take the following two actions: (1) document communication protocols for notifying federal agencies and states of changes in the national threat level and for providing guidance and threat information to these entities, including methods and time periods for sharing information, to better manage these entities' expectations regarding the methods, timing, and content of information shared; 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, including, to the extent possible, information on the nature, location, and time periods of threats and guidance on protective measures to take in response to those threats.

Agency Comments

We provided a draft copy of this report to DHS for comment. DHS generally concurred with the findings and recommendations in the report and provided formal written comments, which are presented in appendix IX. In commenting on the draft report, DHS expressed concern that we generalize examples cited in the report across all states and localities, rather than characterizing the examples as isolated experiences. As previously discussed, we surveyed 56 states and territories to obtain information on their experiences related to national threat level changes. We discuss the results of this questionnaire throughout the report, including information on the number of states that provided similar responses. After citing the number of states that provide a similar response related to a code-orange alert issue, we frequently use examples to illustrate those perspectives. We did not cite all examples we received, but rather those that most effectively

illustrate our message. Thus, we believe the report accurately portrays state perspectives on code-orange alerts. In regard to DHS's comments on the examples we discuss related to localities, we believe that we appropriately cautioned the reader in the report's introduction and scope and methodology sections that information from the 16 localities we visited or from which we received questionnaire responses were used only as anecdotal examples and cannot be generalized across all localities in the United States. DHS also provided technical comments, which we have incorporated as appropriate.

We plan no further distribution of this report until 14 days after the date of this report. At that time, we will send copies of this report to the Subcommittee on Terrorism, Technology, and Homeland Security, Senate Committee on the Judiciary; the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform; the Secretary of Homeland Security; the Director, Office of Management and Budget; and other interested parties. Copies will be made available to others on request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at (202) 512-8777 or by e-mail at jenkinswo@gao.gov. Other GAO contacts and key contributors are listed in appendix X.

William O. Jenkins, Jr.
Director, Homeland Security and Justice Issues

Federal Agencies', States', Localities', and Foreign Countries' Threat Advisory Systems

Some federal agencies, states, localities, and foreign countries had threat advisory systems in place prior to the implementation of the Homeland Security Advisory System in March 2002, while others have since developed such systems. Some of these advisory systems were generally similar to the Homeland Security Advisory System, identifying different threat levels and requiring or suggesting certain protective actions be taken at each threat level. However, other systems differed in terms of structural and operational characteristics—such as the number of threat levels, the issuance of local or regional alerts, and the dissemination of threat advisories to the public.

Federal Agencies' Threat Advisory Systems

Seven of the 25 federal agencies[1] responding to our questionnaire reported that they operated their own threat advisory systems prior to the establishment of the Homeland Security Advisory System in March 2002. One agency, for example, indicated that it developed its own five-level alert system 8 years ago to ensure protection of critical national security assets. These seven agencies currently follow the Homeland Security Advisory System as well as their own agency advisory system that conforms to the Homeland Security Advisory System. Three of these agencies also reported they could independently raise agency threat levels in response to threats or events that specifically affect their operations, regardless of whether the national threat level is raised at the same time. However, they generally cannot lower a facility threat level below that specified by the agency head or other designated agency authority. Further, although these agencies can operate at a threat level that is higher than the Homeland Security Advisory System national threat level (e.g., at code-orange when the national threat level is code-yellow), they generally cannot operate at a lower threat level.

Unlike federal civilian agencies, Department of Defense (DOD) military installations are exempt from following the Homeland Security Advisory System. Accordingly, DOD operates under its own terrorist threat advisory system—known as the Force Protection Condition system. According to DOD officials, this system has five threat conditions—normal, alpha, bravo, charlie, delta—indicating increasing threats of a terrorist attack, and the system prescribes mandatory minimum protective measures for all units and installations for each condition level. Each of the nine DOD Unified

[1]DHS was not formally established until March 1, 2003. Thus, we did not include DHS in our analysis of federal agencies with threat advisory systems in place prior to the creation of the Homeland Security Advisory System.

Combatant Commands[2]—for example, Central Command (Middle East and Asia)—establishes a force protection condition for the entire Command, based on a variety of information including threat and vulnerability assessments from such sources as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Defense Intelligence Agency. Beyond this level of protection, installation and unit commanders may then require additional protective measures, also based on intelligence assessments. This system, therefore, provides flexibility to base commanders to set protective measures based on local threat conditions. In contrast to civilian federal agencies, changes in the Homeland Security Advisory System do not necessarily result in changes in DOD's force protection condition. When the national threat level is raised to code-orange, DOD reviews and analyzes the same intelligence used by DHS to decide to raise the national threat level. Based on this analysis, DOD military commanders then decide whether any change is warranted in their own force protection condition.

States' and Localities' Threat Advisory Systems

As discussed earlier in the report, the Homeland Security Advisory System is not binding on states or localities and they are not required to conform their advisory systems to the Homeland Security Advisory System. However, 42 of the 43 states responding to our questionnaire[3] indicated they currently followed the Homeland Security Advisory System, an equivalent state system, or both.

Eight of the states responding to our questionnaire and 1 locality we visited indicated that they had implemented their threat advisory systems prior to the Homeland Security Advisory System. For example, 1 state told us that it amended its state emergency response plan and implemented a state

[2]Operational control of U.S. combat forces is assigned to the nation's Unified Combatant Commands. A Unified Combatant Command is composed of forces from two or more military services, has a broad and continuing mission, and is normally organized on a geographical basis. There are currently nine Unified Combatant Commands.

[3]One state did not respond to our questions about whether it currently followed the Homeland Security Advisory System or its own state advisory system, or whether it had established a state advisory system prior to the Homeland Security Advisory System. We contacted this state and determined that it currently follows the Homeland Security Advisory System, as well as its own state system that does not conform to the Homeland Security Advisory System and was implemented prior to the Homeland Security Advisory System. Therefore, this state is included in our analysis of the questionnaire responses in this section.

advisory system in 1998, in response to the bombing of the federal building in Oklahoma City.

Twenty-two states responding to our questionnaire and 5 localities we visited indicated that they currently operate their own advisory systems. Most of these states reported that their systems provided information about the type or location of the threat, notified other governmental entities, and identified protective measures to be taken—while most localities indicated their systems conformed to the Homeland Security Advisory System. Some state and local advisory systems are similar to the Homeland Security Advisory System, but contain a different number of threat levels than the Homeland Security Advisory System. For example:

- One state uses a numbered, 4-level threat advisory system, which is similar to the Homeland Security Advisory System but combines the levels of Blue and Yellow into a single threat level.

- One locality uses a 4-level advisory system, which does not include the Homeland Security Advisory System Blue threat level.

State and local advisory systems typically identified actions or protective measures that were to be taken at each threat level. For example, one state advisory system identified state, county, and local government actions, as well as specific security recommendations; while another identified actions for law enforcement agencies, non-law enforcement agencies, businesses, and citizens. One locality advisory system identified general security recommendations, as well as specific agency action checklists identifying a minimum level of response by agencies and departments within the locality. Some states and localities can raise their systems' threat levels based on specific threats or events independent of changes in the national threat level. One state, for example, raised its state threat level in early February 2003 (prior to the February 2003 code-orange alert) in response to the crash of the space shuttle Columbia. One locality could change its threat level locally based on information and coordination with the local FBI office, the state's department of public safety, and the locality's police department.

Foreign Countries' Systems

The United Kingdom has a developed threat advisory system and processes for communicating threat information that are similar to the Homeland Security Advisory System but, unlike the U.S. system, it does not require that terrorism threat alerts be issued to the public. According to United

Kingdom officials, under the United Kingdom's threat advisory system, (1) threat levels are assigned nationwide, as well as to specific regions and economic sectors; and (2) these levels and related changes are communicated to government and law enforcement agencies and private sector entities with responsibility for critical infrastructure protection, but not to the public. The United Kingdom does not publicly announce these threat warnings because it wants to protect its intelligence sources and avoid alerting terrorists that the government is aware of the threat. If terrorists know that the government is aware of their planned attack, the terrorists may change their plans and modes of operation, allowing them to carry out attacks that are even more lethal. Additionally, the United Kingdom is concerned about causing public anxiety regarding possible threats, when, in most cases, the public cannot do anything to mitigate the threat.

However, United Kingdom officials noted that if warnings are necessary to protect public safety from specific and credible threats, the United Kingdom will issue public warnings. Additionally, the United Kingdom instituted a public campaign to encourage public vigilance regarding potential terrorist activity. The campaign included posters warning the public to alert the police to unattended baggage, as shown in figure 1.

Figure 1: London Metropolitan Police Antiterror Alert Poster

Source: Directorate of Public Affairs and Internal Communications, Publicity Branch, Metropolitan Police, London, England.

Unlike the United Kingdom system, the Australian threat advisory system places a greater emphasis on publicizing changes in national threat levels. Australia implemented its current four-level, national counter-terrorist threat alert system in June 2003.[4] As in the United States, a threat level condition is publicly announced and defined. Under the Australian system, each level of alert is defined as follows:

- Low—no information to suggest a terrorist attack in Australia.
- Medium—medium risk of a terrorist attack in Australia.

[4]This four-level system replaced a three-level system that had been in use since 1978.

- High—high risk of a terrorist attack in Australia.

- Extreme—terrorist attack is imminent or has occurred.

According to the Australian Attorney-General's Department, the system was not introduced as a reaction to any particular threat, but rather as an arrangement to help inform national preparation and planning and provide greater flexibility for responding to threats. Accordingly, should any intelligence information come to light which causes the government to change the assessed level of threat, the public is to be advised immediately.

Conversely, Norway does not have a nationwide threat advisory system. According to Norwegian officials, the Norwegian Police Security Service conducts threat assessments—which are graded into levels of low, medium, and high—and these are issued to government agencies with responsibilities for preventing and responding to threats within their jurisdictions. Unlike the Homeland Security Advisory System, there are no routines in place for communicating these threat assessments directly to local governments, private sector entities or the general public, but a decision to do so can be made depending on the situation. National government agencies and county governors can be instructed to take action to address various types of emergencies. However, municipalities, private sector entities, and the general public cannot be instructed to take specific action, except in situations where such instructions are warranted by law.

Like Norway, Germany does not have a uniform nationwide system of threat levels or requirements that specific actions be taken by governmental entities in response to different types of emergencies, including terror attacks. However, Germany does have a single, central 24-hour communication center. For natural disasters and other threats, this center collects, screens, and processes the incoming information for subsequent forwarding to other government agencies regarding actions to take. According to German officials, the central communication center is concerned primarily with information management, rather than with controlling and warning functions. After receiving the threat assessments from the central communication center, governmental entities at the German federal and state level are each responsible for deciding which measures are to be taken, based on the threat.

According to German officials, threat information is communicated to affected persons, individual institutions, the business community, and the

general public by law enforcement agencies, the state governments or the German federal government, according to the nature of the threat or danger concerned and the underlying situation. For example, the federal Criminal Police Office informs the business community on a regular basis as to the current assessment of the situation regarding Islamic terrorism.

Additionally, Germany has a satellite-based warning system that enables official warnings to be broadcast to the public. Government agencies and emergency situation centers are linked via satellite and are able to relay warnings and information on prevailing dangers to the connected media in a matter of seconds.

Scope and Methodology

To determine the process that the Department of Homeland Security (DHS) used to make decisions about changes in the national threat level, we met with and obtained information from DHS officials. We examined this information to identify DHS's processes for determining whether to raise or lower the national threat level and for issuing threat products to federal agencies, states, localities, and private sector entities. We also analyzed DHS threat products to determine the type of threat information and guidance on protective measures that DHS included in the products.

To determine guidance and information provided to federal agencies, states, and localities; protective measures these entities implemented in response to the three code-orange alerts from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004; and additional costs these entities reported for the code-orange alert periods, we sent questionnaires to (1) 28 federal agencies;[1] and (2) the homeland security or emergency management offices in the 50 states, the District of Columbia, American Samoa, Guam, the Northern Islands, Puerto Rico, and the U.S. Virgin Islands. We selected the 28 federal agencies because they reported receiving homeland security funding for fiscal year 2003 to the Office of Management and Budget (OMB) and are Chief Financial Officers Act agencies. We sent the questionnaire to the 25 federal agencies that reported homeland security funding for fiscal year 2003 to OMB and to 3 other federal agencies that are Chief Financial Officers Act agencies but did not report homeland security funding for fiscal year 2003.[2]

To develop the questionnaires, we met with and obtained information from 8 federal agencies, 4 states, the District of Columbia, and 9 localities. Overall, the questionnaires sent to federal agencies and states were very similar. We obtained comments on draft versions of the federal questionnaire from the 8 federal agencies. We adapted the final version of the federal questionnaire to create the state questionnaire. We pretested

[1]We sent DHS a modified version of the questionnaire we sent to the other 27 federal agencies.We sent DHS a modified questionnaire because some of the questions included in the questionnaire sent to the other 27 federal agencies did not apply to DHS. For example, we asked the other federal agencies to indicate the methods by which they received notification of changes in the national threat level from DHS.

[2]We sent the questionnaire to all Chief Financial Officers Act agencies except DOD. Although DOD is a Chief Financial Officers Act agency and, along with the Army Corps of Engineers-Civil Works, reported homeland security funding for fiscal year 2003, we did not send the questionnaire to these agencies because these agencies and their component entities do not follow the Homeland Security Advisory System.

the questionnaires with 4 federal agencies and 3 states and made relevant changes to the questions based on these pretests. See appendixes VII and VIII for the federal and state questionnaires.

As of April 20, 2004, we received questionnaire responses from 26 federal agencies,[3] which account for about 99 percent of total fiscal year 2003 nondefense homeland security funding as reported to OMB, and 43 states,[4] for a 77 percent response rate. We made extensive efforts to encourage federal agencies and states to complete and return the questionnaires, such as contacting all nonrespondents on multiple occasions and sending additional copies of questionnaires when requested. We performed this work from October 2003 through May 2004.

Because our surveys were not statistical sample surveys, but rather a survey of a nonprobability selection of federal agencies and a census of all states, there are no sampling errors. However, the practical difficulties of conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, measurement errors are introduced if difficulties exist in how a particular question is interpreted or in the sources of information available to respondents in answering a question. In addition, coding errors may occur if mistakes are entered into a database. We took extensive steps in the development of the questionnaires, the collection of data, and the editing and analysis of data to minimize total survey error. As noted above, to reduce measurement error and ensure questions and response categories were interpreted in a consistent manner, we pretested the questionnaires with several federal agencies and states.

[3]See appendix VI for a list of federal agencies that responded to our questionnaire. We did not receive questionnaire responses from 2 federal agencies in time to include their responses in the report. The 2 federal agencies were the Office of Personnel Management and U.S. Agency for International Development. Of the other 26 federal agencies, 24 provided one questionnaire response for the entire agency. The Department of Justice and DHS provided questionnaire responses for their component entities. For these 2 agencies, we consolidated their component entities' responses into one response for the entire agency. In most cases, we did this by identifying the responses most often selected by the component entities.

[4]We did not receive questionnaire responses from 13 states in time to include their responses in the report. The 13 states were California, Colorado, the District of Columbia, Hawaii, Indiana, Maryland, Neveda, Oregon, Rhode Island, Virginia, American Samoa, Northern Mariana Islands, and the U.S. Virgin Islands. One state for which we received a questionnaire response indicated that it did not follow the Homeland Security Advisory System. We analyzed questionnaire responses for the other 42 states that indicated following the Homeland Security Advivory System.

We edited all completed surveys for consistency, such as ensuring that responses were provided for all appropriate questions, and, if necessary, contacted respondents to clarify responses. All questionnaire responses were double key-entered into our database (i.e., the entries were 100 percent verified), and random samples of the questionnaires were further verified for completeness and accuracy of data entry. Furthermore, all computer syntax was peer reviewed and verified by separate staff to ensure that the syntax was written and executed correctly.

In addition to sending questionnaires to 28 federal agencies and 56 states, we conducted site visits at 12 localities (eight cities and four counties) and sent a questionnaire to another 8 localities. The 12 localities were Atlanta and Fulton County, Georgia; Denver, Colorado Springs, and Douglas County, Colorado; Norfolk, Virginia; Portland and Wasco County, Oregon; Chicago and Cook County, Illinois; and Boston and Fitchburg, Massachusetts. We selected these localities based on the following criteria: the locality's receipt of urban area grants[5] from DHS, geographic location, topography (e.g., inland, border, or seaport), and type of locality (e.g., metropolitan or nonmetropolitan area). We selected four cities and one county that received grants from DHS and four cities and three counties that did not. We also selected cities and counties from different geographic regions and with different topographic characteristics, as well as some cities and counties located in metropolitan areas and some cities and counties located in nonmetropolitan areas. We used a structured data collection instrument to interview emergency management officials and first responders in these localities. We selected the 8 localities that we surveyed based on their populations and geographic locations. We received responses from 4 of these localities;[6] 3 with populations of less than 40,000 – Helena, Montana; Mankato, Minnesota; and Rock Springs, Wyoming – and 1 with a population of greater than 40,000 – San Jose, California.

To determine the extent to which risk communication principles could be incorporated into the Homeland Security Advisory System, we spoke with and obtained information from individuals and organizations with expertise in homeland security issues and risk communication. We analyzed reports and documents from the ANSER Institute for Homeland

[5]The Urban Areas Security Initiative grants are awarded based on a combination of current threat estimates, critical assets within the urban area, and population density.

[6]We did not receive responses from Miami/Dade County, Florida; Seattle, Washington; Jamestown, North Dakota; and New York City, New York.

Security, Carnegie Mellon University, the Center for Strategic and International Studies, the Department of Health and Human Services, the Harvard Center for Risk Analysis, the Oak Ridge National Laboratory, and the Partnership for Public Warning.

To assess the reliability of cost data provided by federal agencies on our questionnaire, we examined the cost information for obvious errors and inconsistencies and examined responses to the questionnaire items requesting information regarding the development of the cost data. If necessary, we contacted respondents to clarify responses and, when provided, reviewed documentation about the cost data. Federal agencies generated their cost data from various sources such as their financial accounting systems, credit card logs, and security services contracts. This cost information is not precise, nor do the costs likely represent all additional costs for the code-orange alert periods. In some cases, we have concerns about the reliability of the cost data source within particular agencies. For example, 6 of the 16 federal agencies reported that they extracted some of the code-orange alert cost data from their agencies' financial accounting systems. As reported in the fiscal year 2005 President's Budget, 5 of these agencies' financial management performance had serious flaws as of December 31, 2003. Despite these limitations, we believe the cost data to be sufficiently reliable as indicators of general ranges of cost and overall trends. However, the data should not be used to determine the cumulative costs for all federal agencies for code-orange alert periods. See appendix V for additional information on cost information reported by federal agencies.

To determine the extent to which DHS has collected information on costs reported by states and localities during periods of code-orange alert, we met with and obtained information from DHS officials on costs that states and their localities submitted to DHS for reimbursement for increased critical infrastructure asset protection during the three code-orange alert periods. We examined this information to identify the methods used by DHS to collect cost information from states and localities. We also met with and obtained information from representatives of OMB regarding the extent to which the office provided guidance to DHS for collecting cost information from states and localities.

We reported these cost data that DHS collected from states and localities for the three code-orange alert periods only to illustrate the range of costs that states reported to DHS for reimbursement. Cost information submitted by states to DHS does not include all costs for states and localities during

the code-orange alert periods. In particular, not all states submitted costs to DHS for reimbursement, and not all state agencies and localities in states that submitted cost information to DHS may have reported costs to their states for submission to DHS. In addition, the cost information submitted by states does not include additional costs for training or equipment and material purchases during code-orange alert periods because these costs are not reimbursable through the critical infrastructure protection grant programs. Moreover, some states have not finished validating costs they plan to submit for reimbursement. Despite these limitations, we believe the cost data to be sufficiently reliable as indicators of general ranges of costs that states submitted for reimbursement to DHS and overall trends. However, because this cost information from states and localities is not complete, it should not be used to reach conclusions about the financial impact of code-orange alerts on states and localities.

To determine the methodologies used by other organizations to develop estimates of costs reported by federal agencies, states, and localities during code-orange alert periods, we spoke with and obtained information from officials at the U.S. Conference of Mayors and the Director of the Center for Strategic and International Studies Homeland Security Initiatives regarding how this organization and this individual developed their estimates. We evaluated methodologies used by the U.S. Conference of Mayors and the Director of the Center for Strategic and International Studies Homeland Security Initiatives based on their scopes, data collection methods, and analyses to assess the reliability of the cost estimates. Moreover, we examined costs estimates reported by other organizations, including the Council on Foreign Relations, the National League of Cities, the National Association of Counties, and the International Association of Emergency Managers. We did not include these organizations' reports in our review because they did not specifically address costs associated with responses to increases in the national threat level.

To obtain information on federal agencies', states', and localities' threat advisory systems, we analyzed questionnaire responses and other documents to determine the number of federal agencies, states, and localities that had their own threat advisory systems in place prior to the establishment of the Homeland Security Advisory System as well as the number of federal agencies, states, and localities that follow their own threat advisory systems and the Homeland Security Advisory System. We reviewed documentation of the threat advisory systems that these federal agencies, states, and localities provided with their questionnaire responses to identify the characteristics of the systems, including systems' threat

levels and protective measures and conformance to the Homeland Security Advisory System. We also met with and received documents from the Department of Defense on its Force Protection Condition System. Furthermore, we spoke with and obtained information from officials of four foreign countries—Australia, Germany, Norway, and the United Kingdom—on these countries' threat advisory systems and information sharing processes.[7] We compared the characteristics of these systems with characteristics of the Homeland Security Advisory System to identify similarities and differences between the systems. We selected the four countries because they are democracies similar to the United States that have generally faced terrorist threats.

We conducted our work from July 2003 to May 2004 in accordance with generally accepted government auditing standards

[7]We also contacted officials from France and Israel, but did not receive information from these officials in sufficient time to include the information in the report.

Guidance and Information Federal Agencies and States Reported Using to Determine Protective Measures

Federal agencies and states responding to our questionnaire indicated that they used guidance from various sources, such as the Federal Emergency Management Agency (FEMA), the Federal Protective Service (FPS), the Department of Justice, and the White House, among other sources, to develop plans for responding to each Homeland Security Advisory System threat level. For example, 12 federal agencies reported using the Department of Justice's *Vulnerability Assessment of Federal Facilities*[1] that established security levels for various types of federal facilities and minimum-security standards for each security level. In addition, to develop their response plans, 8 federal agencies indicated that they used Homeland Security Presidential Directive 3, which established the Homeland Security Advisory System and suggested general protective measures for each advisory system threat level. Six states reported using terrorism alerts and guidelines from FEMA to develop their plans for protective measures for national threat levels.

In addition to their response plans for national threat levels, federal agencies and states responding to our questionnaires reported using guidance and information from various sources to determine protective measures to implement or enhance in response to the three code-orange alert periods from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004. As shown in tables 6 and 7, these federal agencies reported using guidance and information and intelligence from such sources as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the White House to determine measures to take in response to the third code-orange alert period in our review. These federal agencies generally reported that this guidance and information and intelligence was useful and timely. Results for the other two code-orange alert periods – March 17 to April 16, 2003; and May 20 to 30, 2003 – were consistent with those reported in tables 6 and 7 for the third code-orange alert period.

[1]Department of Justice, *Vunerability Assessment of Federal Facilities* (Washington, D.C.: June 28, 1995). The Department of Justice developed the assessment in consultation with the General Services Administration, the Department of Defense, the Secret Service, the Department of State, the Social Security Administration, and the Administrative Office of the U.S. Courts.

Table 6: Number of Federal Agencies That Used Guidance from Sources and Found It Useful and Timely for the Code-Orange Alert Period December 21, 2003, to January 9, 2004

	Number of federal agencies n = 26		
Source of guidance	Number that reported using guidance	Number that reported that the guidance was useful[a]	Number that reported that the guidance was timely[b]
DHS[c]	16	14	11
FBI	9	9	9
White House	6	5	5
Local law enforcement	3	3	3

Source: GAO analysis of questionnaire data.

[a]We asked federal agencies to indicate whether the guidance they received was very useful, somewhat useful, or of little or nor use. Useful reflects respondents' ratings of very useful and somewhat useful.

[b]We also asked agencies to indicate whether the guidance they received was timely by responding yes or no.

[c]In the questionnaire we sent to DHS, we did not include DHS as a choice for guidance used to determine protective measures to take during the three code-orange alert periods.

Table 7: Number of Federal Agencies That Used Information and Intelligence from Sources and Found It Useful and Timely for the Code-Orange Alert Period December 21, 2003, to January 9, 2004

	Number of federal agencies n = 26		
Source of information/intelligence	Number that reported using information and intelligence	Number that reported that the information and intelligence was useful[a]	Number that reported that the information and intelligence was timely[b]
DHS[c]	16	14	14
FBI	17	16	15
White House	8	7	7
Local law enforcement	7	7	6
National Joint Terrorism Task Force[d]	11	11	10
Agency intelligence sources	9	9	8

Source: GAO analysis of questionnaire data.

[a]We asked federal agencies to indicate whether the information and intelligence they received was very useful, somewhat useful, or of little or nor use. Useful reflects respondents' ratings of very useful and somewhat useful.

[b]We also asked agencies to indicate whether the information and intelligence they received was timely by responding yes or no.

[c]In the questionnaire we sent to DHS, we did not include DHS as a choice for information and intelligence used to determine protective measures to take during the three code-orange alert periods.

[d]The task force is comprised of numerous federal agencies co-located in the Strategic Information and Operations Center at FBI headquarters. This task force provides a central fusion point for terrorism information and intelligence to the Joint Terrorism Task Forces, which include state and local law enforcement officers, federal agents, and other federal personnel who work in the field to prevent and investigate acts of terrorism.

As shown in tables 8 and 9, states responding to our questionnaire also indicated that they used guidance and information from sources such as DHS, other federal entities, and state, territory, and local law enforcement agencies to determine actions to take in response to the third code-orange alert period. These states generally reported that this guidance and information and intelligence was useful and timely. Results for the other two code-orange alert periods in our review were similar to those reported in tables 8 and 9.

Table 8: Number of States That Used Guidance from Sources and Found It Useful and Timely for the Code-Orange Alert Period December 21, 2003, to January 9, 2004

	Number of states n = 41[a]		
Source of guidance	Number that reported using guidance	Number that reported that guidance was useful[b]	Number that reported that guidance was timely[c]
DHS	34	30	29
Other federal entity, such as the FBI	30	27	28
Other state, territory, or local government agency	15	15	15
Regional, state, or local law enforcement agencies	19	18	18
Governor or legislature	20	20	20
Private sector organizations	10	9	10

Source: GAO analysis of questionnaire data.

[a]One of the states responding to our questionnaire did not provide responses to the questions on guidance and information and intelligence used to determine protective measures to take for the three code-orange alert periods. Additionally, 1 reported that it did not follow the Homeland Security Advisory System. Thus, these 2 states are not included in our analysis of guidance and information and intelligence used to determine protective measures.

[b]We asked states to indicate whether the guidance they received was very useful, somewhat useful, or of little or nor use. Useful reflects respondents' ratings of very useful and somewhat useful.

[c]We also asked states to indicate whether the guidance they received was timely by responding yes or no.

Table 9: Number of States That Used Information and Intelligence from Sources and Found It Useful and Timely for the Code-Orange Alert Period December 21, 2003, to January 9, 2004

	Number of states n = 41[a]		
Source of information/intelligence	Number that reported using information and intelligence	Number that reported that information and intelligence was useful[b]	Number that reported that information and intelligence was timely[c]
DHS	32	29	27
Other federal entity, such as the FBI	30	28	27
Other state, territory, or local government agency	14	14	14
Regional, state, or local law enforcement agencies	21	20	19
Governor or legislature	11	11	11
Private sector organizations	10	10	10

Source: GAO analysis of questionnaire data.

[a]One of the states responding to our questionnaire did not provide responses to the questions on guidance and information and intelligence used to determine protective measures to take for the three code-orange alert periods. Additionally, 1 state reported that it did not follow the Homeland Security Advisory System. Thus, these 2 states are not included in our analysis of guidance and information and intelligence used to determine protective measures.

[b]We asked states to indicate whether the information and intelligence they received was very useful, somewhat useful, or of little or nor use. Useful reflects respondents' ratings of very useful and somewhat useful.

[c]We also asked states to indicate whether the information and intelligence they received was timely by responding yes or no.

Most Commonly Implemented Protective Measures, Measures Tested, and Methods of Confirmation

Federal agencies and states responding to our questionnaires reported having a variety of protective measures in place for responding to the three code-orange alert periods from March 17 to April 16, 2003; May 20 to 30, 2003; and December 21, 2003, to January 9, 2004, regardless of whether the measures were most commonly enhanced, maintained at pre-code-orange alert levels, or implemented solely in response to the code-orange alerts. Table 10 provides examples of the protective measures that federal agencies most commonly reported having in place for the third code-orange alert period in our review. Results from the other two code-orange alert periods are consistent with those reported in the following table for the third code-orange alert period.

Table 10: Protective Measures Most Commonly Reported by Federal Agencies Responding to Our Questionnaire for the December 21, 2003, to January 9, 2004, Code-Orange Alert Period

	Number of federal agencies n = 24[a]			
Protective measures	Number that reported measure	Number that indicated no change in measure that was already in place[b]	Number that enhanced measure that was already in place[c]	Number that implemented measure for code-orange only[d]
Implement facility patrols	24	3	21	0
Activate monitoring systems	24	16	8	0
Screen mail and deliveries	24	12	12	0
Screen facility visitors	23	12	11	0
Activate instrusion detection systems	23	19	4	0
Escort facility visitors	22	10	9	3
Ensure that response procedures and plans are up to date	21	4	17	0
Conduct emergency response drills and/or training	20	10	10	0

Source: GAO analysis of questionnaire data.

[a]One federal agency responding to our questionnaire reported that it does not implement protective measures because it is located in a privately owned building and is not responsible for its own security. Another federal agency did not provide a response to questions related to the protective measures taken during code-orange alerts due to security concerns. Thus, these 2 federal agencies are not included in our analysis of protective measures.

[b]No change in a protective measure indicates that the measure was already in place prior to the code-orange alert period and continued at the same level of use or frequency during a code-orange alert.

[c]The enhancement of a measure that was already in place refers to the increased use of an existing protective measure, such as more frequent facility security patrols or increased volume of mail screened.

[d]The implementation of a measure for code-orange only refers to the use of an additional measure that was not already in place solely to respond to a code-orange alert.

Table 11 provides examples of the protective measures that states most commonly reported having in place during the third code-orange alert period in our review. Results for the other two code-orange alert periods in our review are similar to those reported in table 11.

Table 11: Protective Measures Most Commonly Reported by States Responding to Our Questionnaire for the December 21, 2003, to January 9, 2004, Code-Orange Alert Period

	Number of states n = 40[a]			
Protective measures	Number that reported measure	Number that indicated no change in measure that was already in place[b]	Number that enhanced measure that was already in place[c]	Number that implemented measure for code-orange only[d]
Alert other state, territorial, local and private sector counterparts	38	4	21	13
Ensure response and communication plans are up to date	36	12	21	3
Issue recommendations or guidance for protective measures	35	2	25	8
Implement facility security patrols	34	3	26	5
Place vehicle barriers around facilities	31	8	17	6
Prepare for possible biological, chemical, or radiological attacks	30	16	13	1
Screen mail and deliveries	30	19	9	2
Restrict parking near facilities	30	5	16	9
Limit number of facility access points	30	11	14	5

Source: GAO analysis of questionnaire data.

[a]Two states responding to our questionnaire did not provide responses on protective measures they had in place for the three periods of code-orange alert. Additionally, 1 state reported that it did not follow the Homeland Security Advisory System. Thus, these 3 states are not included in our analysis on protective measures.

[b]No change in a protective measure indicates that the measure was already in place prior to the code-orange alert period and continued at the same level of use or frequency during a code-orange alert.

[c]The enhancement of a measure that was already in place refers to the increased use of an existing protective measure, such as more frequent facility security patrols or increased volume of mail screened.

[d]The implementation of a measure for code-orange only refers to the use of an additional measure that was not already in place solely to respond to a code-orange alert.

To ensure that protective measures operate as intended and are implemented as planned, most of the federal agencies and states responding to our questionnaires indicated that they had conducted tests or exercises on the functionality and reliability of protective measures within the past year. Table 12 provides examples of protective measures on which federal agencies and states reported conducting tests and exercises.

Table 12: Number of Federal Agencies and States That Reported Conducting Tests or Exercises on the Functionality and Reliability of Protective Measures

Protective measures	Number of federal agencies that reported testing protective measure n = 25[a]	Number of states that reported testing protective measure n = 37[b]
Intrusion detection systems	25	14
Visitor and employee screening equipment and procedures	24	22
Vehicle inspection equipment and procedures	24	23
Baggage and cargo screening equipment and procedures	16	14
Mail and delivery screening procedures	25	23
Monitoring systems, such as surveillance cameras	25	24
Continuity of operations measures	25	21
Emergency response measures	25	32

Source: GAO analysis of questionnaire data.

[a]One federal agency responding to our questionnaire reported that it does not implement protective measures because it is located in a privately owned building and is not responsible for its own security. Thus, this agency is not included in our analysis of protective measures tested by federal agencies.

[b]Six states responding to our questionnaire did not provide responses on the testing of protective measures they had in place for the three periods of code-orange alert. Thus, these 6 states are not included in our analysis of protective measures tested by states.

In addition, most of the federal agencies and states responding to our questionnaires reported receiving confirmation from component entities, offices, or personnel that protective measures were actually enhanced or implemented during the three code-orange alert periods. Table 13 provides examples of the methods by which federal agencies and states reported receiving confirmation from their component entities, offices, and personnel, for the code-orange alert period from December 21, 2003, to January 9, 2004. Results for the other two code-orange alert periods from March 17 to April 16, 2003, and May 20 to 30, 2003, are consistent with those reported in table 13.

Table 13: Number of Federal Agencies and States That Reported Receiving Confirmation on the Implementation of Protective Measures through Various Methods for the Code-Orange Alert Period from December 21, 2003, to January 9, 2004

Methods of confirmation	Number of federal agencies that reported receiving confirmation n = 25[a]	Number of states that reported receiving confirmation n = 41[b]
Oral notification of protective measures implementation	20	35
Written notification of protective measures implementation	18	23
Inspection of protective measures implementation	22	16

Source: GAO analysis of questionnaire data.

[a]One federal agency responding to our questionnaire reported that it does not implement protective measures because it is located in a privately owned building and is not responsible for its own security. Thus, this agency is not included in our analysis of the confirmation of protective measures.

[b]One state responding to our questionnaire did not provide responses on the receipt of confirmation of the implementation of protective measures. Additionally, 1 state reported that it did not follow the Homeland Security Advisory System. Thus, these 2 states are not included in our analysis of the confirmation of protective measures.

Cost Information Provided by Federal Agencies, States, and Localities

Cost Information Provided by Federal Agencies

Table 14: Number of Federal Agencies That Provided Cost Information and the Type of Cost Information They Provided for Each Code-Orange Alert Period under Review

	Number of federal agencies n = 26		
Cost information	**March 17 to April 16, 2003**	**May 20 to 30, 2003**	**December 21, 2003, to January 9, 2004**
Provided code-orange alert cost information	21	21	21
• Incurred additional costs	16	15	15
• Provided cost estimates	13	13	13
• Provided actual costs	3	2	2
• Provided costs for immediately preceding code-yellow alert period	12	11	11
• Did not incur additional costs	5	6	6
Did not provide code-orange alert cost information	5	5	5

Source: GAO analysis of questionnaire data.

For each code-orange alert period, the federal agencies that reported incurring additional costs generally provided cost estimates. Many of these agencies reported using similar methods to develop their estimates. For example, 8 of these agencies reported using the additional hours accumulated by security personnel during code-orange alerts and the hourly rates of security personnel to develop estimates for additional personnel costs incurred during code-orange alerts. The majority of additional costs reported by federal agencies are personnel costs. One federal agency indicated that it provided cost estimates rather than actual costs for the code-orange alert periods because, given the short durations of the code-orange alerts and the changes required to track these limited costs in the accounting system, it was more efficient to utilize security cost estimates.

Six federal agencies that provided cost information extracted at least some of their cost data from their agencies' financial accounting systems. However, as reported in the fiscal year 2005 President's Budget, 5 of these

agencies' financial management performance had serious flaws as of December 31, 2003. Thus, we have concerns regarding the accuracy of the cost information these 5 agencies provided to us.

Agencies that did not provide cost information indicated that either they did not track additional code-orange alert costs or they did not have the capability to separate additional code-orange alert costs from their total annual security-related costs.

Cost Information Provided by States

In our questionnaire, we asked states to provide information on additional costs incurred by the state during the three code-orange alert periods in our review. However, of the 42 states that responded to our questionnaire and follow the Homeland Security Advisory System, only 6 reported additional costs incurred by state agencies during at least one of the three code-orange alerts in our review. Therefore, we did not collect sufficient cost information from our questionnaire to provide ranges or assess general trends in costs incurred by states during code-orange alert periods.

Twenty-two of the 42 states that responded to our questionnaire and follow the Homeland Security Advisory System provided us with cost information they submitted to DHS in order to be reimbursed for state and local critical infrastructure protection costs through the State Homeland Security Grant Program – Part II and the Urban Areas Security Initiative – Part II. As discussed previously in this report, through these two grant programs, DHS offered financial assistance to reimburse costs incurred by state agencies and localities as a result of increased security measures at critical infrastructure sites during the period of hostilities with Iraq and for other periods of heightened alert. We obtained this critical infrastructure protection cost information from DHS for 40 states and their localities for the March 17 to April 16, 2003, and May 20 to 30, 2003, code-orange alert periods and for 33 states and their localities for the December 21, 2003, to January 9, 2004, code-orange alert period. However, this cost information does not represent all additional costs incurred by states and localities during code-orange alert periods.

Cost Information Provided by Localities

We also received information on additional code-orange alert costs from 14 select metropolitan and rural localities. However, information on localities' costs is most appropriately used anecdotally, as these cities and counties

represent a small, nonprobability sample of localities within the United States.

The rural localities from which we obtained information indicated that they did not incur additional costs for any of the code-orange alert periods because they did not take significant action in response to the alert. These localities explained that they had insufficient resources to do so or did not perceive their localities to be at risk.

Acknowledgment of Agency and Government Contributors

We would like to acknowledge the time and effort made by agencies and governments that provided information by responding to questionnaires and talked with us during site visits.

Federal Agencies

Department of Agriculture
Department of Commerce
Department of Education
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of the Treasury
Department of Veterans Affairs
Corporation for National and Community Service
Environmental Protection Agency
Federal Communications Commission
General Services Administration
National Aeronautics and Space Administration
National Archives and Records Administration
National Science Foundation
Nuclear Regulatory Commission
Small Business Administration
Smithsonian Institution
Social Security Administration
United States Holocaust Memorial Museum

States and Territories

Alabama
Alaska
Arizona
Arkansas
Connecticut
Delaware
Florida
Georgia

Idaho
Illinois
Iowa
Kansas
Kentucky
Louisiana
Maine
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
Nebraska
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota
Ohio
Oklahoma
Pennsylvania
South Carolina
South Dakota
Tennessee
Texas
Utah
Vermont
Washington
West Virginia
Wisconsin
Wyoming
Guam
Puerto Rico

Localities

Atlanta, Ga.
Fulton County, Ga.
Denver, Colo.
Douglas County, Colo.
Colorado Springs, Colo.

Portland, Ore.
Wasco County, Ore.
Boston, Mass.
Fitchburg, Mass.
Norfolk, Va.
Chicago, Ill.
Cook County, Ill.
Mankato, Minn.
Helena, Mont.
San Jose, Calif.
Rock Springs, Wyo.[1]

[1]In addition to the federal agencies listed, we sent questionnaires to the Agency for International Development and the Office of Personnel Management. Also, in addition to the states and territories listed, we sent questionnaires to California, Colorado, the District of Columbia, Hawaii, Indiana, Maryland, Nevada, Oregon, Rhode Island, Virginia, American Samoa, Northern Mariana Islands, and the U.S. Virgin Islands. We also sent questionnaires to Miami/Dade County, Florida; Seattle, Washington; Jamestown, North Dakota; and New York City, New York.

Federal Agency Questionnaire

United States General Accounting Office

Survey of Federal Agencies' Protective Measures, Guidance, and Costs for Elevated Threat Alerts

The U.S. General Accounting Office (GAO) has been requested by Congress to review federal agencies' security-related protective measures, guidance, and costs for periods when the national threat level was raised from yellow (elevated) to orange (high). As part of this request, GAO is surveying 28 federal agencies that received homeland security funding in fiscal year 2003, as reported to the Office of Management and Budget, and/or are Chief Financial Officers Act agencies. Results from this survey will help GAO to inform Congress of (1) protective measures taken by federal agencies during periods of orange alert, specifically for the periods March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004; (2) guidance and other information used by federal agencies in implementing those measures; and (3) costs incurred by federal agencies as a result of protective measures implemented during those three orange alert periods.

This questionnaire should be completed by the person(s) most knowledgeable about your agency's security-related measures, guidance, and costs for the orange alerts from March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004, including your agency's protective measures for threat levels; guidance and other information used by your agency in developing and implementing protective measures during those periods; your agency's methods for tracking or collecting cost data and ensuring data reliability; your agency's national threat level notification processes; and financial and operational challenges your agency faced during the three orange alert periods. **If your agency, or certain of its facilities, remains on orange alert even though the national threat level has been lowered, please answer the questions about the most recent orange alert period considering your agency's actions and costs through January 9, 2004.** Most of the questions can be answered by marking boxes or filling in blanks. Space has been provided at the end of the survey for any additional comments, and we encourage you to provide whatever additional comments you think appropriate. In our report, the responses from your agency will be presented only after they have been aggregated with responses from other responding agencies. GAO will not release individual agency responses to any entity unless requested by Congress or compelled by law. In addition, GAO will take appropriate measures to safeguard any sensitive information provided by your agency, and, upon request, can provide security clearance information for staff reviewing survey responses.

Please complete this questionnaire within 2 weeks of receipt. Your agency's participation is important! A member of our staff will pick up your completed questionnaire. If you have any questions or when you are ready for your questionnaire and any accompanying materials to be picked up, please contact Dr. Jonathan Tumin on (202) 512-3595, Rebecca Gambler on (202) 512-6912, or Kristy Brown on (202) 512-8697.

_____

Please provide the name, title, agency, and telephone number of the primary person completing this questionnaire so that we may contact that person if we need to clarify any responses.

Name: _____

Title: _____

Agency: _____

Telephone number: (_____)_____

We modified the format of this questionnaire slightly for inclusion in this report, but we did not change the content of the questionnaire.

Definition of term "agency": Any entity within the executive branch, including federal departments, independent establishments, and government corporations. If the questionnaire is to be completed by a federal agency's components, then "agency" refers to the component entity rather than the department.

Agency Protective Measures for National Threat Levels

1. According to Homeland Security Presidential Directive 3, issued in March 2002, federal agencies are responsible for developing their own protective measures and other antiterrorism or self-protection and continuity plans for national threat levels. *(See highlighted passage on page 2 of the attachment.)*

   Has your agency developed protective measures for national threat levels? *(Please check only one answer.)*

   1. ❒ Yes, agency modified protective measures developed prior to the directive to conform with national threat levels established in the directive ➡ Please provide a copy of the measures along with your completed questionnaire.

   2. ❒ Yes, agency developed protective measures for national threat levels after issuance of the directive ➡ Please provide a copy of the measures along with your completed questionnaire.

   3. ❒ Agency is in the process of modifying or developing protective measures ➡ Please provide time frames your agency has established for completing the measures:

      _____

      _____

   4. ❒ No, agency has not modified or developed protective measures ➡ Please briefly describe the reasons why your agency has not modified or developed the measures:

      _____

      _____

      _____

      _____

      If you answer #4, please skip to question 5; otherwise, please continue.

2. Did your agency use guidance and/or information from any of the following sources in developing your protective measures for national threat levels? *(Please check one answer in each row.)*

Source	Yes	No	Don't know
a. Federal Emergency Management Agency (FEMA)			
b. Federal Protective Service (FPS)			
c. Department of Defense			
d. Department of Justice			
e. White House			
f. Local law enforcement			
g. Vulnerability assessments for your agency			
h. Other sources *(Please specify.)* _____ _____			

3. ***If you answered "yes" for any source in question 2, please answer:***
Please list the source and titles or topics of any written guidance used by your agency in developing your protective measures for national threat levels.

Source	Title or topic (e.g., how to identify critical infrastructure)
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

4. Within the past year, did your agency (or at least one component) conduct exercises or tests on the functionality and reliability of any of the following protective measures? *(Please check one answer in each row.)*

Protective measure	Yes	No	Don't know	Not applicable
a. Intrusion detection systems				
b. Visitor/employee screening equipment and procedures				
c. Vehicle inspection equipment and procedures				
d. Baggage and/or cargo screening equipment and procedures				
e. Mail and delivery screening procedures				
f. Monitoring systems, such as surveillance cameras				
g. Continuity of operations measures				
h. Emergency response measures				
i. Other measures *(Please specify.)* _____ _____				

5. Homeland Security Presidential Directive 3 requires federal agencies to develop and submit to the President, through the Assistant to the President for Homeland Security, an annual written report on steps taken to develop and implement protective measures for national threat levels. *(See highlighted passage on page 2 of the attachment.)*

   In accordance with this directive, what is the status of your agency's most recent annual report to the President? *(Please check one answer.)*

   1. ❒ Agency has completed and submitted the annual report ➡ Please provide a copy of the report along with your completed questionnaire.

   2. ❒ Agency has completed but not submitted the annual report ➡ Please provide time frames your agency has established for submitting the report, and a copy of the report if possible:

      _____

      _____

      _____

      _____

   3. ❒ Agency is in the process of completing the annual report ➡ Please provide time frames your agency has established for completing and submitting the report:

      _____

      _____

      _____

   4. ❒ Agency has not begun the annual report but intends to do so ➡ Please provide time frames your agency has established for beginning, completing, and submitting the report:

      _____

      _____

      _____

   5. ❒ Agency has not begun the annual report and does not intend to do so ➡ Please briefly describe the reasons why your agency does not intend to prepare and submit an annual report:

      _____

      _____

      _____

      _____

Homeland Security Advisory System

6. Did your agency have its own threat-advisory system for preparing and responding to homeland security threats prior to the establishment of the Homeland Security Advisory System (HSAS) in March 2002? *(Please check only one answer.)*

   1. ❒ Yes, agency had its own threat-advisory system ➡ Please provide the name of your agency's threat-advisory system and a copy of system documentation, if available, along with your completed questionnaire

      _____

   2. ❒ No, agency did not have its own threat-advisory system

7. To what extent, if at all, does your agency follow the Homeland Security Advisory System (HSAS) for preparing and responding to homeland security threats? *(Please check only one answer.)*

   1. ❒ Agency only follows the HSAS

   2. ❒ Agency follows the HSAS and its own threat–advisory system that conforms with the HSAS ➡ Please provide the name of your agency's threat-advisory system and a copy of system documentation, if available, along with your completed questionnaire.

      _____

   3. ❒ Agency follows the HSAS and its own threat–advisory system that does not conform with the HSAS ➡ Please provide the name of your agency's threat-advisory system and a copy of system documentation, if available, along with your completed questionnaire.

      _____

   4. ❒ Agency does not follow the HSAS, but uses its own threat–advisory system ➡ Please provide the name of your agency's threat-advisory system and a copy of system documentation, if available, along with your completed questionnaire.

      _____

   If you answered #4, please stop and return this questionnaire according to the instructions on page 1.

   5. ❒ Agency does not follow the HSAS and does not use its own threat–advisory system, but uses another threat-level system (e.g., the Department of Defense's Force Protection Condition system) ➡ Please provide the name of the other threat-advisory system used by your agency.

      _____

   If you answered #5, please stop and return this questionnaire according to the instructions on page 1.

   6. ❒ Agency does not follow any threat-advisory system

   If you answered #6, please stop and return this questionnaire according to the instructions on page 1.

GAO Survey on Threat Alerts

Types of Protective Measures Used During HSAS Code-Yellow Alerts and Specifically in Response to Code-Orange Alerts from March 17 to April 16, 2003, from May 20 to May 30, 2003, and from December 21, 2003 to January 9, 2004

8. We would like to know the types of protective measures your agency has in place during Code-Yellow alerts and the types of measures used during the Code-Orange alerts from March 17 to April 16, 2003, from May 20 to May 30, 2003, and from December 21, 2003 to January 9, 2004.

8a. Please indicate the protective measures your agency (or at least one component) has in place for Code-Yellow alerts. *(Please check "Yes", "No", or "Not applicable-N/A" for each measure.)*

8b, 8c, and 8d. Please indicate the protective measures your agency (or at least one component) implemented or increased the use of specifically in response to the Code-Orange alerts, that is, measures implemented in addition to the measures used in the preceding Code-Yellow alert period. *(Please check "Implemented, Code-Orange only", "Increased use of", or "N/A or no change in measure" for each measure in each column.)*

	Question 8a	Question 8b	Question 8c	Question 8d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17–April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20–May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003–Jan. 9, 2004**
1. Protection of agency facilities including critical infrastructure), personnel, and systems				
❒ If your agency did not implement any types of measures in category "1", please check this box and skip to category "2".				
a. Implement facility security patrols	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
b. Implement random shift changes for security personnel	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
c. Extend shifts for security personnel	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
d. Inspect visitors and their belongings upon entry	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
e. Inspect employees and their belongings upon entry	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
f. Inspect vehicles entering or parking near facilities	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
g. Restrict parking near facilities	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure

Continued on next page

GAO Survey on Threat Alerts

	Question 8a	Question 8b	Question 8c	Question 8d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17–April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20–May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003–Jan. 9, 2004**
h. Place vehicle barriers around facilities	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
i. Expand security perimeter at facilities	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
j. Limit number of facility access points	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
k. Screen mail and/or other deliveries	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
l. Escort facility visitors	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
m. Activate monitoring systems, such as surveillance cameras	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
n. Activate intrusion detection systems	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
o. Recommend that employees limit travel	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
p. Limit and/or close facilities to visitors	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
q. Limit and/or close facilities to non-essential employees	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
r. Close facilities to essential employees and/or move operations to alternative site	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
s. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure

Continued on next page

GAO Survey on Threat Alerts

	Question 8a	Question 8b	Question 8c	Question 8d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17–April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20–May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003–Jan. 9, 2004**
2. Border and transportation security efforts ❒ If your agency did not implement any types of measures in category "2", please check this box and skip to category "3".				
a. Deploy inspectors, patrol agents, passenger and baggage screeners, and/or Air and Sea Marshals	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
b. Implement random shift changes for inspectors, patrol agents, and screeners	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
c. Extend shifts for inspectors, patrols agents, screeners, and/or Air and Sea Marshals	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
d. Implement air-, water-, and land-based patrols around borders and ports of entry	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
e. Inspect/screen vehicles, cargo, baggage and persons	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
f. Screen and/or detain visa and asylum applicants	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
g. Escort ferries and cruise ships	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
h. Activate monitoring systems at ports of entry	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
i. Conduct security checks of sensitive areas at ports of entry	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
j. Other measures in this category (Please specify.) _____ _____	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure

Continued on next page

GAO Survey on Threat Alerts

	Question 8a	Question 8b	Question 8c	Question 8d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17–April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20–May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003–Jan. 9, 2004**
3. Information collection, analysis, and dissemination ❒ If your agency did not implement any types of measures in category "3", please check this box and skip to category "4".				
a. Convene emergency response/crisis management team	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
b. Alert federal, state, local, private sector, and international counterparts	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
c. Issue recommendations or guidance for protective measures to federal, state, local, and private sector officials	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
d. Report measures taken to the Department of Homeland Security (DHS) or other federal entities	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
e. Activate agency 24-hour operation/command center	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
f. Detail staff to the Homeland Security Operations Center	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
g. Conduct surveillance and monitoring of persons and goods	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
h. Conduct interviews of persons and information contacts	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
i. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure

Continued on next page

GAO Survey on Threat Alerts

	Question 8a	Question 8b	Question 8c	Question 8d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17–April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20–May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003–Jan. 9, 2004**
4. Emergency response preparations ❒ If your agency did not implement any types of measures in category "4", please check this box and skip to category "5".				
a. Extend shifts for emergency workers	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
b. Detail federal personnel to state or local jurisdictions	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
c. Mobilize emergency response teams	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
d. Activate reserve personnel or make arrangements for military reserve personnel called to serve	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
e. Ensure that response procedures and communication plans are up to date	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
f. Ensure emergency response materials are staged, secured, and complete	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
g. Conduct emergency response drills and/or training	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
h. Prepare for possible biological, chemical, or radiological attacks	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
i. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure
5. Other types of measures ***(Please specify.)*** _____ _____	❒ Yes ❒ No ❒ N/A	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change in measure

9. We would like to know about the guidance and/or information/intelligence your agency received and used to determine the protective measures implemented specifically in response to the Code-Orange alert from March 17 to April 16, 2003.

9a. In addition to your agency's planned protective measures for national threat levels, did your agency receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **March 17 to April 16, 2003**? *(Please check one answer in each row under question 9a.)*

9b. ***For each item you answer "yes" in question 9a, please answer:*** Did your agency use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **March 17 to April 16, 2003**?

9c. ***For each item you answer "yes" in question 9b, please answer questions 9c and 9d:*** How useful was the guidance and/or information/ intelligence from the source?

9d. Was the guidance and/or information/ intelligence from the source timely?

	Question 9a Received?				Question 9b Used?				Question 9c Useful?				Question 9d Timely?	
Guidance and/or information/ intelligence and sources	Yes	No	Don't know	If "yes" to Q9a ➡	Yes	No	Don't know	If "yes" to Q9b ➡	Very useful	Somewhat useful	Of little or no use	➡	Yes	No
1. Guidance (e.g., recommended measures, identification of critical infrastructure) **from:**														
a. DHS (including FPS and FEMA)														
b. Federal Bureau of Investigation (FBI)														
c. White House														
d. Local law enforcement														
e. Other sources (Please specify.) _____														
2. Information/Intelligence (e.g., region, sector or site-specific threats, threat timeframes) **from:**				***If "yes" to Q9a*** ➡				***If "yes" to Q9b*** ➡				➡		
a. DHS (including FPS and FEMA)														
b. FBI														
c. White House														
d. National or regional Joint Terrorism Task Force														
e. Your agency's own intelligence sources														
f. Local law enforcement														
g. Other sources (Please specify.) _____														

10. We would like to know about the guidance and/or information/intelligence your agency received and used to determine the protective measures implemented specifically in response to the Code-Orange alert from **May 20 to May 30, 2003**.

10a. In addition to your agency's planned protective measures for national threat levels, did your agency receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **May 20 to May 30, 2003**? *(Please check one answer in each row under question 10a.)*

10b. ***For each item you answer "yes" in question 10a, please answer:*** Did your agency use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **May 20 to May 30, 2003**?

10c. ***For each item you answer "yes" in question 10b, please answer questions 10c and 10d:*** How useful was the guidance and/or information/intelligence from the source?

10d. Was the guidance and/or information/ intelligence from the source timely?

	Question 10a Received?				Question 10b Used?				Question 10c Useful?				Question 10d Timely?	
Guidance and/or information/ intelligence and sources	Yes	No	Don't know	*If "yes" to Q10a* ➡	Yes	No	Don't know	*If "yes" to Q10b* ➡	Very useful	Somewhat useful	Of little or no use	➡	Yes	No
1. Guidance (e.g., recommended measures, identification of critical infrastructure) **from:**														
a. DHS (including FPS and FEMA)														
b. FBI														
c. White House														
d. Local law enforcement														
e. Other sources *(Please specify.)* _____														
2. Information/Intelligence (e.g., region, sector or site-specific threats, threat timeframes) **from:**														
a. DHS (including FPS and FEMA)														
b. FBI														
c. White House														
d. National or regional Joint Terrorism Task Force														
e. Your agency's own intelligence sources														
f. Local law enforcement														
g. Other sources *(Please specify.)* _____														

GAO Survey on Threat Alerts

11. We would like to know about the guidance and/or information/intelligence your agency received and used to determine the protective measures implemented specifically in response to the Code-Orange alert from **December 21, 2003 to January 9, 2004**.

11a. In addition to your agency's planned protective measures for national threat levels, did your agency receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **December 21, 2003 to January 9, 2004**? *(Please check one answer in each row under question 11a.)*

11b. ***For each item you answer "yes" in question 11a, please answer:*** Did your agency use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **December 21, 2003 to January 9, 2004**?

11c. ***For each item you answer "yes" in question 11b, please answer questions 11c and 11d:*** How useful was the guidance and/or information/intelligence from the source?

11d. Was the guidance and/or information/ intelligence from the source timely?

Guidance and/or information/ intelligence and sources	Question 11a Received? Yes	No	Don't know	*If "yes" to Q11a* ➡	Question 11b Used? Yes	No	Don't know	*If "yes" to Q11b* ➡	Question 11c Useful? Very useful	Somewhat useful	Of little or no use	➡	Question 11d Timely? Yes	No
1. Guidance (e.g., recommended measures, identification of critical infrastructure) **from:**														
a. DHS (including FPS and FEMA)														
b. FBI														
c. White House														
d. Local law enforcement														
e. Other sources *(Please specify.)* _____														
2. Information/Intelligence (e.g., region, sector or site-specific threats, threat timeframes) **from:**				*If "yes" to Q11a* ➡				*If "yes" to Q11b* ➡				➡		
a. DHS (including FPS and FEMA)														
b. FBI														
c. White House														
d. National or regional Joint Terrorism Task Force														
e. Your agency's own intelligence sources														
f. Local law enforcement														
g. Other sources *(Please specify.)* _____														

12. In addition to guidance and information indicated above, what other types of information, if any, would have been helpful to your agency in deciding what protective measures to implement specifically in response to the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Types of information	Part A **Code-Orange Alert March 17 - April 16, 2003**	Part B **Code-Orange Alert May 20 – May 30, 2003**	Part C **Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004**
a. Information on regional or sector-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Information on site or event-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Information on threat time frames	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Recommended measures for preventing incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Recommended measures for responding to incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
f. Other types of information *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

13. Please describe examples of ways in which protective measures implemented during the Code-Orange alerts (March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004) benefited your agency.

_____

_____

_____

_____

_____

14. Please describe examples of ways in which your agency's operations were affected during the Code-Orange alerts (March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004), such as longer lines for visitors or shifting of resources from normal operations.

_____

_____

_____

_____

_____

15. Did your agency receive confirmation from component entities, offices, and/or personnel that the additional protective measures indicated in questions 8b, 8c, and 8d (on pages 6 through 10) were actually implemented during the HSAS Code-Orange alert from: *(Please check one answer in each row.)*

Code-Orange alert period	Yes	No	Don't know
a. March 17 to April 16, 2003?			
b. May 20 to May 30, 2003?			
c. December 21, 2003 to January 9, 2004?			

If you answered "yes" for <u>any</u> of the three Code-Orange alert periods in question 15 (a, b, or c), please answer question 16; otherwise, skip to question 17:

16. How did your agency receive confirmation that the additional protective measures indicated in questions 8b, 8c, and 8d were actually implemented during the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)*

    a. <u>March 17 to April 16, 2003</u>?
    b. <u>May 20 to May 30, 2003</u>?
    c. <u>December 21, 2003 to January 9, 2004</u>?

Method	**Part A** **Code-Orange Alert March 17 - April 16, 2003**	**Part B** **Code-Orange Alert May 20 – May 30, 2003**	**Part C** **Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004**
a. Received **oral** notification of implementation of protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Received **written** notification of implementation of protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Inspected implementation of protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

Costs Incurred During the HSAS Code-Orange Alerts

17. Does your agency have any data on actual or estimated additional security-related costs incurred during the HSAS <u>Code-Orange alert period from March 17 to April 16, 2003</u>? *(Please check only one answer.)*

    1. ❒ Yes ➡ ***(Continue with question 18.)***
    2. ❒ No ➡ ***(Skip to question 23.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from March 17 to April 16, 2003, please answer:

18. What were your agency's **total security-related** costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, that immediately preceded the HSAS Code-Orange alert period from March 17 to April 16, 2003?

19. What **additional security-related costs**, if any, did your agency incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from March 17 to April 16, 2003?

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know" costs for the category.*
For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)

Types of security-related costs	Question 18 **Total security-related costs for Code-Yellow alert, February 28 to March 16, 2003**		Question 19 **Additional security-related costs for Code-Orange alert, March 17 to April 16, 2003**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 18 and/or 19, please answer questions 20 and 21; otherwise, skip to question 22:

20. Please describe how your agency determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, and/or the HSAS Code-Orange alert period from March 17 to April 16, 2003 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

21. Please briefly list the procedures used by your agency to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 18 and/or 19, please answer question 22; otherwise, skip to question 23:

22. Please briefly describe how your agency developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, and/or the HSAS Code-Orange alert period from March 17 to April 16, 2003.

_____

_____

_____

_____

23. Does your agency have any data on actual or estimated additional security-related costs incurred during the HSAS Code-Orange alert period from May 20 to May 30, 2003? *(Please check only one answer.)*

1. ❒ Yes ➡ ***(Continue with question 24.)***
2. ❒ No ➡ ***(Skip to question 29.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from May 20 to May 30, 2003, please answer:

24. What were your agency's **total security-related** costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, that preceded the HSAS Code-Orange alert period from May 20 to May 30, 2003?

25. What **additional security-related costs**, if any, did your agency incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from May 20 to May 30, 2003?

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know" costs for the category.*
For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)

Types of security-related costs	Question 24 **Total security-related costs for Code-Yellow alert, April 17 to May 19, 2003**		Question 25 **Additional security-related costs for Code-Orange alert, May 20 to May 30, 2003**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 24 and/or 25, please answer questions 26 and 27; otherwise, skip to question 28:

26. Please describe how your agency determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, and/or the HSAS Code-Orange alert period from May 20 to May 30, 2003 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

27. Please briefly list the procedures used by your agency to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 24 and/or 25, please answer question 28; otherwise, skip to question 29:

28. Please briefly describe how your agency developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, and/or the HSAS Code-Orange alert period from May 20 to May 30, 2003.

_____

_____

_____

_____

29. Does your agency have any data on actual or estimated additional security-related costs incurred during the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004? *(Please check only one answer.)*

    1. ❒ Yes ➡ ***(Continue with question 30.)***
    2. ❒ No ➡ ***(Skip to question 35.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004, please answer:

30. What were your agency's **total security-related** costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, that preceded the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004?

31. What **additional security-related costs**, if any, did your agency incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004?

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know" costs for the category.*
For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)

Types of security-related costs	Question 30 **Total security-related costs for Code-Yellow alert, May 31 to Dec. 20, 2003**		Question 31 **Additional security-related costs for Code-Orange alert, Dec. 21, 2003 to Jan. 9, 2004**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 30 and/or 31, please answer questions 32 and 33; otherwise, skip to question 34:

32. Please describe how your agency determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, and/or the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

33. Please briefly list the procedures used by your agency to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 30 and/or 31, please answer question 34; otherwise, skip to question 35:

34. Please briefly describe how your agency developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, and/or the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004.

_____

_____

_____

_____

Agency Notification Process

35. How did your agency learn about the HSAS Code-Orange alert from:
(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each column.)

a. March 17 to April 16, 2003?
b. May 20 to May 30, 2003?
c. December 21, 2003 to January 9, 2004?

Method	Part A Code-Orange Alert March 17 - April 16, 2003	Part B Code-Orange Alert May 20 – May 30, 2003	Part C Code-Orange Alert Dec. 21, 2003 - Jan. 9, 2004
a. Direct notification from DHS (not via media sources)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Direct notification by another federal entity, such as the White House or the FBI (not via media sources)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Media sources	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" that your agency received direct notification from DHS for any period in question 35 (Part A, Part B, or Part C) above, please answer questions 36 and 37; otherwise, skip to question 38:

36. How did DHS notify your agency about the HSAS Code-Orange alert from:
(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)

a. March 17 to April 16, 2003?
b. May 20 to May 30, 2003?
c. December 21, 2003 to January 9, 2004?

Method	Part A Code-Orange Alert March 17 - April 16, 2003	Part B Code-Orange Alert May 20 – May 30, 2003	Part C Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004
a. Through your agency representatives at the Homeland Security Operations Center	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Through a single official announcement to all federal agencies via telephone, E-mail, or fax	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Through an individual agency message via telephone, E-mail, or fax	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Through an electronic communications system, such as the Washington Area Warning Alert System (WAWAS)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

37. What type(s) of information was included in DHS's official notification for the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Method	Part A **Code-Orange Alert March 17 - April 16, 2003**	Part B **Code-Orange Alert May 20 – May 30, 2003**	Part C **Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004**
a. Notification only of a national threat-level increase	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. General information on homeland security threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Information on regional or sector-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Information on site or event-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Information on threat time frames	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
f. Recommended measures for preventing incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
g. Recommended measures for responding to incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
h. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

38. What types of information would your agency like to receive along with the notification of future national threat-level changes? *(Please check one answer in each row.)*

Types of information	Yes	No	Don't know
a. Information on regional or sector-specific threats			
b. Information on site or event-specific threats			
c. Information on threat time frames			
d. Recommended measures for preventing incidents			
e. Recommended measures for responding to incidents			
f. Other types of information *(Please specify.)* _____ _____			

39. For each of the methods listed below, please indicate whether or not your agency would like to be notified of future changes in the national threat-level through this method. *(Please check one answer in each row.)*

Method	Yes	No	Don't know
a. Through your agency representatives at the Homeland Security Operations Center			
b. Through a single official announcement to all federal agencies via telephone, E-mail, or fax			
c. Through an individual agency message via telephone, E-mail, or fax			
d. Through an electronic communications system such as the Washington Area Warning Alert System (WAWAS)			
e. Other methods *(Please specify.)* _____ _____			

Financial and Operational Challenges in Implementing HSAS Code-Orange Alert Measures

40. What financial challenges, if any, did your agency face in responding to the HSAS Code-Orange alert from: *(Please check one answer ("Yes"," No", or "Don't Know-DK") in each row in each column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Method	Part A **Code-Orange Alert March 17 - April 16, 2003**	Part B **Code-Orange Alert May 20 – May 30, 2003**	Part C **Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004**
a. Insufficient funding available to implement measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Difficulty redirecting other funds to security-related measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Difficulty tracking costs for measures implemented	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" to any financial challenge in rows a through d in question 40 (Part A, Part B, or Part C) above, please answer question 41; otherwise, skip to question 42:

41. Briefly describe one or more examples of financial challenges faced during the alerts.

_____

_____

_____

_____

_____

42. What operational challenges, if any, did your agency face in responding to the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Method	Part A **Code-Orange Alert March 17 - April 16, 2003**	Part B **Code-Orange Alert May 20 – May 30, 2003**	Part C **Code-Orange Alert Dec. 21, 2003 – Jan. 9, 2004**
a. Insufficient information on the threat	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Insufficient number of available personnel	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Insufficient training of personnel to implement assigned measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Insufficient equipment and/or materials	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Technological or other limitations of available equipment and/or materials	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
f. Insufficient facilities and/or space	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
g. Insufficient guidance to implement measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
h. Lack of federal government-wide coordination	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
i. Other *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" to any operational challenge in rows a through i in question 42 (Part A, Part B, or Part C) above, please answer question 43; otherwise, skip to question 44:

43. Briefly describe one or more examples of operational challenges faced during the alerts.

_____

_____

_____

_____

_____

_____

44. If you have any comments regarding any of the issues covered in this questionnaire or have any other comments about protective measures, guidance, and costs for HSAS Code-Orange alerts, please use the space provided.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Thank you for your assistance. Please return the questionnaire and, dependent on your answers to questions 1, 5, 6, or 7, any accompanying documentation according to the instructions on page 1.

State and Territory Questionnaire

United States General Accounting Office

Survey of State and Territory Plans, Protective Measures, Guidance, and Costs for Elevated Threat Levels

The U.S. General Accounting Office (GAO), an investigative arm of Congress, has been requested by the Congress to review states' and U.S. territories' security-related protective measures, guidance, and costs for periods when the national threat level was raised from yellow (elevated) to orange (high). As part of this request, GAO is surveying the 50 states, U.S. territories, and Washington, D.C. to determine (1) what, if any, protective measures were taken during periods of orange alert, specifically for periods March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004; (2) guidance and other information used by states and territories in implementing those measures; and (3) costs incurred by states and territories as a result of protective measures implemented during these three orange alert periods. To better inform the Congress on the Homeland Security Advisory System (HSAS) and identify potential improvements, GAO is also collecting data on (1) applicable threat alert systems used by states and territories prior to the establishment of the HSAS and (2) operational and financial challenges faced by states and territories as a result of responding to code-orange alerts.

This questionnaire should be completed by the person(s) most knowledgeable about the guidance received and protective measures taken by your state or territory during the periods identified above, including the protective measures your jurisdiction developed to respond to national threat levels, any threat-advisory system you have in place, types of protective measures taken, costs incurred during these periods of orange alert, how your state or territory was notified of the increase in the national threat level, and financial and operational challenges your state or territory faced during these periods of orange alert. **If your state or territory, or certain of its facilities, remains on orange alert even though the national threat level has been lowered, please answer the questions about the most recent orange alert period considering your state or territory's actions and costs through January 9, 2004.** Most of the questions can be answered by marking boxes or filling in blanks. Space has also been provided for comments and we encourage you to provide whatever additional comments you think appropriate; please feel free to type out these comments on a separate attachment (identified by question number) if you prefer. In our report, the responses from your state or territory will be presented only after they have been aggregated with responses from other states and territories. GAO will not release individual responses to any entity unless requested by Congress or compelled by law. In addition, GAO will take appropriate measures to safeguard any sensitive information you provide, and, upon request, can provide security clearance information for staff reviewing survey responses.

Please complete this questionnaire and return it within 2 weeks of receipt. Your participation is important! A pre-addressed Federal Express envelope has been included to return this questionnaire. If you have any questions or misplace the return envelope, please contact Nancy Briggs at (202) 512-5703 or Gladys Toro at (202) 512-3047.

Please provide the name, title, and telephone number of the primary person completing this questionnaire and your state or territory name so that we may contact that person if we need to clarify any responses.

Name: _____

Title: _____

Telephone number: (_____)_____

State or Territory: _____

We modified the format of this questionnaire slightly for inclusion in this report, but we did not change the content of the questionnaire.

Sections I and II of this questionnaire ask you to report on your state's or territory's protective measures and advisory systems for all levels of national alert; the remaining sections ask you specifically about Code-Orange alerts. When completing this questionnaire, please consider only actions taken and costs incurred at the state or territory level; **do not include local level actions and costs**.

I. State and Territory Protective Measures for Responding to National Threat Levels

1. According to Homeland Security Presidential Directive 3, issued in March 2002, states and territories are encouraged to develop protective measures and other antiterrorism or self-protection and continuity plans for responding to national threat levels (*see bolded passage on page 2 of the attachment*).

   Has your state or territory developed protective measures for responding to national threat levels? *(Please check only one answer.)*

   1. ❒ Yes, state or territory has developed protective measures for responding to national threat levels

   2. ❒ No, state or territory has not developed protective measures for responding to national threat levels

   If you answered "no" to question 1, please skip to question 5; otherwise, please continue.

2. Did your state or territory use guidance and/or information from any of the following sources in developing your protective measures for responding to national threat levels? *Please note that the Department of Homeland Security was not established until March 2003. Thus, it would not be a source of guidance for performance measures developed in March 2002. (Please check one answer in each row.)*

Source	Yes	No	Don't know
a. Federal Emergency Management Agency (FEMA)			
b. Department of Justice, including the FBI			
c. Another federal agency *(Please specify.)* _____ _____			
d. Governor or legislature			
e. State, territorial, or local law enforcement			
f. Another state or territorial governmental agency (*Please specify.*) _____ _____			
g. Vulnerability assessments for your state or territory			
h. Private sector entity			
i. Other methods *(Please specify.)* _____ _____			

If you answered "yes" for any source in question 2, answer question 3; otherwise, skip to question 4.

3. Please list the source and titles or topics of any written guidance used by your state or territory in developing protective measures for responding to national threat levels?

Source	Title or topic (e.g., how to identify critical infrastructure)
_____	_____
_____	_____
_____	_____
_____	_____

4. Within the past year, did your state or territory test the functionality and reliability of any of the following protective measures to determine vulnerabilities? *(Please check one answer in each row.)*

Protective measure	Yes	No	Don't know	Not applicable
a. Intrusion detection systems				
b. Visitor/employee screening equipment and procedures				
c. Vehicle inspection equipment and procedures				
d. Baggage and/or cargo screening equipment and procedures				
e. Mail and delivery screening procedures				
f. Monitoring systems, such as surveillance cameras				
g. Technology security systems				
h. Continuity of operations measures				
i. Emergency response measures				
j. Other measures *(Please specify.)* _____ _____				

II. Threat Advisory Systems

To better inform the Congress on the Homeland Security Advisory System (HSAS) and identify potential improvements, GAO is collecting data on applicable alert systems used by states and territories to possibly identify best practices that could potentially be incorporated in future revisions of the HSAS.

5. Did your state or territory have its own threat-advisory system for assessing and responding to threats and emergency situations prior to the establishment of the HSAS in March 2002?
(Please check only one answer.)

   1. ❒ Yes, state or territory had its own threat-advisory system in place prior to March 2002 ➡ Please provide the name of your threat-advisory system _____

   2. ❒ No, state or territory did not have its own threat-advisory system

If you answered "yes" to question 5, please answer question 6; otherwise, skip to question 7.

6. Did your system contain any of the following characteristics: *(Please check one answer in each row.)*

Characteristics	Yes	No	Don't know
a. Identified specific threat levels			
b. Provided specific information about the type or location of threat			
c. Provided for notification of other state or territorial agencies			
d. Provided for notification of city, county, or local agencies			
e. Provided for notification of private sector entities			
f. Specified protective measures to be taken			

7. Does your state or territory currently have its own threat-advisory system in place that could operate independently of the HSAS in assessing and responding to threats and emergency situations? *(Please check only one answer.)*

   1. ❒ Yes, state or territory currently has its own threat-advisory in place

   2. ❒ No, state or territory does not currently have its own threat-advisory system in place

If you answered "yes" to question 7, please answer question 8; otherwise, skip to question 9.

8. Does your system contain any of the following characteristics: *(Please check one answer in each row.)*

Characteristics	Yes	No	Don't know
a. Identifies specific threat levels			
b. Provides specific information about the type or location of threat			
c. Provides for notification of other state or territorial agencies			
d. Provides for notification of city, county, or local agencies			
e. Provides for notification of private sector entities			
f. Specifies protective measures to be taken			

9. To what extent, if at all, does your state or territory follow the HSAS for identifying and responding to homeland security threats? *(Please check only one answer.)*

   1. ❒ State or territory only follows the HSAS

   2. ❒ State or territory follows the HSAS and its own threat advisory system that conforms to the HSAS

   3. ❒ State or territory follows the HSAS and its own threat advisory system that does not conform to the HSAS

   4. ❒ State or territory does not follow the HSAS, but uses its own threat advisory system

   5. ❒ State or territory does not follow the HSAS and does not use its own threat–advisory system, but follows another threat-level system (e.g., the Department of Defense's Force Protection Condition system)

   6. ❒ State or territory does not follow any threat-advisory system

If you answered #4, #5, or #6 to question 9, please stop and return this questionnaire according to the instructions on page 1.

III. Types of Protective Measures Used During HSAS Code-Yellow Alerts and Specifically in Response to Code-Orange Alerts from March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004

10. We would like to know about the guidance and/or information/intelligence your state or territory received and used to determine the protective measures to implement specifically in response to the Code-Orange alert from **March 17 to April 16, 2003**.

10a. Please indicate the protective measures your state or territory (or at least one state or territory department) has in place for Code-Yellow alerts. *(Please check "Yes", "No", "Not applicable-N/A", or "Don't Know-DK" for each measure).*

10b, 10c, and 10d. Please indicate the protective measures your state or territory (or at least one state or territory department) implemented or increased the use of specifically in response to the Code-Orange alerts, that is, measures implemented in addition to the measures used in the preceding Code-Yellow alert period. *(Please check "Implemented, Code-Orange only", "Increased use of", "N/A or no change," or "Don't Know-DK" for each measure in each column)*

	Question 10a	Question 10b	Question 10c	Question 10d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17 – April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20 – May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003 – Jan. 9, 2004**
1. Protection of state or territorial facilities (including critical infrastructure), personnel, and systems				
❒ If your state or territory did not implement any types of measures in category "1", please check this box and skip to category "2".				
a. Implement facility security patrols	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
b. Implement random shift changes for security or law enforcement personnel	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
c. Extend shifts for security or law enforcement personnel	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
d. Inspect visitors and their belongings upon entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
e. Inspect employees and their belongings upon entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
f. Inspect vehicles entering or parking near facilities	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
g. Restrict parking near facilities	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK

GAO State Survey on Terrorist Alerts

	Question 10a	Question 10b	Question 10c	Question 10d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17 – April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20 – May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003 – Jan. 9, 2004**
h. Place vehicle barriers around facilities	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
i. Expand security perimeter at facilities	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
j. Limit number of facility access points	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
k. Screen mail and/or other deliveries	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
l. Escort facility visitors	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
m. Activate monitoring systems, such as surveillance cameras	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
n. Activate intrusion detection systems	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
o. Recommend that employees limit travel	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
p. Limit and/or close facilities to visitors	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
q. Limit and/or close facilities to non-essential employees	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
r. Close facilities to essential employees and/or move operations to alternative site	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
s. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK

GAO State Survey on Terrorist Alerts

	Question 10a	Question 10b	Question 10c	Question 10d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17 – April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20 – May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003 – Jan. 9, 2004**
2. Border and transportation security efforts				
❒ If your state or territory did not implement any types of measures in category "2", please check this box and skip to category "3".				
a. Deploy inspectors, patrol agents, and/or passenger and baggage screeners	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
b. Implement random shift changes for inspectors, patrol agents, and screeners	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
c. Extend shifts for inspectors, patrols agents, and/or screeners	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
d. Implement air-, water-, and land-based patrols around borders and ports of entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
e. Inspect/screen vehicles, cargo, baggage and persons	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
f. Screen for and/or detain visa and asylum applicants or prevent illegal entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
g. Escort ferries and cruise ships	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
h. Activate monitoring systems at ports of entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
i. Conduct security checks of sensitive areas at ports of entry	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
j. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK

GAO State Survey on Terrorist Alerts

	Question 10a	Question 10b	Question 10c	Question 10d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17 – April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20 – May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003 – Jan. 9, 2004**
3. Information collection, analysis, and dissemination				
❒ If your state or territory did not implement any types of measures in category "3", please check this box and skip to category "4".				
a. Convene emergency response/crisis management team	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
b. Alert other state, territorial, local, and private sector counterparts	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
c. Issue recommendations or guidance for protective measures to state, territorial, local, or private sector officials	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
d. Report measures taken to the Department of Homeland Security (DHS) or other federal entities	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
e. Activate 24 hour operations command center	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
f. Detail staff to the Department of Homeland Security Operations Center	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
g. Conduct surveillance and monitoring of persons and goods	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
h. Conduct interviews of information contacts	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
i. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK

GAO State Survey on Terrorist Alerts

	Question 10a	Question 10b	Question 10c	Question 10d
	Measure already in place for Code-Yellow alerts	**Implemented or increased use of measure for Code-Orange alert, March 17 – April 16, 2003**	**Implemented or increased use of measure for Code-Orange alert, May 20 – May 30, 2003**	**Implemented or increased use of measure for Code-Orange alert, Dec. 21, 2003 – Jan. 9, 2004**
4. Emergency response preparations ❒ If your state or territory did not implement any types of measures in category "4", please check this box and skip to category "5".				
a. Extend shifts for emergency workers	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
b. Detail state personnel to regional or local jurisdictions	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
c. Mobilize emergency response teams	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
d. Activate reserve personnel or make arrangements for military reserve personnel called to serve	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
e. Ensure that response procedures and communication plans are up to date	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
f. Ensure emergency response materials are staged, secured, and complete	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
g. Conduct emergency response drills and/or training	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
h. Prepare for possible biological, chemical, or radiological attacks	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
i. Other measures in this category *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK
5. Other types of measures ***(Please specify.)*** _____ _____ _____	❒ Yes ❒ No ❒ N/A ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK	❒ Implemented, Code-Orange only ❒ Increased use of ❒ N/A or no change ❒ DK

GAO State Survey on Terrorist Alerts

11. We would like to know about the guidance and/or information/intelligence your state or territory received and used to determine the protective measures to implement specifically in response to the Code-Orange alert from **March 17 to April 16, 2003**.

11a. In addition to planned protective measures for national threat levels, did your state or territory receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **March 17 to April 16, 2003**? *(Please check one answer in each row under question 11a.)*

11b. ***For each item you answer "yes" in question 11a, please answer:*** Did your state or territory use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **March 17 to April 16, 2003**?

11c. ***For each item you answer "yes" in question 11b, please answer questions 11c and 11d:*** How useful was the guidance and/or information/intelligence from the source?

11d. Was the guidance and/or information/intelligence from the source timely

	Question 11a Received?				Question 11b Used?				Question 11c Useful?				Question 11d Timely?	
Guidance and/or information/ intelligence and sources	Yes	No	Don't know	*If "yes" to Q11a* ➡	Yes	No	Don't know	*If "yes" to Q11b* ➡	Very useful	Somewhat useful	Of little or no use		Yes	No
1. **Guidance** (e.g., recommended measures, identification of critical infrastructure) **from**:														
a. DHS (including FEMA)														
b. Other federal agency, such as the FBI and its Joint Terrorism Task Force (JTTF) *(Please specify.* _____														
c. Other state, territorial, or local government agencies *(Please specify.)*														
d. Private sector														
e. Regional, state or local law enforcement														
f. Governor or legislature														
g. Other sources *(Please specify.)* _____														
2. **Information/Intelligence** (e.g., region, sector or site-specific threats, threat timeframes) **from**:				*If "yes" to Q11a* ➡				*If "yes" to Q11b* ➡						
a. DHS (including FEMA)														
b. Other federal agency, such as the FBI and its JTTF *(Please specify.)*														
c. Other state, territorial, or local government agencies *(Please specify).*														
d. Private sector														
e. Regional, state or local law enforcement														
f. Governor or legislature														
g. Other sources *(Please specify.)* _____														

11

GAO State Survey on Terrorist Alerts

12. We would like to know about the guidance and/or information/intelligence your state or territory received and used to determine the protective measures to implement specifically in response to the Code-Orange alert from **May 20 to May 30, 2003**.

12a. In addition to planned protective measures for national threat levels, did your state or territory receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **May 20 to May 30, 2003**? *(Please check one answer in each row under question 12a.)*

12b. ***For each item you answer "yes" in question 12a, please answer:*** Did your state or territory use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **May 20 to May 30, 2003**?

12c. ***For each item you answer "yes" in question 12b, please answer questions 12c and 12d:*** How useful was the guidance and/or information/intelligence from the source?

12d. Was the guidance and/or information/intelligence from the source timely?

Guidance and/or information/ intelligence and sources	Question 12a Received? Yes	No	Don't know	*If "yes" to Q12a*	Question 12b Used? Yes	No	Don't know	*If "yes" to Q12b*	Question 12c Useful? Very useful	Somewhat useful	Of little or no use	Question 12d Timely? Yes	No
1. **Guidance** (e.g., recommended measures, identification of critical infrastructure) **from**:													
a. DHS (including FEMA)													
b. Other federal agency, such as the FBI and its JTTF *(Please specify.)* _____													
c. Other state, territorial, or local government agencies *(Please specify.)*													
d. Private sector													
e. Regional, state, or local law enforcement													
f. Governor or legislature													
g. Other sources *(Please specify.)* _____													
2. **Information/Intelligence** (e.g., region, sector or site-specific threats, threat timeframes) **from**:				*If "yes" to Q12a*				*If "yes" to Q12b*					
a. DHS (including FEMA)													
b. Other federal agency, such as the FBI and its JTTF *(Please specify.)* _____													
c. Other state, territorial, or local government agencies *(Please specify.)*													
d. Private sector													
e. Regional, state, or local law enforcement													
f. Governor or legislature													
g. Other sources *(Please specify.)* _____													

GAO State Survey on Terrorist Alerts

13. We would like to know about the guidance and/or information/intelligence your state or territory received and used to determine the protective measures to implement specifically in response to the Code-Orange alert from **December 21, 2003 to January 9, 2004**.

13a. In addition to planned protective measures for national threat levels, did your state or territory receive guidance and/or information/intelligence from any of the following sources to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **December 21, 2003 to January 9, 2004**? *(Please check one answer in each row under question 13a.)*

13b. ***For each item you answer "yes" in question 13a, please answer:*** Did your state or territory use the guidance and/or information/intelligence received from the source to determine the measures implemented specifically in response to the HSAS Code-Orange alert from **Dec. 21, 2003 to Jan. 9, 2004**?

13c. ***For each item you answer "yes" in question 13b, please answer questions 13c and 13d:*** How useful was the guidance and/or information/intelligence from the source?

13d. Was the guidance and/or information/ intelligence from the source timely?

Guidance and/or information/ intelligence and sources	Question 13a Received? Yes	No	Don't know	*If "yes" to Q13a*	Question 13b Used? Yes	No	Don't know	*If "yes" to Q13b*	Question 13c Useful? Very useful	Somewhat useful	Of little or no use	Question 13d Timely? Yes	No
1. **Guidance** (e.g., recommended measures, identification of critical infrastructure) **from**:													
a. DHS (including FEMA)													
b. Other federal agency, such as the FBI and its JTTF *(Please specify.)* _____													
c. Other state, territorial, or local government agencies *(Please specify.)*													
d. Private sector													
e. Regional, state or local law enforcement													
f. Governor or legislature													
g. Other sources *(Please specify.)* _____													
2. **Information/Intelligence** (e.g., region, sector or site-specific threats, threat timeframes) **from**:				*If "yes" to Q13a*				*If "yes" to Q13b*					
a. DHS (including FEMA)													
b. Other federal agency, such as the FBI and its JTTF *(Please specify.)* _____													
c. Other state, territorial, or local government agencies *(Please specify.)*													
d. Private sector													
e. Regional, state or local law enforcement													
f. Governor or legislature													
g. Other sources *(Please specify.)* _____													

13

14. In addition to guidance and information indicated above, what other types of information, if any, would have been helpful in deciding what protective measures to implement specifically in response to the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", "Don't Know-DK", or "Already Received") in each row in each applicable column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

	Part A	**Part B**	**Part C**
Types of information	**Code-Orange alert March 17 - April 16, 2003**	**Code-Orange alert May 20 – May 30, 2003**	**Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004**
a. Information on regional or sector-specific threats	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received
b. Information on site or event-specific threats	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received
c. Information on threat time frames	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received
d. Recommended measures for preventing incidents	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received
e. Recommended measures for responding to incidents	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received
f. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received	❒ Yes ❒ No ❒ DK ❒ Already received

15. Please describe examples of ways in which protective measures implemented during the Code-Orange alerts benefited your state or territory.

_____

_____

_____

_____

_____

16. Please describe examples of ways in which your state or territory's operations were affected during the Code-Orange alerts, such as, but not limited to, shifting resources from normal operations or reduced tourism.

_____

_____

_____

_____

_____

17. Did your state or territory receive confirmation from agencies, offices, and/or personnel within your jurisdiction that the additional protective measures indicated in questions 10b, 10c, and 10d (on pages 6 through 10) were actually implemented during the HSAS Code-Orange alert from: *(Please check one answer in each row.)*

Code-Orange alert period	Yes, received confirmation for **all** protective measures	Yes, received confirmation for **some** protective measures	No	Don't know
a. March 17 to April 16, 2003?				
b. May 20 to May 30, 2003?				
c. December 21, 2003 to January 9, 2004?				

If you answered "yes" or "some" for <u>any</u> of the three Code-Orange alert periods in question 17 (a, b, or c), please answer question 18; otherwise, skip to question 19:

18. How did your state or territory receive confirmation that the additional protective measures indicated in questions 10b, 10c, and 10d were actually implemented during the HSAS Code-Orange alert from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)*

    a. <u>March 17 to April 16, 2003</u>?
    b. <u>May 20 to May 30, 2003</u>?
    c. <u>December 21, 2003 to January 9, 2004</u>?

Method	**Part A** **Code-Orange alert March 17 - April 16, 2003**	**Part B** **Code-Orange alert May 20 – May 30, 2003**	**Part C** **Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004**
a. Received **oral** notification of implementation of some or all protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Received **written** notification of some or all implementation of protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Inspected implementation of some or all protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

19. Has DHS requested any of the following types of information on protective measures taken in response to increased national threat levels? *(Please check one answer in each row in each applicable column.)*

	Code-Orange alert March 17 - April 16, 2003	**Code-Orange alert May 20 – May 30, 2003**	**Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004**
a. Information about the types of security actions taken in response to the elevated threat	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Information about security actions taken at specific critical infrastructures or assets	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Information on the effectiveness of state or government security actions taken	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other information *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

IV. Costs Incurred During the HSAS Code-Orange Alerts

20. Does your state or territory have any data on actual or estimated additional security-related costs incurred during the HSAS Code-Orange alert period from March 17 to April 16, 2003? *(Please check only one answer.)*

1. ❒ Yes ➡ ***(Continue with question 21.)***
2. ❒ No ➡ ***(Skip to question 26.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from March 17 to April 16, 2003, we are assuming that the total security costs incurred during the HSAS Code-Yellow alert period from February 28 to March 16, 2003 will serve as your baseline.

21. What were your state or territory's **total security-related** costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, that immediately preceded the HSAS Code-Orange alert period from March 17 to April 16, 2003? *(Please provide your answer in the table below.)*

22. What **additional security-related costs**, if any, did your state or territory incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from March 17 to April 16, 2003? *(Please provide your answer in the table below.)*

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know". For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)*

Types of security-related costs	Question 21 **Total security-related costs for Code-Yellow alert, February 28 to March 16, 2003**		Question 22 **Additional security-related costs for Code-Orange alert, March 17 to April 16, 2003**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 21 and/or 22, please answer questions 23 and 24; otherwise, skip to question 25:

23. Please describe how your state or territory determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, and/or the HSAS Code-Orange alert period from March 17 to April 16, 2003 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

24. Please briefly list the procedures used by your state or territory to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 21 and/or 22, please answer question 25; otherwise, skip to question 26:

25. Please briefly describe how your state or territory developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from February 28 to March 16, 2003, and/or the HSAS Code-Orange alert period from March 17 to April 16, 2003.

_____

_____

_____

_____

26. If you have **any other data** on costs incurred during the HSAS Code-Orange alert period from March 17 to April 16, 2003 **that are not reported above**, please briefly describe.

_____

_____

_____

_____

27. Does your state or territory have any data on actual or estimated additional security-related costs incurred during the HSAS Code-Orange alert period from May 20 to May 30, 2003? *(Please check only one answer.)*

1. ❒ Yes ➡ ***(Continue with question 28.)***
2. ❒ No ➡ ***(Skip to question 33.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from May 20 to May 30, 2003, we are assuming that the total security costs incurred during the HSAS Code-Yellow alert period from April 17 to May 19, 2003 will serve as your baseline.

28. What were your state or territory's **total security-related** costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, that preceded the HSAS Code-Orange alert period from May 20 to May 30, 2003? *(Please provide your answer in the table below.)*

29. What **additional security-related costs**, if any, did your state or territory incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from May 20 to May 30, 2003? *(Please provide your answer in the table below.)*

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know". For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)*

Types of security-related costs	Question 28 **Total security-related costs for Code-Yellow alert, April 17 to May 19, 2003**		Question 29 **Additional security-related costs for Code-Orange alert, May 20 to May 30, 2003**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 28 and/or 29, please answer questions 30 and 31; otherwise, skip to question 32:

30. Please describe how your state or territory determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, and/or the HSAS Code-Orange alert period from May 20 to May 30, 2003 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

31. Please briefly list the procedures used by your state or territory to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 28 and/or 29, please answer question 32; otherwise, skip to question 33:

32. Please briefly describe how your state or territory developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from April 17 to May 19, 2003, and/or the HSAS Code-Orange alert period from May 20 to May 30, 2003.

_____

_____

_____

_____

33. If you have **any other data** on costs incurred during the HSAS Code-Orange alert period from May 20 to May 30, 2003 **that are not reported above**, please briefly describe.

_____

_____

_____

_____

34. Does your state or territory have any data on actual or estimated additional security-related costs incurred during the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004? *(Please check only one answer.)*

1. ❒ Yes ➡ ***(Continue with question 35.)***
2. ❒ No ➡ ***(Skip to question 40.)***

To provide a context for assessing additional costs incurred during the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004, we are assuming that the total security costs incurred during the HSAS Code-Yellow alert period from May 31 to December 20, 2003 will serve as your baseline.

35. What were your state or territory's **total security-related** costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, that preceded the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004? *(Please provide your answer in the table below.)*

36. What **additional security-related costs**, if any, did your state or territory incur for protective measures implemented specifically in response to the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004? *(Please provide your answer in the table below.)*

*(**NOTE:** For each category, please indicate whether the costs provided are **actual** or **estimated,** or if you "Don't Know". For categories where no costs were incurred, please list costs as $0. If costs by category cannot be provided, give "Grand total costs".)*

Types of security-related costs	Question 35 **Total security-related costs for Code-Yellow alert, May 31 to Dec. 20, 2003**		Question 36 **Additional security-related costs for Code-Orange alert, Dec. 21, 2003 to Jan. 9, 2004**	
a. **Personnel** *(e.g., security personnel, overtime)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
b. **Equipment/materials** *(e.g., screening equipment, canine/explosives detection materials, patrol vehicles)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
c. **Other costs** *(e.g., travel, training)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____
d. **Grand total costs** *(add items a, b, c from above)*	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____	❒ Actual costs ❒ Estimated costs ❒ Don't know costs	$_____

If you provided data for actual security-related costs in questions 35 and/or 36, please answer questions 37 and 38; otherwise, skip to question 39:

37. Please describe how your state or territory determined the total and/or additional security-related costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, and/or the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004 (e.g., financial accounting system, Microsoft Excel spreadsheet).

_____

_____

_____

_____

38. Please briefly list the procedures used by your state or territory to review and certify the reliability of this financial data (e.g., internal auditing procedures).

_____

_____

_____

_____

If you provided data for estimated security-related costs in questions 35 and/or 36, please answer question 39; otherwise, skip to question 40:

39. Please briefly describe how your state or territory developed the estimates for total and/or additional security-related costs for the HSAS Code-Yellow alert period from May 31 to December 20, 2003, and/or the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004.

_____

_____

_____

40. If you have **any other data** on costs incurred during the HSAS Code-Orange alert period from December 21, 2003 to January 9, 2004 **that are not reported above**, please briefly describe.

_____

_____

_____

_____

41. What guidance, if any, did your state or territory use to track costs incurred in response to the Code-Orange alerts of March 17 to April 16, 2003, May 20 to May 30, 2003, and/or December 21, 2003 to January 9, 2004? *(Please provide the source and the title or topic of the guidance.)*

Source	Title or topic
_____	_____
_____	_____
_____	_____

❒ Did not use any guidance

42. Has DHS provided any guidance to your state or territory on how or whether you should track costs incurred in response to increased national threat levels? *(Please check only one answer.)*

1. ❒ Yes, DHS has provided guidance on how or whether to track costs

2. ❒ No, DHS has not provided guidance on how or whether to track costs

If you answer "yes" to question 42, please answer question 43; otherwise skip to question 44.

43. How useful were the following types of guidance from DHS on how or whether to track costs, if provided? *(Please check one answer in each row.)*

Type of guidance provided	Very useful	Somewhat useful	Of little or no use	Not provided
a. Tracking total costs incurred in response to elevated threat levels				
b. Tracking costs incurred that are eligible for federal reimbursement				
c. Other methods *(Please specify.)* _____ _____				

44. Has DHS requested any data on additional costs incurred in response to the Code-Orange alert periods March 17 to April 16, 2003, May 20 to May 30, 2003, and December 21, 2003 to January 9, 2004 from your state or territory? *(Please check one answer in each row.)*

Code-Orange alert period	Yes	No	Don't know
a. March 17 to April 16, 2003?			
b. May 20 to May 30, 2003?			
c. December 21, 2003 to January 9, 2004?			

45. Have you submitted any security-related costs for reimbursement to DHS for any of the following Code-Orange alert periods? *(Please check one answer in each row.)*

Code-Orange alert period	Yes	No	Don't know
a. March 17 to April 16, 2003?			
b. May 20 to May 30, 2003?			
c. December 21, 2003 to January 9, 2004?			

46. Have you used any grant funds to reimburse your Code-Orange alert costs? *(Please check only one answer.)*

1. ❒ Yes ➡ Please provide the name of the grant(s) and amount(s).

_____

_____

_____

2. ❒ No

V. Homeland Security Advisory System (HSAS) Notification Process

47. In which of the following ways did your state or territory learn about the HSAS Code-Orange alerts for:
(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each column.)

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Method	Part A Code-Orange alert March 17 - April 16, 2003	Part B Code-Orange alert May 20 – May 30, 2003	Part C Code-Orange alert Dec. 21, 2003 - Jan. 9, 2004
a. Direct notification from DHS (not via media sources)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Direct notification by another federal entity, such as the FBI (not via media sources)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Media sources	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Notification from a state or territorial entity, such as a state law enforcement agency	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" that your state or territory received direct notification from DHS for any period in question 47 (Part A, Part B, or Part C) above, please answer questions 48 and 49; otherwise, skip to question 50:

48. How did DHS notify your state or territory about the HSAS Code-Orange alerts from:
(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Method	Part A Code-Orange alert March 17 - April 16, 2003	Part B Code-Orange alert May 20 – May 30, 2003	Part C Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004
a. Through your state or territory representatives at the Department of Homeland Security Operations Center	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Through a single official announcement to all state and territories via telephone, E-mail, or fax	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Through an individual message via telephone, E-mail, or fax	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Through an nation-wide communications system, such as the National Law Enforcement Telecommunications System (NLETS)	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

49. What type(s) of information was included in DHS's official notification for the HSAS Code-Orange alerts from: *(Please check one answer ("Yes", "No", or "Don't Know-DK") in each row in each applicable column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Type of information	**Part A** **Code-Orange alert March 17 - April 16, 2003**	**Part B** **Code-Orange alert May 20 – May 30, 2003**	**Part C** **Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004**
a. Notification only of a national threat-level increase	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. General information on homeland security threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Information on regional or sector-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Information on site or event-specific threats	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Information on threat time frames	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
f. Recommended measures for preventing incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
g. Recommended measures for responding to incidents	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
h. Other methods *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

50. What types of information would your state or territory like to receive along with the notification of future national threat-level changes? *(Please check one answer in each row.)*

Types of information	Yes	No	Don't know
a. Information on regional or sector-specific threats			
b. Information on site or event-specific threats			
c. Information on threat time frames			
d. Recommended measures for preventing incidents			
e. Recommended measures for responding to incidents			
f. Other types of information *(Please specify.)* _____ _____			

51. For each of the methods listed below, please indicate whether or not your state or territory would like to be notified of future changes in the national threat-level through this method. *(Please check one answer in each row.)*

Method	Yes	No	Don't know	N/A
a. Through your representatives at the Department of Homeland Security Operations Center				
b. Through a single official announcement to all state and territories via telephone, E-mail, or fax				
c. Through an individual message via telephone, E-mail, or fax				
d. Through an electronic communications system, such as the National Law Enforcement Telecommunications System (NLETS)				
e. Other methods *(Please specify.)* _____ _____				

VI. Financial and Operational Challenges in Implementing HSAS Code-Orange Alert Measures

52. What financial challenges, if any, did your state or territory face in responding to the HSAS Code-Orange alerts from: *(Please check one answer ("Yes," "No", or "Don't Know-DK") in each row in each column.)*

a. March 17 to April 16, 2003?
b. May 20 to May 30, 2003?
c. December 21, 2003 to January 9, 2004?

Challenge	Part A Code-Orange alert March 17 - April 16, 2003	Part B Code-Orange alert May 20 – May 30, 2003	Part C Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004
a. Unable to implement some protective measures due to insufficient funding	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Difficulty redirecting other funds to security-related measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Difficulty tracking costs for measures implemented	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Other challenges *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" to any financial challenge in rows a through d in question 52 (Part A, Part B, or Part C) above, please answer question 53; otherwise, skip to question 54:

53. Briefly describe examples of financial challenges and the consequences of these faced during the alerts.

_____

_____

_____

_____

_____

54. What operational challenges, if any, did your state or territory face in responding to the HSAS Code-Orange alerts from: *(Please check one answer ("Yes," "No", or "Don't Know-DK") in each row in each column.)*

    a. March 17 to April 16, 2003?
    b. May 20 to May 30, 2003?
    c. December 21, 2003 to January 9, 2004?

Challenge	**Part A** **Code-Orange alert March 17 - April 16, 2003**	**Part B** **Code-Orange alert May 20 – May 30, 2003**	**Part C** **Code-Orange alert Dec. 21, 2003 – Jan. 9, 2004**
a. Insufficient information on the threat	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
b. Insufficient number of available personnel	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
c. Insufficient training of personnel to implement assigned measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
d. Insufficient equipment and/or materials	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
e. Technological or other limitations of available equipment and/or materials	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
f. Insufficient facilities and/or space	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
g. Insufficient guidance to implement measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
h. Lack of federal government-wide coordination	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
i. Legal restrictions against taking certain protective measures	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK
j. Other challenges *(Please specify.)* _____ _____	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK	❒ Yes ❒ No ❒ DK

If you answered "yes" to any operational challenge in rows a through j in question 54 (Part A, Part B, or Part C) above, please answer question 55; otherwise, skip to question 56:

55. Briefly describe examples of operational challenges and the consequences of these faced during the alerts.

_____

_____

_____

_____

_____

56. During the HSAS Code-Orange alerts, was your state prevented from taking any specific protective measure because of a legal prohibition(s)?

1. ❒ Yes, state or territory was prevented from taking specific protective measures because of a legal prohibition(s)

2. ❒ No, state or territory was not prevented from taking specific protective measures because of a legal prohibition(s)

If you answered "yes" to question 56, please continue with question 57; otherwise, skip to question 58.

57. Please identify the specific HSAS Code-Orange alert(s), the protective measure involved, and the prohibition(s) that prevented its implementation, along with any relevant legal citation(s).

_____

_____

_____

_____

_____

58. If you have any comments regarding any of the issues covered in this questionnaire or have any other comments about protective measures, guidance, and costs for HSAS Code-Orange alerts, please use the space provided.

Thank you for your assistance.
Please return the questionnaire according to the instructions on page 1.

Agency Comments

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 8, 2004

William O. Jenkins, Jr.
Director, Homeland Security and Justice Issues
United States General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Jenkins:

Thank you for the opportunity to review and comment on the GAO Draft Report, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System (GAO-04-682).* We concur with the purpose of the report and generally concur with its contents. We fully agree that the provision of accurate and timely threat information is critical to the nation's security. Your report effectively discusses many of the important issues in this area and will be of great value.

While the report carefully notes when only one state or a particular entity reported or observed something, there are instances where the report uses the term "one state" or "one locality" as an example (as noted in the critical asset discussion for Liberty Shield). This could be misleading to some readers who might not look carefully and jump to the conclusion that one particular point of view is an accurate characterization of the whole.

With respect to the two recommendations, we concur subject to the comments provided:

Recommendation 1: The Under Secretary for Information Analysis and Infrastructure Protection should document communication protocols for notifying federal agencies and states of changes in the national threat level and for providing guidance and threat information to these entities, including methods and time periods for sharing information, to better manage these entities' expectations regarding the methods, timing, and content of information shared.

Response: Concur. I am pleased to report that the Department is moving forward and making significant progress in developing a thoughtful and balanced approach to documenting these protocols. Communication protocols must provide clear guidance to federal agencies and states. However, the Department must also retain appropriate flexibility in adapting threat communications to a variety of circumstances. The Department is moving deliberately to create such flexible communications protocols and continues to work with federal agencies and states in refining these protocols.

www.dhs.gov

Recommendation 2: The Under Secretary for Information Analysis and Infrastructure Protection should incorporate risk communication principles into the Homeland Security Advisory System to assist in determining and documenting information to provide to federal agencies and states, including, to the extent possible, information on the nature, location, and time periods of threats and guidance on protective measures to take in response to those threats.

Response: Concur. The Department is also committed to incorporating appropriate risk communications principles and procedures when we develop our written communications protocols. As the report notes, the cited risk communication procedures have primarily been developed in response to threats such as severe weather, traffic situations, and hazardous materials contamination. The report implies, and we fully agree, that terrorist threats are substantially different in nature and as such full application of the risk communication principles will be somewhat problematic in many situations. For example, it will be rare that we ever have the degree of specificity in threat information that we or the receiving audience would prefer.

Additionally, we have forwarded a number of technical comments, under separate cover, which we believe will add value to and improve the accuracy of this report.

We look forward to receiving your final report. If you or your staff have any questions or need additional information, contact John Daley at 202-282-8381.

Sincerely,

Anna F. Dixon
Director, Bankcard Programs
and GAO/OIG Liaison

2

GAO Contacts and Staff Acknowledgments

GAO Contacts

William O. Jenkins, Jr. (202) 512-8777
Debra B. Sebastian (202) 512-9385

Staff Acknowledgments

In addition to the individuals named above, David P. Alexander, Fredrick D. Berry, Nancy A. Briggs, Kristy N. Brown, Philip D. Caramia, Christine F. Davis, Michele Fejfar, Rebecca Gambler, Catherine M. Hurley, Gladys Toro, Jonathan R. Tumin, Tamika S. Weerasingha, and Kathryn G. Young made key contributions to this report.

Bibliography

Dory, Amanda. "American Civil Security: The U.S. Public and Homeland Security." *The Washington Quarterly*, vol. 27, no. 1 (2003-2004) 37-52.

Fischoff, Baruch. "Assessing and Communicating the Risks of Terrorism." *Science and Technology in a Vulnerable World*. eds. Albert H. Teich, Stephen D. Nelson, and Stephen J. Lita. Washington, D.C.: American Association for the Advancement of Science, 2003: 51-64.

Fischoff, Baruch, Roxana M. Gonzalez, Deborah A. Small, and Jennifer S. Lerner. "Evaluating the Success of Terror Risk Communications." *Biosecurity and Bioterrorism: Biodenfense Strategy, Practice, and Science*, vol. 1, no. 4 (2003) 255-258.

Gray, George M., and David P. Ropeik. "Dealing with the Dangers of Fear: The Role of Risk Communication." *Health Affairs*, vol. 21, no. 6 (2002) 106-116.

Mileti, Dennis S., 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.

Mitchell, Charles, and Chris Decker. "Apply Risk-Based Decision-Making Methods and Tools to U.S. Navy Antiterrorism Capabilities." *Journal of Homeland Security.* February 2004.

National Research Council. *Improving Risk Communication*. Washington, D.C.: National Academy Press, 1989.

Partnership for Public Warning. *A National Strategy for Integrated Public Warning Policy and Capability.* McLean, VA: May 16, 2003.

Partnership for Public Warning. *Developing a Unified All-Hazard Public Warning System*. Emmitsburg, MD: Nov. 25, 2002.

Ropeik, David, and Paul Slovic. "Risk Communication: A Neglected Tool in Protecting Public Health." *Risk in Perspective*, vol. 11, no. 2 (2003) 1-4.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00