Order Code RL32023

CRS Report for Congress

Homeland Security Advisory System: Possible Issues for Congressional Oversight

Updated December 28, 2006

Shawn Reese
Analyst in American National Government
Government and Finance Division

Prepared for Members and Committees of Congress

Homeland Security Advisory System: Possible Issues for Congressional Oversight

Summary

The Homeland Security Advisory System (HSAS), established on March 12, 2002, is a color-coded terrorist threat warning system administered by the Department of Homeland Security (DHS). The system, which federal departments and agencies are required to implement and use, provides recommended protective measures for federal departments and agencies to prevent, prepare for, mitigate against, and respond to terrorist attacks.

DHS disseminates HSAS terrorist threat warnings to federal departments, state and local agencies, the public, and private-sector entities. DHS, however, only provides protective measures for federal departments. This dissemination of warnings is conducted through multiple communication systems and public announcements.

HSAS has five threat levels: low, guarded, elevated, high, and severe. From March 2002 to the present, the HSAS threat level has been no lower than elevated, and has been raised to high seven times. The first time it was raised to high was on September 10, 2002, due to the fear of terrorist attacks on the anniversary of the terrorist attacks of September 11, 2001. The most recent time it was raised to high was on July 7, 2005, due to terrorist bombings of the London mass transit systems. DHS raised the threat level for mass transit systems only.

In the 109th Congress, the House of Representative's Committee on Government Reform's Subcommittee on National Security, Emerging Threats, and International Relations held a hearing on the HSAS, its threat codes, and public response to it. This hearing focused on the information DHS issued the public the seven times the HSAS threat level was raised from "yellow" to "orange."

While the need for terrorist threat warnings seems to be widely acknowledged, there are numerous issues associated with HSAS and its effects on states, localities, the public, and the private sector. These issues include the following:

- vagueness of warnings;
- lack of specific protective measures for state and local governments, the public, and the private sector;
- dissemination of warnings to states, localities, the public, and the private sector;
- coordination of HSAS with other federal warning systems; and
- cost of threat level changes.

This report will be updated as congressional or executive actions warrant.

Contents

List of Tables

Homeland Security Advisory System: Possible Issues for Congressional Oversight

On March 12, 2002, Governor Tom Ridge — then Director of the White House Office of Homeland Security (OHS), and formerly Secretary of the Department of Homeland Security (DHS) — announced the establishment of the Homeland Security Advisory System (HSAS). The HSAS is designed to measure and evaluate terrorist threats and communicate these threats to federal, state, and local governments, the public, and the private sector in a timely manner. Although HSAS is a nationwide system, it can also be used at a smaller scale to warn of threats against a state, city, critical infrastructure, or industry.[1] From inception to August 2004, the HSAS has been raised from "elevated" to "high" seven times (see **Table 2**).

The HSAS was developed by OHS using information collected from state and local first responders, business leaders, and the public. Following the March 12 announcement, the general public and the private sector were asked to provide comments on the system, with a deadline for comments on April 26, 2002.[2]

Within DHS, the Undersecretary for Information Assurance and Infrastructure Protection — as head of the Information Assurance and Infrastructure Protection directorate (IAIP) — is responsible for administering the HSAS. Specifically, IAIP is responsible for providing, in coordination with other agencies of the federal government, specific warning information and advice about appropriate protective measures and countermeasures to state and local government agencies and authorities, the private sector, other entities, and the public.[3]

Threat Conditions

The advisory system is based on five threat levels: low, guarded, elevated, high, and severe. Each level, with its corresponding identification color, indicates protective measures mandatory for federal departments and agencies.[4]

---

[1] Office of the White House Press Secretary, "Remarks by Governor Ridge Announcing Homeland Security Advisory System," press release, (Washington: March 12, 2002). Available at [http://www.whitehouse.gov/news/releases/2002/03/20020312-14.html],visited March 15, 2003.

[2] Ibid.

[3] P.L. 107-296, Title II, subtitle A, sec. 201(d)(7).

[4] U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002. Available at [http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html], visited June 3, 2003.

Table 1. HSAS Threat Levels

Threat Level	Risk of Terrorist Attack	Protective Measures
GREEN Low	Low	- Refine preplanned protective measures - Ensure personnel trained on HSAS and preplanned protective measures - Institutionalize a process for assuring all facilities are assessed for vulnerabilities and measures are taken to mitigate these vulnerabilities
BLUE Guarded	General	- Check emergency response communications - Review and update emergency response procedures - Provide information to public that would strengthen its ability to react to an attack
YELLOW Elevated	Significant	- Increase surveillance of critical locations - Coordinate emergency plans with other federal, state, and local facilities - Assess the threat and refine protective measures as necessary - Implement emergency response plans
ORANGE High	High	- Coordinate security efforts with federal, state, and local law enforcement agencies - Take additional protective measures at public events, changing venues, or consider cancelling if necessary - Prepare to execute contingency operations - Restrict facility access to essential personnel
RED Severe	Severe	- Increase or redirect personnel to address critical emergency needs - Assign emergency response personnel and mobilize specially trained teams - Monitor, and redirect transportation systems - Close public and government facilities

Source: U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002. Available at [http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html], visited Jun. 3, 2002.

DHS receives threat information from the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Drug Enforcement Agency (DEA), the Department of Defense (DOD), the Terrorist Threat Integration Center (TTIC), and other agencies. DHS uses this information to determine what terrorist threat level to set.[5]

Assigning a threat condition involves a variety of considerations, among which are the following:

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific and imminent?

[5] U.S. Department of Homeland Security, "Threats & Protection: Synthesizing and Disseminating Information," [http://www.dhs.gov/dhspublic/theme_home6.jsp], visited June 3, 2003; Office of the White House Press Secretary, "Fact Sheet: Strengthening Intelligence to Better Protect America," press release, Jan. 28, 2003. Available at [http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html], visited Mar. 4, 2004.

- How grave are the potential consequences of the threat?[6]

The DHS Secretary decides to raise or lower the threat level in consultation with the Homeland Security Council.[7] When the decision to change the threat level is made, DHS sends an electronic notification to state homeland security centers and to federal, state, and local agencies via the National Law Enforcement Telecommunications System (NLETS).[8] If circumstances and time permit, the DHS Secretary or his representative makes an advance conference call to alert governors, state homeland security advisors, and mayors of selected cities that the terrorism threat level has been changed and that electronic notification is about to be sent.

Homeland Security Council Membership

Secretary of Homeland Security
Secretary of the Treasury
Secretary of Defense
Attorney General
Secretary of Health and Human Services
Secretary of Transportation
Director of Office Management and Budget
Director of Central Intelligence
Director of Federal Bureau of Investigation
Director of Federal Emergency Management Agency
Chief of Staff to the President
Chief of Staff to the Vice President

Source: Executive Office of the President, "Fact Sheet: Homeland Security Council," press release, Oct. 29, 2001.

Following the first conference call and electronic notification via NLETS, DHS makes a second conference call to as many state and local law enforcement associations as can be reached. Following the second conference call, DHS initiates a secure call using the Business Roundtable's Critical Emergency Operations Communications Link (CEO COM LINK) to notify chief executive officers of the nation's top businesses and industries.[9] They are asked to dial into a secure conference call, and after each CEO goes through a multi-step authentication process

---

[6] U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002. Available at [http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html], visited June 3, 2003.

[7] U.S. Department of Homeland Security, "Threats & Protection: Advisory System," [http://www.dhs.gov/dhspublic/display?theme=29], visited May 12, 2003.

[8] U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges*, unprinted hearing of 108th Cong., 1st sess., May 1, 2003.

[9] CEO COM LINK is a secure telecommunications network that is activated during national crises and threats. Due to the sensitive nature of CEO COM LINK, a list of businesses and industries that participate in the system is not publicly available.

to ensure security, DHS or other federal officials brief them on developments and threats.[10]

Following the conference call via CEO COM LINK, DHS makes a public announcement through a press conference. Finally, critical infrastructure associations and other business groups are notified.[11]

Past Congressional Action

Several bills were introduced in the 109th Congress that addressed administration of the HSAS or alert notification of federal, state, and local entities; the private sector; and the public. Some of these included H.R. 2101,[12] S. 1753,[13] and H.R. 5001.[14] H.R. 2101 proposed to require DHS to establish a telephone alert network to warn the public of imminent or current emergencies caused by terrorist incidents and disasters. The warning would have provided information on appropriate protective measures.[15] S. 1753 proposed to establish a National Alert System administered by a National Alert Office. The National Alert Office would have been established within the National Oceanic and Atmospheric Administration, and the National Alert System would have provided a public alert on national, regional, and local emergencies requiring a public response.[16] H.R. 5001 would have required the DHS Undersecretary for Information and Analysis to implement changes to HSAS. The proposed changes included the requirement for every HSAS alert to be accompanied by information on the threat and appropriate protective measures. The HSAS warning would have been limited in scope for every warning to a specific region, locality, or economic sector believed to be at risk. Finally, H.R. 5001 would have required DHS to use some means of warning the nation without the use of color designations.[17]

---

[10] Business Roundtable, "Questions and Answers on CEO COM LINK," available at [http://www.brtable.org/document.cfm/760], visited May 12, 2003.

[11] U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges*, May 1, 2003.

[12] H.R. 2101, "To Amend the Homeland Security Act of 2002 to Direct the Secretary of Homeland Security to Develop and Implement the READICall Emergency Alert System," introduced by Honorable Kendrick Meek, May 4, 2005.

[13] S. 1753, "Warning, Alert, and Response Network Act," introduced by Honorable Jim DeMint, Sep. 22, 2005.

[14] H.R. 5001, "Homeland Security Information Sharing Enhancement Act of 2006," introduced by Honorable Rob Simmons, Mar. 16, 2006.

[15] H.R. 2101, Sec. 510.

[16] S. 1753, Sec. 102.

[17] H.R. 5001, Sec. 3.

Issues

Since the creation of the HSAS, a number of issues have arisen, among which are: the vagueness of warnings disseminated by the system; the system's lack of protective measures recommended for state and local governments, and the public; the perceived inadequacy of disseminating threats to state and local governments, the public, and the private sector; and how best to coordinate HSAS with other existing warning systems. In the 109th Congress, the House of Representative's Committee on Government Reform's Subcommittee on National Security, Emerging Threats, and International Relations held a hearing on the HSAS, its threat codes, and public response to it. This hearing focused on the information DHS issued the public the seven times the HSAS threat level was raised from "yellow" to "orange."[18] These issues and pertinent oversight options available to Congress are discussed below.

Vagueness of Warnings

The HSAS threat level has been raised seven times from "yellow" to "orange" since its activation on March 12, 2002. With each change, the Attorney General or DHS Secretary cited intelligence information but offered little specificity, except on August 1, 2004, when former DHS Secretary Ridge identified financial institutions in New York, Washington, DC, and New Jersey as being targeted by Al Qaeda. The only other time any specifics were given on possible terrorist attack targets was on February 7, 2003, when former DHS Secretary Ridge cited intelligence reports suggesting Al Qaeda attacks on apartment buildings, hotels, and other soft skin targets.[19] But in this case, no region, state, or city was identified as possible locations of attacks. Moreover, DHS has never explained the sources and quality of intelligence upon which the threat levels were based.[20]

Analysis and Options. Some observers have asserted that when federal government officials announce a new warning about terrorist attacks, the threats are too vague.[21] The vagueness that characterized the seven increases in the threat

---

[18] U.S. Congress, House Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, *Homeland Security Advisory System: Threat Codes and Public Responses*, Mar. 16, 2004.

[19] U.S. Department of Homeland Security, Office of the Press Secretary, "Threat Level Raised to Orange," press release, Feb. 7, 2003. Available at [http://www.dhs.gov/dhspublic/display?content=459], visited Mar. 4, 2004.

[20] Eunice Moscoso, "Government Hikes Terror Alert Status to 'High'," *Cox News Service*, Sept. 10, 2002, sec. Washington, General News. "Threats and Responses," *New York Times*, Sept. 11, 2002, p. A12. U.S. Department of Homeland Security, Office of Press Secretary, "Statement by Homeland Security Secretary Tom Ridge on Raising Threat Level," press release, May 20, 2003, available at [http://www.dhs.gov/dhspublic/display?content=741], visited June 4, 2003. Allyson Price, U.S. Department of Homeland Security, Congressional Liaison, telephone conversation with author, June 20, 2003.

[21] Dan Barry, and Al Baker, "Security Tighter in New York After Vague Terrorist Threat," *New York Times*, May 22, 2002. Philip Shenon, "Suicide Attacks Certain in U.S., Mueller Warns," *New York Times*, May 21, 2002.

condition in the past two years has raised concerns that the public may begin to question the authenticity of the HSAS threat level. Former Secretary Ridge told reporters on June 6, 2003, that DHS is worried about the credibility of the system. He said that the system needs to be further refined.[22]

Questions about the credibility of the threat, say other observers, might cause the public to wonder how to act or whether to take any special action at all. Some observers maintain that, without specific terrorist threat information, there is no basis for formulating a clear, easily understood public announcement of what appropriate protective measures to take.[23] Others assert that the continued lack of specific information arguably can lead to complacency.[24]

DHS officials cite the lack of specificity in intelligence as the reason for a lack of detailed information when the threat level is changed. Former Secretary Ridge has been quoted saying that the intelligence gathered so far has been generic; but he maintained that DHS, and the federal intelligence community that provides information about terrorist threats will improve. [25]

Option 1: Status Quo. Congress may view the evolution of the process, and decisions relating to it are best left to the Department. The lack of specificity may be due to the need to protect intelligence sources or a desire by DHS to issue warnings when threat information is generic, but nonetheless credible. Maintaining the status quo places the burden of responding to complaints about the vagueness of HSAS warnings and the critiques of DHS's perceived inability to give adequate terrorist attack warnings on the Department.

Option 2: Provide General Warnings. Due to the reported misunderstanding of HSAS threat levels, and the system's lack of recommended protective measures for state and local agencies, the public, and private-sector entities, Congress could consider directing DHS to issue general warnings concerning the threat of terrorist attacks *without* using the HSAS to notify state and local governments, the public, and the private sector. General warnings via public statements, in coordination with HSAS warnings to the federal government, would ensure that notices of terrorist threats are issued to state and local governments, the public, and the private sector. DHS chose to provide general warnings on September 4, 2003, and November 21, 2003. On September 4, 2003, DHS cited recent federal interagency reviews of information that raised concerns about possible Al Qaeda plans to attack the U.S. and U.S. interests overseas. This general warning listed aviation, critical infrastructure, WMD, and soft target threats, however, no specifics were given on possible location

---

[22] John Mintz, "Ridge Seeking Fewer Changes in Terror Alerts," *Washington Post*, June 6, 2003, sec. p. A11.

[23] Ross Kerber, "The Pallette of Warning Terror-Alert System Called Inadequate," *The Boston Globe*, May 31, 2003, Business section, p. C1.

[24] David A. Fahrenthold, "This Time, Orange Alert Seems Less So," *Washington Post*, May 22, 2003, p. B2.

[25] Ibid.

or type of attacks.[26] Another general warning was issued on November 21, 2003, when DHS cited a high volume of reports concerning the possible threats against U.S. interests during the Muslim holiday of Ramadan. These reports suggested Al Qaeda remained interested in using commercial aircraft as weapons against critical infrastructure; however, no location of possible attacks was specified.[27] This approach would address the concerns of some who have asserted that the HSAS causes misunderstanding at the state and local level, but it would not address the issue raised by those who say DHS does not give enough specificity in its terrorist attack warnings.

Option 3: Increase Specificity of Warnings. Were Congress to decide that the terrorist warnings issued by DHS are too vague and cause complacency in state and local agencies, the public, and the private sector, it might instruct DHS to use the HSAS to provide specific warnings to targeted federal facilities, regions, states, localities, and private sector industries to the extent that is possible. DHS has said that its goal is to have the capability to issue high alerts to designated cities, geographical regions, industry, or critical infrastructure.[28] This approach arguably would address the concerns about the perceived vagueness of HSAS warnings. One could argue that DHS is getting better at providing specificity with the latest alert issued on August 1, 2004.

Lack of Specific Protective Measures for State and Local Governments, the Public, and the Private Sector

The HSAS provides a set of protective measures for each threat condition, but these protective measures are identified only for federal agencies. DHS only recommends protective measures for states, localities, the public, or the private sector, however, the recommended protective measures are the same ones issued to federal agencies. These recommended protective measures provide no specificity for states, localities, the public, or the private sector.

Analysis and Options. HSAS silence with regard to protective measures for the public, the private sector, and state and local governments has drawn the attention of some interested observers. Early on, William B. Berger, President of the International Association of Chiefs of Police, testified before the Senate Governmental Affairs Committee that the lack of defined response protocols for state

---

[26] U.S. Department of Homeland Security, Office of the Press Secretary, "DHS Advisory to Security Personnel, No Change to Threat Level," press release, (Washington: Sept. 4, 2003). Available at [http://www.dhs.gov/dhspublic/display?content=1442], visited Mar. 8, 2004.

[27] Ibid., "Statement by the Department of Homeland Security on Continued Al Qaida Threats," press release, Nov. 21, 2003. Available at [http://www.dhs.gov/dhspublic/display ?content=3017], visited Mar. 8, 2004.

[28] David A. Fahrenthold, "This Time, Orange Alert Seems Less So," *Washington Post*, May 22, 2003, p. B2.

and local governments was an area of concern among local law enforcement agencies.[29]

Citing what some contend is a lack of DHS guidance on protective measures, non-federal entities are beginning to fill the perceived void. For example, the American Red Cross recommends protective measures for individuals, families, neighborhoods, schools and businesses at each of the HSAS threat levels.[30] Further, the State of Maryland has adopted the American Red Cross protective measures.[31]

Without federal guidance, some cities have adopted the following types of protective measures when the HSAS threat condition is raised to "orange":

- Surveillance cameras are activated.
- Law enforcement officers are not granted time off.
- Port security patrols are increased.
- Law enforcement officers are required to carry biological/chemical protective masks.
- First responders are placed on alert.
- Mass transit authorities broadcast warnings and instructions.
- Mass transit law enforcement officers increase patrols.
- Law enforcement agencies make security checks in sensitive areas, such as bridges, shopping centers, religious establishments, and courthouses.[32]

Option 1: Status Quo. The HSAS was designed for federal government use and Congress may deem the system adequate for the federal government. This approach can encourage states and localities to conduct threat and vulnerability assessments that would then assist in the development of specific protective measures geared to each state and locality's homeland security needs. On the other hand, this approach might cause confusion among states and localities in their attempts to prepare for terrorist attacks without federal guidance on protective measures.

Option 2: Federal Guidelines for State and Local Protective Measures. If Congress decided that there were a need for more guidance for states, localities, the public, and the private sector, it could either encourage DHS to establish HSAS protective measure guidance for states, localities, the public, and the private sector, or it could enact legislation mandating these activities. These protective measures

---

[29] U.S. Congress, Senate Governmental Affairs Committee, *Communities and Homeland Security,* unprinted hearing of the 107th Cong., 2nd sess., Dec. 11, 2001.

[30] American Red Cross, "American Red Cross Homeland Security Advisory System Recommendations for Individuals, Families, Neighborhoods, Schools, and Businesses," [http://www.redcross.org/services/disaster/beprepared/hsas.html], visited June 3, 2003.

[31] Maryland Emergency Management Agency, "Overview of the Maryland Threat Alert System and Guidance for Citizens, Schools, and Businesses," available at [http://www.mdsp.org/downloads/alert_public_info.pdf], visited June 10, 2003.

[32] David A. Fahrenthold, "This Time Orange Alert Seems Less So," *The Washington Post,* May 22, 2003, p. B2-3.

could match the federal government preparedness and response activities identified in the HSAS. This approach could provide federal government guidance on how to be prepared for and mitigate against a terrorist attack. A list of general protective measures for states, localities, the public, and the private sector may not, however, be as effective as state and locally devised protective measures.

Communication of Terrorist Threats to State and Local Governments, the Public, and the Private Sector

DHS uses a variety of communications systems to provide terrorist threat warnings to states, localities, the public, and the private sector. These systems include, for an example, conference calls, public announcements, CEO COM LINK, and NLETS, but DHS has no single communication system it uses to issue HSAS terrorist warnings.

Analysis and Options. On April 30, 2003, Jeffery Horvath, chief of the Dover, Delaware police department told the Senate Governmental Affairs Committee that his department has never received any official notification of a change of HSAS threat condition and has relied on the news media for this information. Michael J. Chitwood, chief of the Portland, Maine police department reiterated this point, and specifically identified the Cable News Network (CNN) as the news medium through which he receives notifications of changes in the HSAS threat level. He added that he received official notification from state authorities eight hours later. Fire chief Edward P. Plaugher of Arlington County, Virginia, also identified CNN as the primary source for notification of changes in the HSAS threat level.[33]

When testifying before the Senate Governmental Affairs Committee, former DHS Secretary Ridge said that the process for notifying state, and local agencies and authorities of a change in the HSAS threat condition needs improvement.[34]

The public is alerted to a change in HSAS threat condition through the news media, following a public announcement from DHS or media leak of the information. There is no Emergency Alert System (EAS) type communication activated to alert the public to a change in threat condition, so the public is not informed of the change until they monitor a public news source.[35]

Private sector alerts are through systems like CEO COM LINK and conference calls. DHS uses CEO COM LINK to notify private sector entities that participate in the system, and then makes calls to other critical infrastructure and business associations. This arguably results in a de facto prioritization of alerted private sector

---

[33] U.S. Congress, Senate Governmental Affairs Committee, *Homeland Security and First Responders,* 108th Cong., 1st sess., April 30, 2003.

[34] U.S. Congress, Senate Governmental Affairs Committee, *State and Local Homeland Security Challenges,* May 1, 2003.

[35] For information on the EAS, see CRS Report RL32527, *Emergency Communications: The Emergency Alert System (EAS) and All-Hazard Warnings*, by Linda K. Moore.

entities, which could result in a targeted private sector entity being attacked without a timely and effective alert.

Option 1: Status Quo. Congress may decide to allow DHS to deal with issues relating to HSAS advisories at this stage of HSAS development. This approach would encourage the continued utilization of the DHS terrorist threat communication systems. Since the HSAS is designed for federal government use, there may be no need for DHS to establish any other communication systems that disseminate changes in the HSAS terrorist threat levels. This would, however, not address the issues some have raised about the dissemination of HSAS advisories. Some would argue that before DHS establishes a specific system that communicates a change in HSAS terrorist threat levels, DHS needs to establish protective measures for states, localities, the public, and the private sector. This argument is based on the belief that there is little value in knowing of a change in the HSAS terrorist threat level in the absence of recommended protective measures.

Option 2: Revise the HSAS Notification Process. Congress could encourage, or enact legislation instructing DHS to revise the HSAS notification process to ensure that state and local law enforcement, and emergency management agencies are informed of changes of the terrorist threat level in a more effective and timely manner. This approach could address the problem of states and localities receiving the notification via the news media without first receiving official notification from DHS. This approach, however, would not address the issue of the public, and private sectors receiving timely notification of changes in the HSAS threat level.

A possible communications system DHS could use for disseminating threat level changes of the HSAS is the Homeland Security Information Network (HSIN). DHS announced an expansion of its HSIN on February 24, 2004. The HSIN is a computer-based counterterrorism communications network connecting DHS to all 50 states, five territories, and 50 major urban areas for a two-way flow of terrorist threat information. This communications system delivers real-time interactive connectivity among state and local partners with the DHS Homeland Security Operations Center (HSOC) through the Joint Regional Information Exchange System (JRIES). The community of users include State Homeland Security Advisors, State Adjutant Generals, State Emergency Operation Centers, and local emergency response providers.[36]

Coordination of HSAS with Other Warning Systems

HSAS is not the only federal warning system; eight separate systems exist to provide timely notification about imminent and potentially catastrophic threats to

---

[36] U.S. Department of Homeland Security, Office of the Press Secretary, "Homeland Security Information Network to Expand Collaboration, Connectivity to States and Major Cities," press release, Feb. 24, 2004. Available at [http://www.dhs.gov/dhspublic/display?content=3350], visited Mar. 4, 2004.

health and safety.[37] The types of hazards covered by these systems include severe weather,[38] contamination from chemical and biological weapon stockpiles scheduled for destruction,[39] terrorist attacks,[40] and any other emergency or hazard the President decides is significant enough to warrant public notification.[41]

Analysis and Options. Some argue for the consolidation of the existing warning systems into one "all-hazard" system. The Partnership for Public Warning is one organization advocating this type of consolidation.[42] Other organizations, such as the Federal Communications Commission's (FCC) Media Security and Reliability Council (MSRC) have recommended that the Emergency Alert System (EAS) should be established and implemented uniformly in all parts of the United States.[43] This enhanced EAS would be fed information from systems such as the HSAS.

Consolidation and coordination of these warning systems would present challenges to administering an "all-hazard" warning system. Some of the challenges include the administration of the warning system, interoperability of existing warning systems, and the involvement of industry.

Congress has directed the President to insure that all appropriate federal agencies are prepared to issue warnings of potential disasters to state and local officials, and that federal agencies provide technical assistance to state and local governments to insure that timely and effective disaster warnings are provided. The President is authorized to utilize or make available to federal, state, and local agencies the facilities of the civil defense communications system, or any other federal communications system, for the purpose of providing warnings to governmental authorities and the civilian population in areas endangered by disasters.[44] Federal agencies that currently administer warning systems include National Oceanic and Atmospheric Administration, Federal Communications Commission, Federal Emergency Management Agency, and Department of Defense. DHS is also responsible for coordinating and distributing warnings to the public.[45]

---

[37] For a summary of these warning systems see CRS Report RS21377, *Federal Emergency Warning Systems: An Overview*, by Shawn Reese.

[38] Advanced Weather Information Processing System (AWIPS), Emergency Managers Weather Information Network (EMWIN), National Oceanic and Atmospheric Administration (NOAA) Weather Radio (NWR), and NOAA Weather Wire Service (NWWS).

[39] Federal Emergency Managers Information System (FEMIS).

[40] Homeland Security Advisory System (HSAS).

[41] Emergency Alert System (EAS) and National Warning System (NAWAS).

[42] [http://www.partnershipforpublicwarning.org], visited June 10, 2003.

[43] Molly M. Peterson, "Experts Call For Uniformity in Anti-Terrorism Alert," *National Journal's Technology Daily*, May 28, 2003.

[44] 42 U.S.C. 5132.

[45] P.L. 107-296, sec. 102 (c)(3).

Existing warning systems are not interoperable. Reasons for this are:

- separate transmitting and receiving equipment;[46]
- separate standard message protocols;
- separate procedures for how warnings are input into dissemination systems; and
- separate training, exercising, and testing of the system.[47]

Since this technology is primarily researched, developed, and operated by private industry, the federal government could establish a relationship with the corporate suppliers of these technologies, a relationship to encourage development and effectively consolidate or provide the means to make the current warning systems interoperable.

Consolidating and coordinating federal warning systems, however, may cause a loss of concentration on the systems' traditional hazards. Mature warning systems have established alerting protocols and routines that, if consolidated, could become too broad, which may result in less effective warnings.

Option 1: Status Quo. Without congressional intervention, federal agencies responsible for issuing warnings will likely continue to narrowly focus on traditional hazards. This approach allows mature warning systems to continue communicating alerts and protective measures to an identified audience. Also, this approach would not incur an increased need for federal funding that would be required to update, test, and ensure compatibility of the systems. On the other hand, this approach would not address issues such as overlap of hazards (terrorist threat warnings of HSAS, and any presidential declared emergency warning issued by EAS), and the potential need to reach a wide audience through the use of multiple warning systems.

Option 2: Coordination and Update of Warning Systems. If Congress decided to address the issue of coordinating warning systems, it could require all federal agencies with hazard warning responsibilities, to establish, and develop a means for coordinating and updating existing warning systems. This approach could allow any warning of man-made or natural hazards to be issued on the full range of federal warning systems. This could ensure that a larger number of the state and local governments, the public, and private sector entities would receive the specific warning in an effective and timely manner. It would require a communication protocol to be developed that allowed one federal warning system to "talk" to a different system.

Updating of warning systems would not only include the ability of one system to "talk" to another, but could also include the ability of such systems as EAS to be

---

[46] This transmitting and receiving equipment include satellite antenna receivers, NOAA Weather Radio, AM and FM radio, television, 1610mHz radio receiver, dedicated computer networks, and dedicated telephone networks.

[47] National Science and Technology Council, Committee on Environment and Natural Resources, *Effective Disaster Warnings*, (Washington: November 2000), pp. 19-20; [http://www.fema.gov/news/newsrelease.fema?id=9985], visited Dec. 23, 2002.

transmitted on off-the-shelf telecommunication devices such as cellular phones. Given the widespread use of wireless communications, some observers have argued for warnings to be issued on wireless devices.[48] In the 108th Congress, S. 564 proposes such an approach that would facilitate the deployment of wireless networks in order to extend the range and reach of EAS. It would also ensure emergency personnel priority access to communications facilities in times of emergency.[49]

Option 3: Consolidation of Warning Systems. If Congress decided that there needs to be an all-hazard warning system, it could enact legislation requiring the federal agencies that have warning responsibilities to develop and implement such a system to warn states, localities, the public, and the private sector. This approach could ensure that any warning of a hazard — man-made or natural — would be disseminated to as many entities as necessary in a timely and effective manner. In the 108th Congress, two bills, S. 118, and H.R. 2537, propose such an approach to all-hazard warnings. The bills propose the establishment of a single all-hazard warning system that would ensure that states, localities, the public, and the private sector would be alerted to specific risks from man-made, and natural hazards.[50] This approach, however, would arguably require federal funding and effort to research, test, develop, and implement an all-hazard warning system.

Cost of Threat Level Changes

An increase in the HSAS threat level imposes both direct and indirect costs on federal, state, and local governments, the private sector, and the public. These costs include the increased security measures undertaken by states and localities, loss to tourism, and the indirect cost on the economy during a period of heightened threat level. In FY2003, the Office for Domestic Preparedness (renamed the Office of Grants and Training) Critical Infrastructure Protection grant program authorized state and local governments to use allocated grants to fund overtime costs associated with heightened threat levels.[51] According to Office of Grants and Training's (G&T) State Homeland Security Grant and Urban Area Security Initiative grant programs guidance, overtime is an authorized expenditure only associated with training or exercises. G&T Law Enforcement Terrorism Prevention program, however, does allow overtime costs specifically related to homeland security efforts.[52]

Analysis and Options. Local governments incur direct costs when they put in place additional security measures to deal with a higher threat condition.[53] An

---

[48] See footnote 35 on the Partnership for Public Warning.

[49] S. 564, sec. 2 (108th Cong.)

[50] S. 118, sec. 3 (108th Cong.), H.R. 2537, sec. 3 (108th Cong.)

[51] ODP's Critical Infrastructure Grant Program received no appropriations in FY2004.

[52] U.S. Department of Homeland Security, Office of Grants and Training, *Fiscal Year 2006 Homeland Security Grant Program: Program Guidance and Application Kit* (Washington: Dec. 2005).

[53] John Mintz, "U.S. Lowers Level of Terror Alert from Orange to Yellow; Intelligence (continued...)

example of this is the cost of random car searches at Atlanta's Hartsfield airport, which reportedly requires $180,000 a month for labor and signage. This cost is borne by Atlanta's police department and airport administration.[54] Because of the budget crisis that many states are experiencing, additional homeland security costs during heightened threat periods are seen as an additional fiscal burden. The costs associated with threat level changes have prompted many state and local officials to complain to DHS.[55] The United States Conference of Mayors released a 145-city survey that reported that during periods of heightened alert homeland security costs increased to additional $70 million a week.[56]

This increase in homeland security costs during heightened threat periods also has localities arguing for direct funding from the federal government. FEMA's Assistance to Firefighters is the only assistance that provide 100% of the funding to localities. G&T's Urban Area Security Initiative grants, however, first pass through the state, which causes some localities to complain about a delay in receiving funding.

Authorized program expenditures are another point of contention that states and localities have with homeland security funding and costs. All homeland security grant programs list authorized equipment and activities that grant allocations can be used to fund. States and localities may argue that these authorized expenditures do not address their specific homeland security needs.

These direct homeland security costs occur not only at the state and local level: when the threat level changes, federal departments and agencies have to adopt prescribed protective measures outlined in the different threat condition levels of the HSAS.

An indirect cost of a heightened threat level is the negative effect on tourism in cities perceived as potential targets of terrorism . It has been observed that increased threat levels and the need for heightened security have hurt the tourism industry of such metropolitan areas as Washington, DC, New York, and Chicago. Washington's Mayor Anthony Williams urged residents to be alert for suspicious activities. He also wanted the city to remain friendly, open, and safe to minimize the affects of the

---

[53] (...continued)
Suggests Less Risk of Attack," *Washington Post,* June 1, 2003, p. A4.

[54] Eunice Moscoso, "U.S. Lowers Alert to Yellow But Urges Caution," *Atlanta Journal-Constitution,* April 17, 2003, p. A3.

[55] John Mintz and Susan Schmidt, "Government Raises Terror Alert Level to Orange; Officials Say Intelligence Suggests Al Qaeda Attacks," *Washington Post,* May 21, 2003, p. A1.

[56] Andy Soloman, United States Conference of Mayors, "War, Threat Alert Increase City Security Costs by $70 Million per Week Nationwide," press release, March 27, 2003. Available at [http://www.usmayors.org/uscm/news/press_releases/documents/surveyrelease_032703.pdf], visited Aug. 4, 2003.

terrorist threat level on tourism.[57] D.C. Delegate Eleanor Holmes Norton agreed with the need to keep Washington open to tourism. She said that the city's tourism industry had been hurt by changes in threat condition, and that she feared some officials would overreact and shut down public buildings.[58] An example of the impact on tourism is the decision by some schools to cancel trips to Washington because of the threat of terrorist attack.[59]

Some municipal officials have had to make a costly decision between homeland security and tourism. Philadelphia's mayor, John F. Street, for instance, chose not to close down a street around Independence Hall after he received a call from DHS Secretary Ridge, who advised its closing. Mayor Street cited traffic and tourism concerns as the reason he chose not to respond to the recommendation.[60] Another indirect cost may be how a change in the HSAS threat condition affects the stock markets.[61]

Option 1: Status Quo. Congress may decide that the G&T grant programs adequately meet the needs of states and localities' homeland security costs due to a heightened HSAS threat. It may be an appropriate approach for ensuring the splitting of homeland security costs among the several tiers of government. This policy approach would not however, address such issues as the needs of some state and local first responder agencies, of hiring additional personnel, the loss of revenue generated by tourism due to an increased terrorist threat level, or the cost the economy incurs when the terrorist threat level is raised.

Option 2: Funding Through Established G&T Grant Programs. Should Congress decide that more funding needs to be provided to cover costs incurred by states and localities due to an increased terrorist threat level, it could consider establishing grant programs that specifically fund such terrorist prevention, preparedness, and mitigation activities as overtime pay for first responders and the purchase of equipment and personnel for the protection of critical infrastructure. In the 108th Congress, S. 1245 proposes such an approach by recommending that a consolidated homeland security grant program provide grant allocations for overtime expenses related to training, activities (as determined by the DHS Secretary) relating to an increase in the HSAS threat level, and emergency preparedness responses to a WMD incident.[62]

---

[57] Spencer S. Hsu, "Tightening the Security Net," *Washington Post*, March 19, 2003, p. A1.

[58] Vaishli Honawar, "Tours of Capitol Get Go-Ahead to Resume," *Washington Times*, April 24, 2003, p. B1.

[59] "New Hampshire News Notes," *Union Leader* (Manchester, NH), Mar. 21, 2003, p. B2.

[60] Alex Fryer, "Feds Guide, Can't Enforce Tight Security at Local Level," *Seattle Times*, May 24, 2003, sec. Domestic News.

[61] Steve Gelsi, "Dow Hits New 2003 High as Stocks Rally," *CBS Market Watch*, May 30, 2003, sec. Market Snapshot. "Stock Market Ticker," *Comtex News Network*, May 30, 2003. Eric Kirzner, "War Footing Keeps Markets In Retreat," *National Post's Financial Post & FP Investing*, March 3, 2003, p. FP 7.

[62] S. 1245, sec. 4 (108th Cong.)

Option 3: Funding Specifically for Heightened Threat Levels. Should Congress decide to provide funding for costs incurred during heightened threat level periods, it could appropriate funds, in addition to G&T homeland security grant programs, specifically to states, localities, and private sector entities to compensate for costs associated with a change in the HSAS threat level. In the 108th Congress, S. 728 proposes such an approach by compensating state and local law enforcement for costs associated with airport security.[63]

[63] S. 728, sec. 4 (108th Cong.)

Table 2. Homeland Security Advisory Threat Level Changes

(March 12, 2002 to Present)

Threat Level	Dates	Number of "Orange" Days	Reason for Threat Level Change to "Orange"
Elevated (Yellow)	Mar. 12, 2002 - Sep. 10, 2002	—	—
High (Orange)	Sep. 11, 2002 - Sep. 24, 2002	13	Terrorist threat information based on debriefings of a senior Al Qaeda operative.[a]
Elevated (Yellow)	Sep. 25, 2002 - Feb. 6, 2003	—	—
High (Orange)	Feb. 7, 2003 - Feb. 27, 2003	20	Intelligence reports suggesting Al Qaeda attacks on apartment buildings, hotels, and other soft skin targets.[b]
Elevated (Yellow)	Feb. 28, 2003 - Mar. 16, 2003	—	—
High (Orange)	Mar. 17, 2003 - Apr. 11, 2003	25	Intelligence reports indicated Al Qaeda would probably attempt to launch terrorist attacks against U.S. interests to defend Muslims and the "Iraqi people."[c]
Elevated (Yellow)	Apr. 12, 2003 - May 19, 2003	—	—
High (Orange)	May 20, 2003 - May 30, 2003	10	In the wake of terrorist bombings in Saudi Arabia and Morocco, the U.S. intelligence community believed Al Qaeda had entered an operational period worldwide, including attacks in the United States.[d]
Elevated (Yellow)	May 31, 2003 - Dec. 20, 2003	—	—
High (Orange)	Dec. 21, 2003 - Jan. 9, 2004	19	Increased terrorist communications indicating attacks.[e]
Elevated (Yellow)	Jan. 10, 2004 - Jul. 31, 2004	—	—
High (Orange)	Aug. 1, 2004 - Nov. 10, 2004	98	Terrorist threat intelligence indicates that Al Qaeda has been planning attacks against financial institutions in New York, Washington, DC, and New Jersey since pre-9/11.[f]
Elevated (Yellow)	Nov. 11, 2004 - Jul. 6, 2005	—	—
High (Orange)	Jul. 7, 2005 - Aug. 12, 2005	36	Due to terrorist bombings of London mass transit systems, DHS raised threat level for mass transit systems only.[g]
Total Number of "Orange" Days		**220**	

Source: U.S. Department of Homeland Security, Office of Press Secretary.

a. U.S. Department of Homeland Secretary, Office of the Press Secretary, "Director Ridge, Attorney General Ashcroft Discuss Threat Level," press release, Sept. 10, 2002. Available at [http://www.dhs.gov/dhspublic/display?content=150], visited Mar. 4, 2004.

b. Ibid., "Threat Level Raised to Orange," press release, Feb. 7, 2003. Available at [http://www.dhs.gov/dhspublic/display?content=459], visited Mar. 4, 2004.

c. Ibid., "Operation Liberty Shield: Statement by Homeland Security Secretary Tom Ridge," press release, Mar. 17, 2003. Available at [http://www.dhs.gov/dhspublic/display?content=519].

d. Ibid., "Statement of Homeland Security Secretary Tom Ridge Raising the Threat Level," press release, May 20, 2003. Available at [http://www.dhs.gov/dhspublic/display?content=741], visited Mar. 4, 2004.

e. CRS could find no DHS press release providing the reason for raising the threat level from "yellow" to "orange" on Dec. 20, 2003. Other news media sources cite the reason as "increased terrorist communications in recent days"; see Frank James, "U.S. Raises Terror Alert," *Chicago Tribune*, Dec. 22, 2003, p. 1.

f. U.S. Department of Homeland Security, Office of Press Secretary, "Remarks by Secretary of Homeland Security Tom Ridge Regarding Recent Threat Reports," press release, Aug. 1, 2004. Available at [http://www.dhs.gov/dhspublic/display?content=3870], visited Aug. 5, 2004.

g. U.S. Department of Homeland Security, Office of Press Secretary, "Transcript from Secretary Michael Chertoff Press Briefing on the London Bombings," press release, July 7, 2005.