



Statement of Shawn Reese
Analyst in American National Government
Congressional Research Service

Before

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

March 16, 2004

on
The Homeland Security Advisory System: Threat Codes and Public Responses

Mr. Chairman and Members of the Committee, I would like to thank you for this opportunity to appear before you today to discuss the Homeland Security Advisory System (HSAS), its threat level codes, and the public response to a threat level change. This statement addresses:

- ! how the system was developed;
- ! how the Department of Homeland Security (DHS) determines the system's threat level;
- ! how DHS disseminates the threat level;
- ! what information is disseminated with a notification of a change in the threat level;
- ! what protective measures are identified with each of the system's threat levels; and
- ! possible options for refining the system.

Background . On March 12, 2002, Governor Tom Ridge—then director of the White House Office of Homeland Security (OHS), and now Secretary of the Department of Homeland Security —announced the establishment of the advisory system. This system is designed to measure and evaluate terrorist threats and communicate threat information to federal, state and local governments, the public, and the private sector in a timely manner. Although it is a nationwide system, it could be used at a smaller scale to warn of threats against a region, state, city, critical infrastructure, or industry.¹ Since inception to present, the advisory system has never been lower than “Elevated—Yellow” and raised to “High—Orange” five times, with the nation being at “Orange” a total of 87 days.

The advisory system 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 private sector were asked to provide comments on the system, with a deadline for comments of 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 advisory system. Specifically, IAIP is responsible for providing, in coordination with other federal agencies and departments, 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

Determining the Threat Level . DHS receives threat information from a number of federal agencies, most notably 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), and the Terrorist Threat Integration Center. DHS uses this information to determine what Homeland Security Advisory System threat level to set.⁴

¹ Office of the White House Press Secretary, “Remarks by Governor Ridge Announcing Homeland Security Advisory System,” press release, (Washington: Mar. 12, 2002). Available at: <http://www.whitehouse.gov/news/releases/2002/03/20020312-14.html>, visited Mar. 8, 2004.

² Ibid.

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

⁴ U.S. Department of Homeland Security, “Threats & Protection: Synthesizing and Disseminating Information,” available at: http://www.dhs.gov/dhspublic/theme_home6.jsp, visited Jun. 3, 2003, and the Office of the White House Press Secretary, “Fact Sheet: Strengthening Intelligence to Better Protect America,” press release, (Washington: Jan. 28, 2003), available at: <http://www.whitehouse.gov/news/releases/2003/01/20030228-12.html>, visited Mar. 4, 2003.

Assigning a threat condition involves a variety of considerations, among which are the following:⁵

- ! 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?
- ! How grave are the potential consequences of the threat?

After considering these factors, DHS decides — in consultation with the Homeland Security Council — whether the threat level needs to be raised or lowered.⁶

Disseminating Threat Level Information . DHS Secretary Ridge stated before the Senate Governmental Affairs Committee, on May 1 2003, that when the decision to change the threat level is made, DHS sends an electronic notification to state homeland security centers, and federal, state and local agencies via the National Law Enforcement Telecommunications System (NLETS). If circumstances and time permit, however, 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.

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 major businesses.⁷

Following the CEO COM LINK conference call, DHS makes a public announcement through a press conference. Finally, critical infrastructure associations and other business groups are notified.⁸

On February 24, 2004, DHS announced the expansion of the Homeland Security Information Network (HSIN). The HSIN is a computer-based, counter-terrorism 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 through the Joint Regional Information Exchange System . The community of users includes State Homeland Security Advisors, State Adjunct Generals, State Emergency Operations Centers, and local emergency response providers.⁹ In the press release

⁵ U.S. President (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, March 11, 2002, available at: <http://www.whitehouse.gov/news/releases/2002/03/20020312-1.html>, visited Mar. 4, 2004.

⁶ U.S. Department of Homeland Security, "Threats & Protection: Advisory System," available at: <http://www.dhs.gov/dhspublic/display?theme=29>, visited Mar. 8, 2004. The Homeland Security Council is comprised of: the Director of the Office of Homeland Security; the Secretary of the Treasury; the Secretary of Defense; the Attorney General; the Secretary of Health and Human Services; the Secretary of Transportation; the Director of the Office of Management and Budget; the Director of Central Intelligence; the Director of the Federal Bureau of Investigation; the Director of the Federal Emergency Management Agency; the Chief of Staff to the President; and the Chief of Staff to the Vice President.

⁷ 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.

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

⁹ 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, (Washington: Feb. 24, 2004), available at: <http://www.dhs.gov/dhspublic/display?content=3213>, visited Mar. 4, 2004.

announcing the system's expansion, DHS did not mention the HSIN being used to disseminate Homeland Security Advisory System threat level changes. The HSIN could be used, however, as a consolidated communications system to announce threat level changes.

Information Disseminated When Threat Level Is Changed . When the advisory system's threat level is changed, DHS disseminates information to federal, state and local governments, the private sector, and the general public in a variety of ways (as discussed earlier in this statement). DHS has not publicly announced the information disseminated to federal, state and local governments, and the private sector during the five increases to "Orange" since March 12, 2002. DHS has, however, issued press releases that contained the following information:

Table 1. DHS Information on Reasons for HSAS Threat Level Changes
(March 12, 2002 to present)

Date of Threat Level Change	Reason for Threat Level Change
September 10, 2002	Terrorist threat information based on debriefings of a senior Al Qaida operative. ¹⁰
February 7, 2003	Intelligence reports suggesting Al Qaida attacks on apartment buildings, hotels, and other soft skin targets. ¹¹
March 17, 2003	Intelligence reports indicated Al Qaida would probably attempt to launch terrorist attacks against U.S. interests to defend Muslims and the "Iraqi people". ¹²
May 20, 2003	In the wake of terrorist bombings in Saudi Arabia and Morocco, the U.S. Intelligence Community believed Al Qaida had entered an operational period worldwide, including attacks in the U.S. ¹³
Dec. 20, 2003	Increased terrorist communications indicating attacks. ¹⁴

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

¹⁰ U.S. Department of Homeland Security, Office of the Press Secretary, "Director Ridge, Attorney General Ashcroft Discuss Threat Level," press release, (Washington: Sept. 10, 2002), available at: <http://www.dhs.gov/dhspublic/display?content=150>, visited Mar. 4, 2004.

¹¹ U.S. Department of Homeland Security, Office of the Press Secretary, "Threat Level Raised to Orange," press release, (Washington: Feb. 7, 2003), available at: <http://www.dhs.gov/dhspublic/display?content=459>, visited Mar. 4, 2004.

¹² U.S. Department of Homeland Security, Office of the Press Secretary, "Operation Liberty Shield: Statement by Homeland Security Secretary Tom Ridge," press release, (Washington: Mar. 17, 2003), available at: <http://www.dhs.gov/dhspublic/display?content=519>, visited Mar. 4, 2004.

¹³ U.S. Department of Homeland Security, Office of the Press Secretary, "Statement of Homeland Security Secretary Tom Ridge Raising the Threat Level," press release, (Washington: May 20, 2003), available at: <http://www.dhs.gov/dhspublic/display?content=741>, visited Mar. 4, 2004.

¹⁴ CRS is unable to identify a DHS press release providing the reason for raising the threat level from "Yellow" to "Orange" on Dec. 20, 2003. News media sources cited the reason as "increased terrorist communications in recent days." See: Frank James, "U.S. Raises Terror Alert," *Chicago Tribune*, Dec. 22, 2003, p. 1.

Protective Measures or Actions During Heightened Threat Levels . The advisory system threat levels, with corresponding identification colors, indicate protective measures mandatory for federal departments and agencies, as identified in Table 2.¹⁵

Table 2. HSAS Threat Levels and Protective Measures

Threat Level	Risk of Terrorist Attack	Protective Measures
GREEN Low	Low	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 W Elevated	Significant	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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, 2003.

DHS only recommends these protective measures for states, localities, the public, and the private sector. This may lead to confusion because these recommended measures are identical to those required of federal agencies. In addition these protective measures provide no specificity for actions to be taken by states, localities, the public, or the private sector. Also, some non-governmental organizations, such as the American Red Cross, recommend protective measures for individuals, families, neighborhoods, schools and businesses at each of the advisory system's threat levels.¹⁶

¹⁵ U.S. President, (Bush), "Homeland Security Advisory System," Homeland Security Presidential Directive 3, Mar. 11, 2002. Available at: <http://www.whitehouse.gov/news/releases/2002/03/20020312-15.html>, visited Mar. 4, 2004.

¹⁶ American Red Cross, "American Red Cross Homeland Security Advisory System Recommendations for Individuals, Families, Neighborhoods, Schools, and Businesses," available at: <http://www.redcross.org/services/disaster/beprepared/hsas.html>, visited Mar. 4, 2004.

The only actions DHS has advised the public to take during heightened threat levels is to remain vigilant, contact the FBI concerning any observed suspicious activity, and to continue daily life with a heightened sense of awareness.¹⁷

Options for Refining the Homeland Security Advisory System . Since the creation of the advisory system, a number of issues has arisen, two of which stand out: the vagueness of warnings disseminated by the system; and the system's lack of protective measures recommended for state and local governments, the public, and the private sector. These two issues and some oversight options available to Congress are discussed below.

Vagueness of Warnings . Some observers have asserted that when government officials announce a new warning about terrorist attacks, the threats are too vague.¹⁸ The lack of specificity of the five increases in the threat condition in the past two years has raised concerns that the public may begin to question the authenticity of the system's threat level. Secretary Ridge acknowledged to reporters on June 6, 2003, that DHS is worried about the credibility of the system. He stated that the system needs to be further refined.¹⁹

Questions about the credibility of the threat, some observers suggest, might cause the public to wonder how to act, or whether to take any special action at all. Other 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 should be taken.²⁰ Still others assert that the continued lack of specific information will arguably lead to complacency.²¹

DHS officials have cited the lack of specificity in intelligence as the reason for lack of detailed information when the threat level is changed. DHS 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.²²

Discussions of the advisory system have explored a number of options. These include:

Option 1: Status Quo . Some policy makers may view the evolution of the process and decisions relating to it as 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 the system's warnings and the critiques of a perceived inability to provide adequate terrorist warnings on the Department.

¹⁷ U.S. Department of Homeland Security, Office of the Press Secretary, "Operation Liberty Shield: Statement by Homeland Security Secretary Tom Ridge," press release, (Washington: Mar. 17, 2003), and "Statement by Homeland Security Tom Ridge on Raising the Threat Level," press release, (Washington: May 20, 2003).

¹⁸ Dan Barry, and Al Baker, "Security Tighter in New York After Vague Terrorist Threat," <http://www.nytimes.com/2003>, visited May 22, 2003. Philip Shenon, "Suicide Attacks Certain in U.S., Mueller Warns," <http://www.nytimes.com/2002>, visited May 21, 2003.

¹⁹ John Mintz, "Ridge Seeking Fewer changes in Terror Alerts," *The Washington Post*, June 6, 2003, 2003, p. A11.

²⁰ Ross Kerber, "The Palette of Warning Terror-Alert System Called Inadequate," *The Boston Globe*, May 31, 2003, p. C1.

²¹ David Fahrenthold, "This Time, Orange Alert Seems Less So," *The Washington Post*, May 22, 2003, p. B2.

²² Ibid.

Option 2: Provide General Warnings . Due to the reported misunderstandings of the system's threat levels, and the system's lack of recommended protective measures for state and local agencies, the public, and the private sector, Congress could consider directing DHS to issue general warnings concerning the threat of terrorist attacks *without* using the advisory system to notify these constituencies. General warnings via public statements, in coordination with the system's warnings to the federal government, may ensure that notices of terrorist threats are issued.

DHS chose to issue general warnings in September and November of 2003 without raising the system's threat level. On September 4, 2003, DHS cited recent federal interagency reviews of information that raised concerns about possible Al Qaida plans to attack the U.S. and U.S. interests overseas. This general warning listed aviation, critical infrastructure, weapons of mass destruction (WMD), and soft target threats. No specifics were given on possible target locations, type of attacks, or what actions should be taken to prepare for these attacks.²³ 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 holy season of Ramadan. These reports suggested Al Qaida remained interested in using commercial aircraft as weapons against critical infrastructure. DHS, however, did not advise on possible attack locations nor provide recommendations on what actions should be taken to prepare for possible attacks.²⁴ This option would address the concerns of some who have asserted that the advisory system 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 . To the extent more specific information was available, DHS could use the advisory system to provide specific warnings to targeted federal facilities, regions, states, localities, and private sector industries. DHS reportedly has said that its goal is to have the capability to issue high alerts to designated cities, geographical regions, industries, or critical infrastructure.²⁵ It is possible that, in at least some instances, DHS would conclude the costs of issuing specific alerts outweigh the benefits.

Lack of Specific Protective Measures for State and Local Governments, the Public, and the Private Sector . 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 and local governments was an area of concern among local law enforcement agencies.²⁶ Subsequently, the advisory system's silence with regard to specific protective measures has drawn the attention of a number of interested observers.

Without federal guidance, some cities have adopted the following types of protective measures when the system's threat level 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;

²³ 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.

²⁴ U.S. Department of Homeland Security, Office of the Press Secretary, "Statement by the Department of Homeland Security on Continued Al Qaida Threats," press release, (Washington: Nov. 21, 2003), available at: <http://www.dhs.gov/dhspublic/display?content=3017>, visited Mar. 8, 2004.

²⁵ Fahrenthold, "This Time, Orange Alert Seems Less So," p. B2.

²⁶ U.S. Congress, Senate Governmental Affairs Committee, *Communities and Homeland Security*, 107th Congress, 2nd sess., Dec. 11, 2001.

- ! mass transit authorities broadcast warnings and instructions;
- ! mass transit law enforcement officers increase patrols; and
- ! law enforcement agencies make security checks in sensitive areas, such as bridges, shopping centers, religious buildings, and courthouses.²⁷

There are at least two policy options that could be considered.

Option 1: Status Quo . The advisory system was designed primarily for federal government use; the system may be deemed adequate for the federal government. Some might suggest that states and localities should conduct their own 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. Moreover, this option fails to address protective measures for either the public or the private sector.

Option 2: Federal Guidelines for State and Local Governments, the Public, and the Private Sector . DHS, with congressional approval, could establish Homeland Security Advisory System protective measure guidelines for states, localities, and other entities. These protective measures could match the federal government preparedness and response activities identified in the system. 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, on the other hand, be as effective as state and locally devised protective measures.

²⁷ Fahrenthold, "This Time, Orange Alert Seems Less So," p. B2-3.