HOMELAND SECURITY ADVISORY SYSTEM: THREAT CODES AND PUBLIC RESPONSES

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 16, 2004

Serial No. 108–166

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

94–837 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

CONTENTS

HOMELAND SECURITY ADVISORY SYSTEM: THREAT CODES AND PUBLIC RESPONSES

TUESDAY, MARCH 16, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING
THREATS AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Turner, Schrock, Ruppersberger and Tierney.

Staff present: Lawrence Halloran, staff director and counsel; R. Nicholas Palarino, senior policy analyst; Robert A. Briggs, clerk; Jean Gosa, minority assistant clerk; and Andrew Su, minority professional staff member.

Mr. SHAYS. The Subcommittee on National Security, Emerging Threats and International Relations hearing entitled, "Homeland Security Advisory System: Threat Codes and Public Responses," is called to order.

After a series of vague warnings and alarms, the utility of the Homeland Security Advisory System [HSAS], is being questioned by State and local officials, first responders and the public. Even Department of Homeland Security Secretary Tom Ridge recently acknowledged the need to refine the code, five-color scheme that seems to me to be losing both its credibility and its audience.

Seeing no difference between a perpetually elevated state of risk, code yellow, and a high risk of terrorism at code orange, Americans risk becoming color blind to the signals that are supposed to prompt public awareness and action.

Since inception of the alert system 2 years ago, the threat level has been raised and lowered five times, flashing between yellow and orange whenever the volume of intelligence on al Qaeda went up or down, but the lack of specificity as to the time, place or nature of the perceived threats provided no basis upon which to calibrate appropriate public or private responses. As a result, governments and critical industries broadly increased security measures and incurred substantial costs. At the same time, exhortations to carry on as usual in the name of economic normalcy dulled any sense of urgency in the public at large.

The Homeland Security Act charges the Under Secretary for Infrastructure Protection to administer the HSAS and to provide specific warning information and advice about appropriate protective

measures and countermeasures to the public. The current system does not yet appear to meet the statutory requirements for specific information or specific advice. Whether due to an excess of caution about intelligence sources or a reluctance to ask for changed public behaviors and sacrifices, the codes and warnings in use today may be a better barometer of political realities than public safety risks.

When a blizzard or hurricane is forecasted, the public is not advised to be brave for America and stay in the eye of the storm, but when the threat of terrorism is elevated, citizens are advised to go about their lives as if no real peril approached. We need to make terrorism alerts at least as targeted and accurate as storm projections.

This week, the Select Committee on Homeland Security will consider legislation to improve Federal preparedness grants. A subcommittee of that bill directs the DHS Secretary to revise the alert system to include with each warning more specific designations of regions or economic sectors at risk. But other refinements could also add to the immediacy and the utility of any publicly disseminated terrorism threat codes.

So we asked our witnesses—and we're very grateful to all our witnesses—to discuss the principles of effective risk communication that should guide public alerts and warnings and to suggest how to improve the Homeland Security Advisory System. We appreciate their being here today, and we look forward to their testimony.

At this time, the Chair would recognize the distinguished vice chairman, Mr. Turner.

[The prepared statement of Hon. Christopher Shays follows:]

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
E-mail: hr.groc@mail.house.gov

Statement of Rep. Christopher Shays
March 16, 2004

After a series of vague warnings and alarms, the utility of the Homeland Security Advisory System (HSAS) is being questioned by state and local officials, first responders, and the public. Even Department of Homeland Security (DHS) Secretary Tom Ridge recently acknowledged the need to refine the five-color scheme that seems to be losing both its credibility and its audience.

Seeing no difference between a perpetually "elevated" state of risk – Code Yellow – and a "high" risk of terrorism at Code Orange, Americans risk becoming color blind to the signals that are supposed to prompt public awareness and action.

Since inception of the alert system two years ago, the threat level has been raised and lowered five times, flashing between yellow and orange whenever the volume of intelligence on al Qe'eda went up or down. But the lack of specificity as to the time, place or nature of the perceived threats provided no basis upon which to calibrate appropriate public or private responses. As a result, governments and critical industries broadly increased security measures and incurred substantial costs. At the same time, exhortations to carry on as usual in the name of economic normalcy dulled any sense of urgency in the public at large.

The Homeland Security Act charges the Undersecretary for Infrastructure Protection to administer the HSAS and to provide "*specific* warning information, and advice about appropriate protective measures and countermeasures" to the public. The current alert system does not yet appear to meet the statutory requirements for specific information or specific advice. Whether due to an excess of caution about intelligence sources, or a reluctance to ask for changed public behaviors and sacrifices, the codes and warnings in use today may be a better barometer of political realities than public safety risks.

When a blizzard or hurricane is forecast, the public is not advised to be brave for America and stay in the eye of the storm. But when the threat of terrorism is "elevated," citizens are advised to go about their lives as if no real peril approached. We need to make terrorism alerts at least as targeted and accurate as storm projections.

This week, the Select Committee on Homeland Security will consider legislation to improve federal preparedness grants. A section of that bill directs the DHS Secretary to revise the alert system to include with each warning more specific designations of regions or economic sectors at risk. But other refinements could also add to the immediacy and utility of any publicly disseminated terrorism threat codes.

So we asked our witnesses to discuss the principles of effective risk communication that should guide public alerts and warnings and to suggest how to improve the Homeland Security Advisory System. We appreciate their being here today and we look forward to their testimony.

Mr. TURNER. Mr. Chairman, thank you. I want to thank you for your continued efforts on reviewing the preparedness of our country and its appropriate response for the continuing terrorist threat that we have.

I appreciate you holding this hearing on an issue that is very important not just for first responders or those who have responsibility such as at our airports for looking at the issues of security but also for everyday Americans who look at the system for guidance.

I would characterize that most of the responses that I have received from airport security personnel, first responders or even people just out in the community or businesses that might have responsibility for protecting important infrastructure is that, as they look at this system, their question continues to remain, now what do we do, and I think that it is important for us to have the discussion as to how the system can be better correlated given a nexus, if you will, to specific responses from the community. Thank you.

Mr. SHAYS. I thank the gentleman.

At this time, I would ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record, and that the record remain open for 3 days for that purpose. Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. And without objection, so ordered.

At this time I would recognize our first panel: General Patrick Hughes, Assistant Secretary for Information Analysis, U.S. Department of Homeland Security; Mr. Randall Yim, Managing Director of Homeland Security and Justice Team, U.S. General Accounting Office; and Mr. Shawn Reese, Analyst in American National Government, Congressional Research Service.

What we'll do is we will start with you, General Hughes, after I swear you all in, and just say that I'm really looking forward to this first panel. I particularly appreciate, General Hughes, your candor when you testified before the Select Committee. I found your testimony on the issue that we're discussing very helpful, and I appreciated that, and I appreciate you being here as well as Mr. Yim and Mr. Reese.

As we do with all our witnesses, if you would stand, raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. Thank you. Note for the record all our witnesses have responded in the affirmative.

The way we'll proceed, General Hughes, is that we have a 5-minute clock. We will roll it over to the second 5 minutes and I would hope that you would stop sometime in between that second if you haven't within the first, but technically we allow 10 minutes for your testimony but hope it will be a little less.

Thank you. General Hughes, you're recognized.

STATEMENTS OF GENERAL PATRICK HUGHES, ASSISTANT SECRETARY FOR INFORMATION ANALYSIS, U.S. DEPARTMENT OF HOMELAND SECURITY; RANDALL YIM, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE TEAM, U.S. GENERAL ACCOUNTING OFFICE; AND SHAWN REESE, ANALYST IN AMERICAN NATIONAL GOVERNMENT, CONGRESSIONAL RESEARCH SERVICE

General HUGHES. Good morning, Mr. Chairman, Congressman Turner. I'd like to thank you very much for the opportunity to appear here today. I do think this is an important topic.

On March 11, 2002, President Bush created the Homeland Security Advisory System [HSAS], as a tool to improve coordination and communication among all levels of government and the private sector and, most importantly, perhaps, with the American public in the fight against terrorism. The advisory system is binding on the executive branch and suggested, although voluntary, for State, local, territorial and tribal governments and the private sector. The advisory system is the foundation for building a comprehensive, flexible and effective communications structure for the dissemination of information regarding the risk of terrorist attacks and protective measures to all levels of government, homeland security professionals and the American people.

The system, created by Homeland Security Presidential Directive 3 and now, pursuant to the Homeland Security Act of 2002, administered by the Department of Homeland Security, identifies a flexible framework for communicating, addressing and mitigating terrorist threats to the Nation utilizing a threat-based but risk-managed system. During periods of heightened concern, the framework provides the ability to change the threat condition on a national level but also affords the opportunity to target communications to particular geographic locales, industry sectors and other affected entities.

The latitude provided by HSPD–3 allows the Department to address unforeseen situations and continue to refine the advisory system as the need arises. This flexibility is critical to the success of the advisory system and essential to its effective implementation.

With the creation of the Department of Homeland Security on March 1, 2003, the advisory system evolved into a framework that married the analytic assets of the intelligence community, which includes the Department of Homeland Security, with the Department's unique responsibility to assess the Nation's vulnerabilities and implement protective measures.

Since its creation on March 11, the HSAS threat condition has been changed on five separate occasions. In each instance, the condition was raised from yellow to orange, but the circumstances surrounding each decision to elevate the threat condition varied.

We recognize that a decision to change the threat condition has significant economic, physical and psychological impacts on the Nation. Therefore, decisions made by the Secretary, in consultation with the Assistant to the President for Homeland Security, to change the threat condition are made only after careful consideration and close coordination with other Federal agency heads, including other members of the Homeland Security Council.

In the future, as the Department matures and our implementation of the Homeland Security Advisory System continues to evolve, we will work diligently to provide information that best suits the needs of Federal, State and local officials, the private sector and the public. We look forward to working with the Congress on ideas to improve the system.

HSAS is simply a tool, one of the many means to an end we're all working toward, which is to secure the homeland.

Thank you, Mr. Chairman, and I'll be pleased to answer any questions you may have.

Mr. SHAYS. Thank you very much, General.

[The prepared statement of General Hughes follows:]

Statement of Assistant Secretary Patrick M. Hughes
Information Analysis and Infrastructure Protection Directorate
U.S. Department of Homeland Security

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

March 16th, 2004
10:00 a.m.

U.S. Department of Homeland Security
Washington, D.C. 20528
202-282-8000

Good morning, Mr. Chairman and Congressman Kucinich. I would like to thank you, as well as the other members of the committee, for providing this opportunity for me to discuss the Homeland Security Advisory System.

On March 11, 2002, President Bush created the Homeland Security Advisory System ("HSAS" or "advisory system") as a tool to improve coordination and communication among all levels of government, the private sector and the American public in the fight against terrorism. The advisory system is binding on the executive branch, and suggested, although voluntary, for State, local, territorial and tribal governments, and the private sector. The advisory system is the foundation for building a comprehensive, flexible and effective communications structure for the dissemination of information regarding the risk of terrorist attacks and protective measures to all levels of government, homeland security professionals and the American people.

The system, created by Homeland Security Presidential Directive-3 (HSPD-3) and now, pursuant to the Homeland Security Act of 2002 , administered by the Department of Homeland Security ("DHS" or "the Department") identifies a flexible framework for communicating, addressing and mitigating terrorist threats to the nation utilizing a threat-based, risk-managed system. During periods of heightened concern, the framework provides the ability to change the Threat Condition on a national level, but also affords the opportunity to target communications to particular geographic locales, industry sectors or other affected entities. The latitude provided by HSPD-3 allows the Department to address unforeseen situations and continue to refine the Advisory System as the need arises. This flexibility is critical to the success of the Advisory System and essential to its effective implementation.

With the creation of the Department on March 1, 2003, the advisory system evolved into a framework that married the analytical assets of the Intelligence Community (which includes DHS) with the Department's unique responsibility to assess the nation's vulnerabilities and implement protective measures. Since its creation on March 11, 2002, the HSAS Threat Condition has been changed on five separate occasions. In each instance, the condition was raised from Yellow to Orange, but the circumstances surrounding each decision to elevate the Threat Condition varied.

We recognize that a decision to change the Threat Condition has significant economic, physical and psychological impacts on the nation. Therefore, decisions made by the Secretary, in consultation with the Assistant to the President for Homeland Security to change the Threat Condition are made only after careful consideration and close coordination with other Federal agency heads, including other members of the Homeland Security Council. Let me take this opportunity to provide some insight into the decision making process.

In the regular course of business, the Intelligence Community constantly reviews available threat information. When that information provides sufficient indication of a plan to execute a terrorist attack, the source and origin of the intelligence are further analyzed to determine the specificity and credibility of the information. It is only when the information received is both specific and credible that the Department takes appropriate action under the advisory system. Even then, the Threat Condition is not automatically raised to the next higher level. The Secretary has a range of actions available to him. These actions range from the issuance of advisories or bulletins up to a determination to change the Threat Condition.

There are instances when the volume and credibility of the intelligence reaches a level that the Department believes it should notify the public of the increased risk and the actions professionals are taking in response to the threat. Although this is a subjective standard, this concept was demonstrated when DHS elevated the Threat Condition from Yellow to Orange for Operation Liberty Shield. The decision to change the Threat Condition was based on intelligence reporting indicating Al Qaida's desire to attack the US in response to the US-led military campaign in Iraq. As you are aware, in this instance during a time of war, DHS recommended nationwide protective measures during a time of war.

Since then Advisory System has evolved as more specific threat information has become available and the Department's ability to communicate threat information and protective actions to those affected improved. One example of this evolution is the development of specific, audience-tailored communications tools to address specific threats and provide measures to be taken in response to threats or vulnerabilities. These products have enabled the Department to implement the advisory system in a more practical and flexible manner. In fact, since March 11, 2002, the protective posture of our nation has increased based on our refined ability to respond to specific information with targeted actions and prevention measures. As a result, today's Threat Condition Yellow is yesterday's Orange, effectively raising the threshold for changing the Threat Condition.

This evolution is best illustrated by the most recent Threat Condition change over the December 2003 holiday period. At that time, the Threat Condition was raised from Yellow to Orange based on intelligence reports indicating a substantial increase in the volume of threat-related reports from credible sources that al Qaida continues to consider using aircraft as a weapon and other threat reporting targeting numerous cities in multiple geographic locales. These were the most specific threat reports that we have seen thus far. Even though the national Threat Condition was lowered on January 9, 2004, DHS recommended that several industry sectors and geographic locales continue on a heightened alert status. In this case, DHS utilized the HSAS communications tools to provide specific recommendations to particular industry sectors and for particular geographic areas in response to specific threat information. For the first time since the creation of the HSAS, the Department lowered the national threat level

but recommended maintaining targeted protections for a particular industry sector or geographic locale.

In addition to the ability to change the Threat Condition, the advisory system also utilizes communications tools, defined as threat products, to provide more targeted and specific information to a broad or narrowly focused audience. In some cases, the protective actions taken by the affected entities affect decisions on raising or lowering the Threat Condition.

Threat products consist of warning and non-warning information designed to inform a particular audience about an existing threat or current incident. Two threat products used by the Department are Threat Advisories and Information Bulletins.

Threat Advisories contain actionable information about incident information or a threat targeting critical national networks, infrastructures, or key assets. These products may suggest a change in readiness posture, protective actions, or response that should be implemented in a timely manner.

Information Bulletins communicate information of interest to the nation's critical infrastructures and other non-governmental entities that does not meet the timeliness, specificity, or significance thresholds of threat advisories. Such information may include statistical reports, summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. Because these products are derived from intelligence they are generally communicated on a need-to-know basis to a targeted audience, such as the intelligence that is shared at both the classified and unclassified level with State, local and private sector officials. Together, these products provide a thorough, well-calibrated system to prevent terrorist attack. The evolutionary nature of the advisory system, and the authority resident in HSPD-3, enable the Secretary to utilize a variety of tools to address terrorist threats that may affect the United States.

Like other advisory systems, the success of the HSAS also depends upon our ability to work closely with Federal, State, and local officials, the private sector and the public. DHS not only communicates threat information but must also provide our partners with specific actions that can be taken at all levels to protect against the threat. The cornerstone of the HSAS is the protective measures that are implemented at each Threat Condition. The Federal government, States and the private sector each have a set of plans and protective measures that are implemented when the Threat Condition is raised. It is these protective measures and those specifically recommended in the HSAS communications tools that reduce the nation's vulnerability to terrorist attacks. However, it must be noted that while DHS encourages the adoption of the HSAS at the State and local level, the HSAS is intended to supplement, not replace, other systems currently implemented by State and local authorities and the private sector.

Prior to announcing a decision to elevate the Threat Condition, DHS communicates directly with its Federal, State, local, private sector and international contacts as appropriate. These communications provide specific information regarding the intelligence supporting the change in the Threat Condition. As appropriate for the audience, protective measures are developed and communicated with the threat information prior to a public announcement of the decision. While at a heightened Threat Condition, DHS maintains regular contact with State and local officials and provides regular updates. In the event that threats are targeted to particular cities or states, DHS provides those State and local officials with the most detailed intelligence information possible at both the classified and unclassified level.

It is important to note that threat information that is shared by the Department, and the ultimate raising of the Threat Condition, are actions primarily intended for security professionals at all levels of government and the private sector. However, in this post 9/11 world, in some cases threat information distributed by the Department or other Federal agencies eventually becomes accessible in the public domain. Based on this reality, the HSAS has again evolved to include a clear public explanation of the threat information to avoid misinterpretation of the information. When a change is made to the Threat Condition, DHS Secretary Tom Ridge includes guidance to the public regarding specific actions that can be taken in response to the threat. In addition to encouraging increased vigilance, DHS has recommended specific actions for the public including guidance for expediting their interactions with Transportation Security Administration airport screeners when traveling by commercial aviation. Although information is provided publicly regarding protective measures, it is important for the public to understand that DHS implements and recommends additional and more specific protective measures to State and local officials that are only disseminated to security professionals.

Increasing citizen and community preparedness is a Departmental priority. One year ago, Secretary Ridge launched a multi-faceted public information campaign in conjunction with the Ad Council, which has received over $150 million in donated advertising. The public information campaign directs callers to a web site or and "800" telephone number that provides critical information on emergency preparedness and different types of terrorist threats. Brochures on this effort are also distributed through Post Offices across the country and Salvation Army distribution centers as well as other private sector partners. The Ready information campaign works in concert with the American Red Cross and Citizen Corps, the department's initiative to mobilize volunteer leaders to increase their community's preparedness. The Ready.gov website provides specific actions individuals and families can take such as creating and testing a family emergency plan and assembling an emergency kit to ensure there are sufficient supplies available when needed.

Along with providing information to the public, DHS also works with State and local officials and the private sector in developing specific protective measures. The Department recognizes that each State, locality and private sector facility is unique and requires the development of different protective measures. For example, the protective measures required for and implemented by New York City are vastly different from the protective measures that Orange County, California will implement. In recognition of this difference, DHS communicates regularly with and provides technical advice to State and local officials to assist in the development of specialized and appropriate protective measures. Certain national law enforcement associations have also been awarded Homeland Security grant funding to further develop their own standard procedures for security measures to correspond with HSAS Threat Conditions.

DHS also works directly with critical infrastructure owners and operators to ensure that adequate protective measures and plans are in place to reduce the vulnerability to terrorism. Through this effort, DHS can deny terrorists the opportunity to use our infrastructure as a weapon. Let me offer two examples of this partnering:

DHS sends out teams consisting of DHS personnel and personnel from other agencies to critical infrastructure sites throughout the country to conduct site assistance visits. These visits are focused on identifying vulnerabilities and shared characteristics of that critical infrastructure sector element. After the visits, a report is prepared about the site and shared with local law enforcement, Federal law enforcement and the owner/operator of the facility. This procedure assists the owner/operator in identifying their vulnerabilities and adding appropriate protective measures.

However, it is not enough just to "look inside the fence" and identify the vulnerabilities of the site. We must work to remove the operational environment for a terrorist outside these facilities. To protect the area outside these critical infrastructure sites, DHS also conducts and prepares buffer zone protection plans. These community-based protection plans facilitate the development of effective preventive measures and make it more difficult for terrorists to conduct surveillance or launch an attack from the immediate vicinity of a high value or high probability of success site. The site assistance visits and buffer zone protection plans are just two ways in which DHS partners with critical infrastructure owners and operators to ensure that they have the best protective measures to guard against any terrorist incident.

Since the creation of the Department of Homeland Security, the HSAS has experienced an evolution from the preventative elevation of the threat level from Yellow to Orange during Operation Liberty Shield to the most recent threat specific elevation during the December 2003 holiday season. Over the past year, the system has been raised and lowered on three separate occasions, and each occurrence demonstrates that the Department's ongoing work to strengthen

the system has improved the implementation of the system specific to each emerging threat. The evolutionary nature of the System, and the authority resident in HSPD-3, enable the Secretary to utilize a wide variety of tools to address threats that may affect the United States.

In the future as the Department matures and our implementation of the HSAS continues to evolve, we will work diligently to provide information that best suits the needs of Federal, State and local officials, the private sector and the public. We look forward to working with the Congress on ideas to improve the system. HSAS is simply a tool and is one of the many means to the end we all are working toward which is a secure homeland.

Thank you Mr. Chairman. I would be pleased to answer any questions you may have.

Mr. SHAYS. Mr. Yim.

Mr. YIM. Chairman Shays, Vice Chairman Turner, members of the subcommittee, I thank you for this opportunity to participate in this hearing examining the Homeland Security Advisory System.

On February 4, 2004, Admiral Lloyd, the Deputy Secretary of the Department of Homeland Security, described the advisory system as a blunt instrument and a work in progress, pointing out for the first time this past December that the advisory system specifically identified economic sectors and geographical regions subject to heightened alerts. He and members of the House Select Committee on Homeland Security agreed that such specificity was critical to maintaining the credibility and usefulness of the system, and these remarks are consistent with the comments we at GAO have received from State and local governments and the private sector.

We last testified before this committee on February 3rd, describing the key characteristics of effective national strategies for homeland security and comparing and contrasting the extent to which several national homeland security strategies contain such characteristics. Our purpose was to assist in continual improvement and refinement of these strategies.

Just as with our previous testimony, we hope that our preliminary observations of the advisory system will identify key characteristics of effective public warning systems, issues and factors to be considered and balanced when determining what information is to be disseminated and assist in continued refinement of the system.

As with the national strategies, the true value of the advisory system will be the extent to which it is useful as guidance for, and actually used in implementation of prevention, vulnerability reduction, response and recovery measures by the relevant parties, including the general public.

Of course, as General Hughes noted, the Homeland Security Advisory System is not and should not be considered the only means by which threat and response information is disseminated. It is but one of many tools, as he said, used to increase our national preparedness. We hope that our testimony will be useful in sharpening this edge and increasing its effectiveness.

Specific threat and vulnerability information is received by Federal agencies and used by the executive branch in determining when to raise or lower the threat advisory systems. The key issues then are to what extent, when and with whom such information should be shared.

In your request, this committee suggested a link between sharing information and the ability of the recipients to act upon this information. While each threat advisory reflects a unique fact and circumstance influencing the what, the when and with whom issues, risk communication strategies that have evolved in numerous contexts have common characteristics that may be useful in assisting evolution of the advisory system. Effective risk communication can and should not only assist in prevention, but also in implementing actions to reduce vulnerabilities, prepare for enhanced response and recovery should an attack occur.

On the other hand, poor risk communication can lead to complacency, misallocation of valuable limited resources and be disruptive

and expensive for the affected parties. Preservation of credibility and public confidence are important considerations in any refinement of the advisory system.

My written statement describes the operations of the system, but, per your request, my oral remarks will focus on the types of information that should be conveyed to the general public.

Terrorist threats, as I said, present unique facts and circumstances and are still relatively unfamiliar to the general public. This uniqueness and unfamiliarity must be acknowledged and recognized in devising refinements to the system. If these terrorist threats are unique, then unique or specific information should be provided to the extent that it's available.

Most would agree that the refinements in the system this past November were more useful, focusing on specific sectors and geographic areas, but unlike more familiar advisories about weather, as you mentioned, Mr. Chairman, or infectious disease, specific terrorist threat warnings may allow terrorists to alter their tactics or targets in response or increase general anxiety in the public for those clearly not at risk. So we must acknowledge and account for the fact that some information available will not be widely distributed.

Further, due to the nature of terrorist organizations and the types of threats, threat information may be vague, may be limited or simply unavailable. Thus, the general public needs to be educated so that they understand that false alarms arise from inherent uncertainty rather than from poor professional practice, that to a certain extent false alarms are inevitable, and we must guard against a cumulative apathy among the public during what I would term prolonged periods of preparedness.

Finally, we have to acknowledge a fact of life, that, despite everyone's best intention, the threat of terrorist activities will cause both rational and not-so-rational responses. So, despite our best efforts, there will be unintended social, psychological and economic consequences. But, as an important point, when designing effective risk communication strategies, that we understand and acknowledge that these effects will occur and design our strategies accordingly to convey information to those receptive, and have the ability to act upon that information, while at the same time understanding that some will receive this information and act or not act upon it in less than optimal ways.

So what does this mean for refinement of the advisory system? As this subcommittee and the chairman has acknowledged, we want to convey information that will increase our national preparedness. That is, we expect some action as a result of our warning. There has to be, then, some connection, some nexus between the information to be shared and the ability and receptivity to take positive action, forcing our planners not only to be intelligence and fact-based providers but, to a certain extent, social and psychological scientists, quite a difficult task.

Risk communication experts generally agree that effective warnings should specify the nature of the threat, when and where it is likely to occur and over what time period, provide guidance or actions to be taken and perhaps, above all, assure that the information is consistent, accurate, clear and provided frequently.

This is much easier said than done for terrorist warnings, but if we focus on the nexus between information and the ability to act and the receptivity to act upon it, then some patterns emerge, such as more specific information can and should be provided to those specially trained to receive and act upon the information such as firefighters, emergency responders, and we've seen that in the hazardous materials area where much more specific information is provided to firefighters in case they must enter a building that contains potentially toxic materials.

For the general public and the private sector, State and local governments, the same principles can apply. Specific information that is useful in making risk management decisions should be conveyed so that the resources and intentions are focused on the highest priorities, and the capabilities of these parties to act are enhanced.

For example, there may be vague threat information about a public sporting event. An individual may still wish to attend, but take some simple precautions such as notifying others that they are attending, carrying contact phone numbers or just simply thinking about the evacuation or escape routes in the event of an emergency. A private business may wish to review and update its emergency shutdown procedures or be sure that people are current on the evacuation routes.

These are all examples of sharing information that is useful for, linked to the capability of the recipients to receive and act upon that information, resulting in what Admiral Lloyd calls a tactically actionable product.

The linkage then between information and capability to act appear to be what other risk communication experts in the second panel discuss when they talk about the psychology of risk and risk management perception related to control, to choice, the potential for personal impact, the risk benefit tradeoffs and trust and a focus on the link on capabilities between information. I think it really affects the trust issue, trust that the information is accurate and useful, trust that the information is being conveyed to those with expertise and the ability to act upon it, like the law enforcement and emergency responders, and trust that the false alarms are due to inherent uncertainty in dealing with terrorist threats rather than a lack of competence. As I said, the credibility is of utmost importance to maintain.

In closing, let me end with a few suggestions. If we want to foster a closer link between information sharing and capabilities, then we need to do a better job of capability assessment. We do not have a good inventory on the types of infrastructure, equipment, people skills that can be brought to bear in a major homeland security emergency or for the major missions of prevention, response and recovery vulnerability assessment, either horizontally across the Federal Government or vertically between the Federal, State, local and private sector.

Homeland Security Presidential Directive 7 was not designed to make changes in the advisory system. However, it mandates that the Department and other Cabinet agencies inventory, use high techniques to map and model, again, to get a basic understanding of the capabilities that the existing infrastructure within the coun-

try can be brought to bear should a crisis arise or we wish to prevent a terrorist attack. That type of modeling inventory should be combined, again, as one of many tools with refinements of the Homeland Security Advisory System.

Finally, if we focus on capabilities, let us not underestimate the capabilities of the general public. I, like many others, continue to be astounded and grateful for the capabilities demonstrated by the public during September 11th, during the days following, from acts of heroic rescue to incredible acts of kindness during response and recovery, to heroism in preventing even greater acts of terrorism.

So I would close by just noting that the capabilities of the general public may be much greater than we think, so let's not shortchange the public by assuming too little about the types of information that are useful for increasing our collective national preparedness.

Thank you, Mr. Chairman; and I'd be pleased to answer any questions.

Mr. SHAYS. I thank you.

First, the substance of your statement, as was the substance of General Hughes, was quite outstanding, but I have never in my 16 years looked at a statement so well organized and so consumer friendly the way you have done it. I'm going to take this statement and give it to my staff as an example of how I would like to see its work done. It's really extraordinary.

Mr. YIM. Thank you, Mr. Chairman.

Mr. SHAYS. Very, very helpful.

Mr. YIM. I give great credit to my staff. I'm just the spokesperson.

Mr. SHAYS. Well, I understand, but you all have developed a system of trying to make things clear, and it's very helpful and an excellent statement as well.

[The prepared statement of Mr. Yim follows:]

United States General Accounting Office

GAO

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

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

HOMELAND SECURITY

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

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

March 2004

GAO
Accountability · Integrity · Reliability

Highlights

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

HOMELAND SECURITY

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

Why GAO Did This Study

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

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

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

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

What GAO Found

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

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

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

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

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

Mr. Chairman and Members of the Subcommittee:

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

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

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

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

Today, my testimony will focus on

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

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

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

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

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

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

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

Background

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

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

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

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

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

How the Homeland Security Advisory System Currently Operates

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

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

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

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

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

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

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

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

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

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

[7]GAO-04-453R.

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

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

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

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

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

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

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

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

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

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

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

- Specific information on the potential threat including, to the greatest extent possible,
  - the nature of the threat,
  - when and where it is likely to occur, and
  - over what time period, and
- Guidance on actions to be taken.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Information Currently Shared by DHS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[31]GAO-04-453R.

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

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

Similarly, one state official noted that receiving more specific information about the type of threat—against bridges and dams, for example—would enable the state to concentrate its response in those areas, a more effective approach than simply blanketing the state with increased general security measures. One local official also noted that specific information about the location of a threat should be provided to law enforcement agencies throughout the nation—not just to localities that are being threatened—thus allowing other local governments to determine whether there would be an indirect impact on them and to respond accordingly. Additionally, according to a national survey on the public's priorities regarding receipt of terror-related information, the public wants honest and accurate information about terror-related situations, even if that information worries them.[33]

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

Concluding Observations

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

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

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

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

GAO Contacts and Staff Acknowledgments

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

Mr. SHAYS. Mr. Reese.

Mr. REESE. Mr. Chairman, Vice Chairman Turner and members of the subcommittee, I thank you for inviting me to testify before you today.

The committee asked me to discuss four points concerning the Homeland Security Advisory System: the process the Department of Homeland Security uses in determining the threat level; the notification process that the Department uses to disseminate a change in the threat level; the information provided to the public when the threat level changes; and the lack of protective measures for States, localities, the public and the private sector.

As General Hughes said, Secretary Ridge, then Director of the White House Office of Homeland Security, announced the establishment of the Homeland Security Advisory System on March 12, 2002. This advisory system has five threat levels. At each threat level the system prescribes protective measures that are mandatory for Federal agencies but only recommends them to State and local governments.

Since the inception to the present, the system has never been lower than elevated or yellow, and has been raised to orange five times, with the Nation being at orange for a total of 87 days.

If I correctly understand it from statements by Secretary Ridge, the process DHS uses in determining the system's threat level has three steps: First, DHS receives intelligence reports from a variety of entities within the U.S. intelligence community.

Second, upon receiving these reports, the Department considers the following: whether the information is credible, whether the information is corroborated, whether the reported threat is specific and imminent and the gravity of the potential consequences of the threat.

Third, in consultation with the Homeland Security Council, the Department decides whether the threat level needs to be raised or lowered.

Once the decision is made to raise the threat level, DHS notifies State and local governments, the public and the private sector through a variety of communications systems. State and local governments receive notification through such systems as the National Law Enforcement Telecommunications System and conference calls to Governors, State homeland security advisers and mayors of selected cities. Selected major industries receive notification through such systems as the critical emergency operations communications link; and, finally, the public is notified through a DHS public statement. These public statements provide general reasons for the change in threat level, but they do not offer specifics.

The Department has said that intelligence reports indicate an increased probability of a terrorist attack. In the written statement I submitted, there is a table that lists the reasons and dates of the five changes from yellow to orange. The only time DHS has provided specifics on possible targets was on February 7, 2003, when the Department stated that intelligence reports suggested possible al Qaeda attacks on apartment buildings, hotels and soft-skinned targets, but no geographical location was identified.

This leads to my final point, which is what some say is a lack of clear guidance on protective measures for States, localities, the public and the private sector.

As I noted earlier, the advisory system has mandatory protective measures for Federal departments. These measures, however, are only recommended for States and localities, but these measures do not address the issue of what actions the public should take during heightened threat level. The only recommended actions the public received during the five orange alerts was to remain vigilant, report suspicious activities to the Federal Bureau of Investigation and to carry on with their daily lives with a heightened sense of awareness.

In summary, the advisory system in its present form does not provide specifics on why the threat level has been changed, nor does it provide clear guidance on actions States, localities, the public and the private sector need to take during a heightened threat level.

I thank you, Mr. Chairman and I will welcome any questions you or the committee might have.

Mr. SHAYS. Thank you very much, Mr. Reese; and we appreciate the work of the Congressional Research Service.

[The prepared statement of Mr. Reese follows:]

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

---

[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.

response providers.[9] In the press release 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]

[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.

[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

(continued...)

Date of Threat Level Change	Reason for Threat Level Change
Dec. 20, 2003	Increased terrorist communications indicating attacks.[14]

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

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	- 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, 2003.

[13] (...continued)
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.

[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.

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]

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

---

[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.

[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.

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.

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,

---

[22] Ibid.

[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.

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;
- 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.

---

[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.

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

Mr. SHAYS. General, I particularly want to thank you for participating with this panel instead of just asking to be separate. That is very appreciated. I think we'll be able to understand this issue better because of it.

We are going to recognize Mr. Turner, Mr. Schrock and then myself for 10 minutes, 5 minutes and then a rollover for 5 additional minutes. If someone is asked a question and you want to respond to it as well, even if you were not requested to answer, please feel free to jump in as well.

OK. Mr. Turner, you have the floor.

Mr. TURNER. Thank you, Mr. Chairman.

Being a former mayor, I talk a lot to individuals who are responsible for local protective functions, police, fire or important infrastructures such as water systems. Also, the security personnel at the airport. What I hear from them, which is echoed in many of your statements, is the lack of direction upon the elevation of the threat level.

In the materials that we have there are obviously some protective measures that are listed, but many times there is a lack of specificity as to what one should do that has responsibility for important infrastructure. For example, local water authority. The threat level was raised. They know they need to increase their security. They need to do something, but they don't really know what necessarily to do. They don't know if enough, if it's not enough. Also, then they worry when the threat level is lowered that lessened security during a time of lowered threat may not really be in the best interest of protecting the community or in responding to the threat.

While one of you acknowledged that the lowest we had gone is yellow, which is elevated—but even in looking at the protective measures between yellow and orange, orange says restrict facility access to essential personnel. Yellow doesn't necessarily provide that.

Mr. Yim and Mr. Reese, could you please talk for a moment about the issue of that lack of nexus, Mr. Yim, that you had mentioned for advice to the local officials and their important infrastructures, if you have knowledge of some of the things that they're doing and the lack of direction that they're receiving on what they should be doing. Because I know this is very troubling to them.

Then, General Hughes, if you could speak as to, you know, why don't we have more specific standardized recommendations to them, more specific direction that—as this code goes up and down, where they might feel that, one, they're rising to the obligation or, two, that they have, you know, a greater direction as to what it means. Mr. Yim.

Mr. YIM. Thank you, Mr. Turner.

I think the general perception is that the color-coded system is too generic; and, as a result, it's not refined enough to be able to provide that specific information. So as we evolve the system, we can conceive of different people with different expertise receiving different information instead of everyone receiving exactly the same. That would go a long way toward curing some of the specificity issues.

So, for example, as we mentioned, if there is to be some link between the types of information you receive and your ability to react and respond to it, then we can or should be providing more specific information to the firefighters, to the first protectors, that are trained to use that information, allocate the resources appropriately and to act upon it.

I'm sure that we can devise some manners when we have security issues surrounding how much information to disclose, if we're limiting the recipients, that perhaps the Federal Government would be a bit—feel a bit more comfortable conveying more specificity to those targeted-type groups.

I think it's important, however, that one of the reasons that we tend to default to more general warnings is often we don't have a good sense of what exactly are the capabilities of the recipients of that information to respond. As I said, we have not done a good assessment nationally of the capabilities of the respective State and local governments to not only respond, but also to prevent terrorist attacks, to assess their vulnerabilities and reduce their vulnerabilities.

So I think, to a certain extent, both the assessment and the warnings will evolve hand in hand as we have a greater sense of the capabilities that the State and local and private sector and public can bring to bear in prevention and response. As that capability evolves over time, as people get more sophisticated in what they need to do, then I think the warnings also need to evolve and provide greater information to them. We're clearly not there yet. We don't have a good sense, and we default then to, as I said, this generic warning system, which almost universally people feel is not that useful.

The only other point I would make on specificity is that let's not go too far in specificity in limiting the recipients of that information. We should not presume who would find the information useful. For example, if we want to target geographical areas and limit the information to just those residents of New York, we may miss people that are doing business via IT or remotely with New York or who are planning a trip to New York that may want to make risk-management decisions based on threats to other geographical areas.

So there is going to be a difficult balance between providing generic information that raises the country's general sense of alert, because we can't always anticipate who would be affected by that information, and providing specific information to those trained to use their resources wisely and to act upon that information.

Mr. REESE. As we've all stated, numerous State and local officials have said that the information that's been provided to the threat level change has been generic. Secretary Ridge has also stated that sometimes the information has seemed generic but there has been a need to provide information to the general public and to selected critical infrastructure and the private sector and State and local officials. There is a need to announce a change in the threat level.

I am not privy to any information that the Department sends out other than what is sent in the public statements to the public, so I will just kind of focus on that.

There seems to be a desire to get a one-glove-fits-all situation, or protective measures that if it works well in New York then it should work well in Los Angeles. I would say the disadvantage to DHS giving specific protective measures or information would be that it doesn't foster State and local governments possibly to do their own threat and risk assessments.

So I think, on one hand, we do want more information to be sent out so people can properly prepare, but on the other—and, as you know, CRS, we try to do the advantages and disadvantages. We want to ensure that we don't hamper State and local officials.

Another issue that State and local officials bring up is when the threat level goes up there's an increase in cost that the government incurs. So if it's a specified threat that is geographically targeted, then, naturally, we'll—and we'll use New York City as an example. If New York City is targeted, naturally, we wouldn't want Los Angeles to incur costs more than they need, but it is universally—with the State and local officials and individuals that work in emergency management, there does seem to be a lack of information that causes people to question what they're supposed to do and when they're supposed to do it.

Mr. TURNER. General Hughes.

General HUGHES. Well, first, I found Mr. Yim's and Mr. Reese's comments to be instructive in several ways. I thought they were very good. But the issue that I'd like to point out to you is the struggle to try to find balance between greater specificity and broader information available to the public on the one hand and on the other hand generating some kind of a reaction in the official State and local, private sector environment and, by the way, in the American public that is broad enough to encompass the general threat; and that's what we strive for at the Department of Homeland Security.

I will just make the flat statement that, as we now administer this system, it is specific, and we do communicate specifically with places that are specifically targeted. We do not do that in the public domain in general for obvious reasons. If we did that in the public domain, we would then give away our knowledge base and we would probably end up disclosing some of our protective and defensive measures. In my view, that would be a very foolhardy thing to do, so——

Mr. TURNER. So, General, are you saying that communities that don't have a specific directive with respect—should consider themselves lucky in that they are not faced with the imminent threat that you're obviously trying to manage?

General HUGHES. Once again, I urge you to have in your minds somehow a balance. But, generally speaking, I think what you just said is right, that the nature of the threat that's communicated to the country at large versus the nature of the threat that is communicated specifically to places, times, circumstances that we have information about are sometimes very different.

But if I may explain two issues here. The nature of the threat can be specific and often is and not rise to the level that requires us to change the broader threat condition. That is, in effect, this morning there are threats in the United States today about specific cities, specific places, specific events and specific conditions, but

this morning they have not risen to a level of concern and to a due consideration for broader change across the country. When they do, as they did in December 2003, then after due consideration we need to make the broader change.

And I have to explain the last piece of this idea, sir. When something is threatened in New York City, the idea seems to be that you can divorce that from events in Seattle, but you cannot. The two are inextricably interconnected now electronically, by transportation, by the features of our social order. We are interdependent; and, indeed, the vector that the threat comes from may not be precisely known.

In some cases, when we have to raise the nature of the threat to encompass the Nation, the country, we're doing so because we may lack specificity, but we have enough general information to cause us to rise to that level of concern.

I'd like to just close my answer on this issue by stating that the idea that these colors, the threat conditions that we use here, stand alone without any interior specific actions is a flawed viewpoint. We do have many different variations on the theme of specific, direct communication and coordination and specific activities that we can undertake within any of these general threat conditions here on this chart.

So I just—I wanted to get that point across, that the basic premise here and some of our conversation seems to me a little flawed.

Mr. SHAYS. Can you make that last point again? I'm missing it.

General HUGHES. Yes, sir. We seem to refer to these colors and the conditions they represent as if they are singular, and they are not. Each of them has a complex background, some of it based upon judgment and specificity of the conditions. So if Secretary Ridge, as an example, in due consultation reaches a decision to raise the threat level from yellow to orange, there are very specific acts based on intelligence that cause that to happen.

There may also be a broad general condition that results from that. The color level is an example, manifestation of the broad general condition, but the specificity interior to that change is very precise. We talk to people directly. We give them the knowledge that we have in some form. Often, by the way, right now especially in this last raised alert condition, we were able to give information that is very closely held in the Federal Government to State and some local authorities for the purposes of explaining what was going on; and they knew in far greater detail than they had in the past what the threat was about.

Mr. SHAYS. I would just make a point to you that you're basically saying to us that this code system is based on substantive determination, and that I can accept. But what I'm going to be wrestling with when I have a chance to talk to you is what does the public have a right to know? In other words, you're saying to us when you went to code orange, which is elevated, you in essence were saying something pretty significant and people better listen, because it wasn't based on a best guess. Then the question is, what does that really mean to the public?

Mr. Turner, your time had run out, but do you have any closing comment you want to make?

Mr. TURNER. Thank you for asking, actually. I thought the General's point was very important when he indicated about the vector of a threat.

For example, we know in the World Trade Center that the threat to New York did not emanate in New York, and I think that's very important. That's an issue that, in just reading these materials and looking at specific threats versus general threats, that we might not all be aware; and it was I think a very important point.

Mr. SHAYS. Mr. Schrock.

Mr. SCHROCK. Thank you, Mr. Chairman. With your indulgence, I'd like to have an opening comment. Then I have a couple of questions.

First, let me thank General Hughes, Mr. Yim and Mr. Reese for their efforts in enhancing the security of our Nation. Ensuring our Nation maintains maximum security and vigilance while protecting our liberties is a challenge and responsibility for which we are all accountable. This task must be accomplished in a reflective manner of efficiency, expediency and comprehensiveness; and I recognize that this is an unprecedented task.

As we proceed, our growing pains will be felt and the learning curve will be challenging. Progress will come from innovative ideas, innovative technologies, technological improvements and old-fashioned American ingenuity. However, in our desire to have in place the very best security advisory system we can, there is a dangerous risk in waiting for the perfect system. It is incumbent upon us to provide the resources and material support for the growth and continued improvement of this system.

I've heard your testimony, read the reports and am becoming educated as to the difficulties you are encountering. I sympathize with the regulatory, physical and even the logistical obstacles that you face.

In the aftermath of the September 11 attacks, we witnessed American resolve as we had never seen before. On all fronts, Americans were thinking outside the box. Americans know how to make things happen, and we succeed when we're challenged. Americans have an inherent right to be informed of the threats we face and should be provided sound information and accurate and available intelligence. With the Homeland Security Presidential Directive 3, the American public is assured of that right, be it through Federal, State or local authorities. It is our obligation to see that right is provided.

Secretary Ridge himself has correctly expressed concerns over the credibility of the system. We are all remiss if day by day efforts are not made and implemented which enhance the system's credibility. God forbid this country should sustain another terrorist attack in the future, but the reality is we had better be prepared.

We have had 2½ years since September 11 and have made incredible leaps forward, but we are not there yet. I fear there has not been sufficient education of the American people regarding our advisory system. I would encourage a variety of public service announcements to educate Americans.

As a kid, I remember the air raid sirens and the blank TV screens hissing the tests of the emergency broadcast system. I think the General and I can relate to that. We knew what that

meant, and we were informed. Perhaps we need to make a similar outreach effort in this age of global terrorism. We must not be a government that cries wolf, but we must be a government of leadership and accountability. I have no doubt that your continued efforts will be successful.

I wish to express my thanks to the witnesses again and the many dedicated personnel who have kept this country free from further attack. Their work is to be commended and your continued efforts to be encouraged.

Question, besides the patent answer of give us more funding, what is it that Congress can do for you to help improve the Homeland Security Advisory System? If more money is the only answer, please lay out for us why, and I mean specifically, what that additional money will buy for the taxpayer.

General, Mr. Yim, Mr. Reese.

General HUGHES. Well, thank you very much. I really appreciated the reference to the Civil Defense System and the long-ago insignia of the triangle on the circle. That's certainly a very poignant memory for me.

Mr. SCHROCK. We knew what it meant, and we remembered.

General HUGHES. We did remember, and I still do to this day.

I think the nature of the threat then, of course, primarily couched in terms of the former Soviet Union and the larger national strategic threat, is still a national strategic threat but couched in a much different way, kind of an ill-defined, fuzzy, nonpolitical entity out there that is striking us now as opposed to potentially striking us. So I see the threat as very imminent in many ways.

With regard to your direct question, what can you do for us, well, I think what you're doing in the course of your work is vital. You are, by holding these kind of hearings and by engaging with us, assisting to inform and educate the American citizenry, and I think that's vital.

I don't think I am in a position to tell you that we need more money. We need your support, and we need your understanding of the difficulty of operating this system, and I appreciated your comments in that regard.

I think that your approach here to try to clarify the system is the same as the Department of Homeland Security's. We have made changes, and that term is kind of interesting. We have not radically changed the system, but we have made small tune-ups. We have identified procedural mechanisms that we have changed or put into use, and other steps have been taken, and, in some measure, some of those steps may have been informed or motivated by your work. So I would just like to say I can't tell you we need any resources right now. Your understanding and your involvement are critical, and I appreciate it and thank you for it.

Mr. YIM. Thank you, Mr. Schrock.

I think, with all due respect to all of the difficult tasks the Department faced, one of the things that the Congress can do is really hold the Department's feet to the fire in terms of doing vulnerability and capability assessments and making those assessments complete within a reasonable period of time.

The new Homeland Security Presidential Directive gave a year deadline for the Department to do these critical infrastructure assessments and to set national preparedness goals. The Congress needs to be an integral part of the development of those national preparedness goals, assessments of the capabilities, not only at the Federal level but at the State and local and the private sector so that Federal programs can be designed—they are grant programs or tax policy or whatever programs—to stimulate enhancement of those capabilities. As we improve the capabilities of the various sectors to respond, then I think, as I said before, we will continue to evolve then the usefulness of the information that can be provided that would link the type of information to the capabilities of the recipients of that information.

So I think there is a public education component, but there's also a tremendous oversight component I think, and that's GAO's role on behalf of the Congress but also in terms of designing Federal programs to stimulate the desired behavior. Because I think it will be absolutely clear that the Federal Government cannot own or fund 100 percent of everything that will need to be done in the Nation for homeland security.

Mr. SCHROCK. I think I've heard you say that before.

Mr. Reese.

Mr. REESE. Sir, as you know, CRS doesn't make policy recommendations, but in my written statement I did provide some options should Congress decide that they would want to refine the Homeland Security Advisory System, and it's basically the two identified in my written statement.

What I'd like to identify now is vagueness of warning and lack of protective measures. Some options for vagueness of warning would possibly be have DHS just provide general warnings, not to use the Homeland Security Advisory System, which they've done twice last year. On September 4, 2003, and November 21, 2003, DHS released public statements, general warnings. They were via public statements, and the system's warning was sent out to State and local governments. This addresses the concerns that have been asserted that it causes misunderstanding at the local level, but it would not address the issue raised by those who say DHS does not give enough specificity in the terrorist attack warnings, because, again, it's just a general warning, not a specific warning.

The second option for that would be increased specificity of warnings when the threat level is raised. This is something that DHS says is a goal. They want to be able to issue high alerts to designated cities, geographical regions and industries and critical infrastructure.

Next issue would be lack of protective measures. Some cities have already—some regions and cities, when going to orange, have already adopted some protective measures on their own. Surveillance cameras are activated. Law enforcement officers are granted—not granted time off, and so on.

There's two policy options that Congress could look at. One would be just continue as is, allow the State and local governments to decide, conduct their own threat and risk assessments and decide what they need to do; and then the other one would be Federal

guidance for State and local governments to the public and the private sector.

The American Red Cross has a list of protective measures for the public schools, businesses, neighborhoods, at the different threat levels. This could be something that DHS could look at but, again, may not be as effective. If DHS were to provide specific guidance to State and local, the public, it may not be as effective if it was done at the State and local level.

Mr. SCHROCK. Mr. Chairman, I know my time is up. Let me just make one more comment to our witnesses.

This is a huge, huge issue with me personally. I represent the port of Hampton Roads, Norfolk, VA, area; and I worry about what they could do to our massive commercial port and the largest naval facilities in the world. Then I see what happened in Spain the other day and what the, "knee jerk reaction was at the polls." I really worry about that. Because what that election told me was the terrorists won, and we simply cannot allow that to happen anywhere. So anything we can do to enhance this not only for this country but share with other countries as well will be most appreciated.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

Mr. Tierney has agreed that I can go next, and then I'll recognize him.

One thing I do know is that the folks in the Department of Homeland Security want a system that works well. I think they know it is a work in process.

For me, the testimony that we have from Kenneth Allen, when he says in his testimony, the most important point that emerged from the PPW workshop, the workshop they had in 2002, was the conclusion that the Homeland Security Advisory System is a threat assessment system and not a complete warning system. The five colors tell the public that something may happen, but it does not identify what and where, and it does not warn citizens when an attack is imminent.

Would any of you disagree with that statement?

General HUGHES. In my written testimony I address that issue and in the verbal testimony I gave you today I addressed that the Federal Government, the executive branch, especially the Federal Government, takes the homeland security advisory mechanism as directive in nature, and it compels us to act, but the State, local and private sector take it as suggestive, that is, the system that we currently operate under. So we do not compel the State and local and private sectors under this system to take specific actions by law. I think that's somewhat constructive.

By the way, my experience so far is that we receive very good cooperation under this system from the State, local and private sector. I certainly know that there are complaints about some of the issues associated with the system.

Mr. SHAYS. I think you're speaking, General, more of what I'm asking. I'm not asking whether the government is compelling anyone to do anything, whether it's Federal, State or local. What I'm asking is whether you agree that it's a threat assessment system and not a complete warning system.

General HUGHES. Well, I think that goes to exactly the issue that I tried to reply to. To me, if it were a complete system, this system might have some compulsory effect throughout our country in all of the levels of our social order.

Mr. SHAYS. Yes. But even if we went one level down and didn't compel action—I realize in a storm warning we can tell people they've got to get off the Outer Banks, but in the system we have, we don't even warn people to get off the Outer Banks.

General HUGHES. We do, sir.

Mr. SHAYS. Not in this system.

General HUGHES. With regard to the Homeland Security Advisory System?

Mr. SHAYS. Yes.

General HUGHES. I think—first of all, I think drawing a parallel—direct parallel between the weather warning or alerting system and the homeland security system is a little bit different. I mean, the nature of the terrorist threat is about a direct attack on some critical feature of our government, our country, our culture, versus the kind of indirect and uncertain work of Mother Nature with regard to a large storm or natural effect.

Mr. SHAYS. See, I feel in a way that the weather threat is more certain than the terrorist threat.

General HUGHES. Indeed, at times it may be. I guess the issue is whether or not the Department of Homeland Security should be in the business of engaging in warning the country about weather and about devastating storms that are approaching.

Mr. SHAYS. And we do that——

General HUGHES. We do that in general terms.

Mr. SHAYS. No, we do that in very specific terms, I think, General.

We anticipate a storm. We anticipate it is going to be in this area. We would not only tell the law enforcement folks and the first responders about it, but you, the general public, should take specific action. You need to leave this area. You need to board up your house, you need to do the following.

I don't see any of that in the system that we have as it relates to terrorism.

General HUGHES. Sir, if I may just say—by the way, I kind of mixed the message there. I meant, we, the Department of Homeland Security, don't do that in specific ways about the weather.

Mr. SHAYS. But can I back up a second? FEMA is part of——

General HUGHES. FEMA is part of that. It is a response mechanism. But the National Weather Service——

Mr. SHAYS. Fair enough. That part you are saying is Commerce.

General HUGHES. In direct answer to your question, though, I think we do have exact parallels to what you are talking about. We do change actions, the actions of people, everyday people at airports, at ports of entry, at transit points. We change the condition in which they act often in connection with threats to the homeland.

To me, it is very similar to asking people to evacuate.

Mr. SHAYS. I am not sure we do it consistently then. When we went from—and let me say that one of the challenges that I have, which is—I understand why the colors confuse people. Green is

low. Blue is guarded or general. Yellow is elevated or significant. Orange is high. Red is severe.

In other words, you have—under threat risk, you have green, you say is low, blue is guarded, yellow is elevated, orange is high, red is severe. We are only going between elevated and high.

General HUGHES. So far.

Mr. SHAYS. Yes. But, you know, there are some parts of the country that probably should be guarded or low, frankly. I mean there are. And you have some—probably places in Montana, you know, and they intuitively know that. And there are some places in Montana that may be the other way, depending on—but what I wrestle with is, when I am told as a Member of Congress what the threat is, I am thinking to myself, whom do I tell? I know what the threat is. I know we are concerned about a dirty bomb. I know that we are concerned that it may be exploded in four or five cities. I know that it may happen at a point in which there is a large gathering of people.

So I process that information and I say, you know, I don't know if I want my daughter going there.

And I also know that we were concerned that there might be a hijacking of a plane with some pretty horrific results, from Europe. Now, I know that. So when I had school kids' parents call me and up and say, we are thinking our school kids are going to Europe, I have to wrestle with whether what I know, I warn them; or whether I just say, no, just do what you normally would do.

Well, I know I am not letting my daughter go there. She can go to South America, she can go to Asia, she is not going to Europe, at least with my recommendation, while you are at code orange. And you know why I am saying that?

And what I also know is that others who had the same warning told me that they would react the same way, and they told their friends. So we told our friends what not to do, but we didn't tell the public.

Walk me through why the public doesn't have a right to know what we are concerned about.

General HUGHES. Well, first, I think the premise that I would like to begin on is that our issue is to warn the public to the degree that judgment dictates that we warn the public, but not to incite the public to unnecessary actions. We try to do that in the system by carefully characterizing the nature of the threat and carefully administering it.

I would just like to say that I am from Montana, by the way.

Mr. SHAYS. I saw you smile.

General HUGHES. The nature of the modern environment here is that some group or person can originate from a place distant from the point of attack like, perhaps, Montana, and could indeed, if the vigilance and alertness and warning level were high enough in Montana, be found out before they get to a point of attack elsewhere, let's say, Los Angeles as an example.

And so the nature of this is, when the condition seems to rise to a level of national concern, we apply these gradations that you talked about here on the chart.

Mr. SHAYS. But let me just be candid with you. There are no gradations, in my judgment. We just go from one to the other. There is a yellow and an orange. We aren't using the others. We aren't.

General HUGHES. Well, I see it differently. In my view, we are going from an elevated condition to a high condition. And in the English language that is a relatively reasonable gradation. Higher means that you are at greater imminence.

Mr. SHAYS. OK. It seems to me, but what it says to me is—we are already at elevated and we are going to high; that says something to me in the general public that I am being told by the Department to discontinue doing what you normally do.

General HUGHES. Once again, sir, that is the specificity I was talking about with the way we administer the system.

In broad, general terms, in the most recent case where we went from yellow to orange, there was no need for us to give specific guidance to the broad population of the United States beyond what we did in raising the threat level condition.

But we did give, sir, much specific guidance to those places, those sectors, those elements of our culture which were specifically affected with regard to the threat information we had.

Mr. SHAYS. Let me ask you this then. What you are really suggesting is that our system is so good that if you tell the authorities, the public that has no need of concern because it is a foolproof system, that they will catch whoever is going to do it.

I don't think the Department would want to be in the position of making that statement.

General HUGHES. I hope I didn't say that. I am trying to illustrate to you the problem we have, and I do think it is a challenge, which Mr. Yim and Mr. Reese have talked about, too, finding balance in this presentation to the American public.

What I would like to say is that I think we have done a good job in the most recent case especially. We are learning as we go along. I think Mr. Turner and Mr. Schrock both noted the evolution of this. We are indeed learning as we go along about how to administer this system.

Mr. SHAYS. Let me just say this—and, Mr. Yim, I am over my time, and I thank Mr. Tierney. But what I want to say to you is, if in fact we went to code orange, as we did based on a dirty bomb and some other things, and if in fact there was a dirty bomb explosion and people had been gathering in a public place, to what extent would the Department have been—not duplicitous—to what extent should it be held responsible?

If my child had gone to a public place that ultimately had what we were concerned might happen, who would be at fault?

General HUGHES. Well, I think that we would, if we have information about that specific place. But we did not have that kind of specific issue in most cases.

You speak there of a period of time and of a place and of a condition or event. In some few cases, we have had that kind of tactical information. But in most cases we had a broad, general kind of threat condition, actually coming from different sorts of—we use the term "information streams," and they are characterized differently. But collectively, when those streams are brought together, the broad threat condition here in the United States during Decem-

ber and January was complex enough and high enough for us to change the color and issue specific instructions, in some cases, you may recall.

Mr. SHAYS. But only to the authorities, not to the general public. To the general public, they were told to do what they normally do?

General HUGHES. Yes. In some cases the general public may have been the beneficiary of the actions of the official government without generally knowing if there was a great threat to them.

Mr. SHAYS. Thank you.

Mr. Yim.

Mr. YIM. Mr. Chairman, I think there are two quick points I would like to make, because I do generally agree that it is more the threat advisory, a threat assessment, than a warning system, for, I think, some subtle reasons.

First, we often consider the color code as a point-in-time warning system or assessment system when, in fact, an effective warning system is a process, as I think some of your witnesses following us will say. It is not just a point-in-time warning.

There are obviously differences between the weather and terrorists. But if you think about how we handle weather advisories, if a storm is very far off the coast, you are very vague in the information about the landfall and points of impact. As we develop more information, we can develop more specificity and give greater information to those that are potentially affected without needlessly warning or needlessly causing anxiety to those that are going to be outside the path of a storm.

The problem that we have, often, with the terrorist threat advisory is, it is either on or off. It is either yellow or orange, on or off, rather than considering it as a process. And I think, as it evolves, more specificity can be given during periods of orange alert. It is not just we declare orange alert on May 17th, here is the information; you are not going to hear from us again until we lower the alert level. I think that process needs to be recognized.

The second point is, we tend to aggregate that. It is clearly a question of balance, as General Hughes points out. But it is also the danger of aggregating data. One of the things that the Department uses when it determines whether to go to orange alert is, they assess both the potential—the risk, the potential of the threat, the probability of the threat, and the severity of the risk should it occur. We probably shouldn't blend that data together. Those are two bits of information that are important for people to know.

So if you have a low consequence, a low probability event, but a tremendously high consequence, you may take certain types of preventive action. If you have a fairly high probability of occurrence, but the consequence is relatively low, it is not a weapon of mass destruction, you may take different types of preventive or response measures.

The aggregation of those two concepts into the decision to raise from yellow to orange, I think, exacerbates the problem, making it worse.

Mr. SHAYS. I am going to say, there is no way, Mr. Tierney, you are going to get the floor right away, just after this statement. I don't pretend this is an easy issue.

For me, I stay up at night thinking what I would do, General Hughes, if I was in your circumstance and we firmly believed that there was the potential of a nuclear attack in a city and that there was a potential cell that we thought had a weapon, material, and that they were somehow planning in a city.

I mean, if you tell the public, there could be a horrific exodus that would kill literally tens of thousands of people; and yet, if it happens and 100,000 people are killed, there would be hell to pay. And I don't know the answer. But I do know we've got to talk about it.

And ultimately the public has to have some sense of what these warnings mean. They can't just be for the law enforcement folks. So we have to find a way to have it make sense. And I would also say, it just seems to me that we should try—and I think the second panel is going to say this—we should try somehow to have the warnings in natural disasters as well as the terrorist disasters somehow have some uniformity in terms of words, in terms of warnings that—and again, I think you are going to learn from some of the second panel.

I hope your folks, as well as the first—and your own comments, and maybe from us, I hope they take the information from this hearing and process it.

Mr. Tierney.

General HUGHES. May I just make one comment about your statement there, Mr. Shays? I think that what you had to say was very important.

I don't know how to explain this, but I take this very personally, since I am the intelligence officer who delivers the information to make this decision. And the thing that keeps me literally awake and on edge was what you described, a catastrophic strike against the United States that goes unwarned.

And there are no easy answers to this, but I would just like to let you know that I appreciate very much your recognizing and verbalizing that point. And that is not procedural so much as it is a matter of judgment, a matter of the heart, a matter of feeling, a matter of intellect and analysis, and a matter of condition and circumstance. It is a vital piece of work that has been given to me to do, and I treat it very, very seriously.

Mr. SHAYS. Thank you, General.

Mr. Tierney, thank you for your patience.

Mr. TIERNEY. You know, when you talk about all of this—and I think the comments that the chairman made about what individuals are supposed to take from this are well taken. But if you put yourself in the position of the local law enforcement or fire fighters or responders on that, what is the status right now of our system in terms of a situation where you go from yellow to orange, what specifically might, say, a police chief in a coastal community like Newburyport, MA know to do with respect to any given asset if it just goes from yellow to orange? Is he to protect the seaport and against a nuclear power plant just north of him, as well as chemical facilities, other things that matter; or is there enough specificity in there that he knows where to marshal his resources?

General HUGHES. Currently, we would deliver specific information to the police or to first responders or to other officials about

a given location, a given sector of endeavor, such as a nuclear power plant's operation, or other conditions that we have specificity about, if we have it—if we have it. And we would do that relatively precisely, and we would not generally do that in public because to disclose that kind of knowledge in a public environment would, first, give away the fact that we have the knowledge and, thereby, potentially put how we got that information at risk; and it would also contribute to a broad, general feeling that would be unnecessary, in my view.

We would accomplish the work of the authorities or the safety of the citizenry in the specificity that we treat that information with.

Mr. TIERNEY. So you are saying, if you went from yellow to orange nationwide, that—and you had information that it was something that might relate to a nuclear power plant in the northeast, that is the information you would give to all interested law enforcement and other first responders across the country, so that others would not be in the same type of cautionary situation as would those people in the northeast?

General HUGHES. That is one way to put it.

The other way to put it—which is, I think, a little bit less palatable, but it is the way in which we have to do it—we would give that information only to the locale that we had specific information about.

Mr. TIERNEY. So here is the thing that I am talking about. That you give an alert from yellow to orange nationwide. Then you let the people in Oregon know that there—you have information specifically for them.

My police department is running around taking care of everything—putting people on overtime, calling the Coast Guard for support over there, calling the National Guard for some other facilities or whatever. Are they right or wrong to react like that?

General HUGHES. They are right. And this is one of the complex issues here. And I think I would like to use Madrid as an example here. We are now under a condition of what I would refer to as simultaneity. We cannot depend upon an attack to come in a single place at a single time.

Mr. TIERNEY. I was talking about an incident where the only information you had about any attack was with some specificity.

General HUGHES. Yes.

Mr. TIERNEY. That is—the answer is still, you don't communicate that to responders across, so that the Oregon people are really heightened, and the other people can take a different, more nuanced look at that, and they have to go full out?

General HUGHES. Yeah. I understood your question, sir. I guess the issue for me is that maybe the premise here is a little bit further than I would care to go.

If we had specific information about a problem in Oregon, we would talk directly to the authorities in Oregon and not raise the national threat condition, depending upon the nature of the information.

Mr. TIERNEY. If you had information that related to nuclear power plants, let's say——

General HUGHES. Then we would talk to the nuclear power plant sector.

Mr. TIERNEY. And not the others?

General HUGHES. OK.

Mr. TIERNEY. So when you go from yellow to orange nationally, then you have less specificity, you are doing that because you have some information, but you are not certain of the extent.

General HUGHES. Before you came in, I explained in the case of the December-January timeframe, we had both specific information about specific issues of threat, and the threat condition generally rose to the level that we decided we needed to make a national change in the threat advisory system. And that probably will occur again in the future.

And I might just say, sir, that in that case, generally it would not be a single piece of specific information, but several in different places.

Mr. TIERNEY. When you notify the local officials on that, what communications system are you using now?

General HUGHES. There are a variety of communications systems to use. For State and local, we have the JRIES system——

Mr. TIERNEY. I was interested in looking at that. In fact, that was going to be my next question, what is the functionality of the JRIES system and how widespread is its use? And how sophisticated are we in that technology?

Because I am aware of similar systems being used in the military, developed out of MIT with General Myers and General Kellogg; and we have looked at those extensively, and they are working quite well in connecting military bases.

Now, I know they are being tried elsewhere. Are you familiar with that? Is that the type of system that JRIES is going to evolve into, and where are we in that evolution?

General HUGHES. Indeed, sir, JRIES grows out of the military system. It was begun by the military, and we have begun to adopt it. We are proliferating it as rapidly as we can. We intend to encipher some of it, especially to the States and major cities, at the Secret level as rapidly as we can do so, so that they have a greater body of knowledge available to them.

Mr. TIERNEY. Simultaneously?

General HUGHES. I think the answer that I would like to give you is, we are not limited by the systems we can use, there are so many, to include, by the way—and I thank my colleagues for mentioning this—the fact that Secretary Ridge and other officials of government do make public statements using our national media to communicate the position of the government.

Mr. TIERNEY. I understand. It was the simultaneity that I was thinking of, of being very effective and very useful. And the JRIES system, if we can raise that to the level that I believe that it can accomplish, to me that is a powerful tool; and you can get on there to address the people that you want, with the specificity that you have, and people have a much more detailed idea of what it is that they have to respond to, just what knowledge that you have, you can keep it to a secure group.

So if I am allowed, Mr. Chairman, just one last?

What is the status of that now in terms of your use? How long—how far along the chain is JRIES?

General HUGHES. I hate to give you a percentage of fielding, but it is very far along. We are proliferating it very rapidly out to the States and the major cities especially, and to some local organizational entities. We have a plan to go to the county level in perhaps not every county in the United States right away, I don't want to make you think that this is going to happen overnight, but over the long term we will evolve to the county level.

We have other alternatives, other communications alternatives that are in being now, that go especially to the State and some localities and, by the way, to the private sector. An example would be SIPRNET, the National Guard communications systems, the national telephone system, which we can use. We have provided secure telephones to State and local officials in many cases, especially in major cities, and often in the private sector those kinds of secure communications means are available. We can use the Internet, and we do for general information.

We really are not limited here. We are trying to make a coherent system that everyone can understand and depend upon. And in my view, I am the key player in that issue, and I would say that by the end of this calendar year, we will achieve a very coherent and very robust, broad system of communications and interaction here in the United States that will not only go from the government to our State, local, private sectors, tribal and other territorial responders, but it will come back to us from them, with their views, their local knowledge, their input. That is, I think, a vital piece of this.

Mr. TIERNEY. Who is your principal contractor in the JRIES?

General HUGHES. I don't think we have a principal contractor for JRIES, because it is a governmental-owned system. But we do have contractors associated with putting it in place, a number of them.

Mr. TIERNEY. OK.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

We are going to go to our next panel, but I want to say this and get some kind of response here. I don't believe, General, that anyone here is questioning whether we should have gone to code orange. I don't even think—and so I am convinced, trust me, I am so convinced that I responded differently based on the code orange. It meant something to me.

What I would like you to do is just comment on what Mr. Yim talked about in terms of risk communication experts generally agree that effective warnings should be specific—the nature of the threat, when and where it is likely to occur, and over what period of time, provide guidance or actions to be taken, and perhaps, above all, assure that the information is consistent, accurate, clear and provided repeatedly.

I guess the issue that I wonder about is, do you disagree with this recommendation, so it is—you shook your head so you don't disagree?

General HUGHES. No, I don't.

Mr. SHAYS. So the question is how we move forward? Is that the issue?

General HUGHES. Yes. I think—once again, I hate to use the word "evolution" or learning and doing all the time, but I think it

is the right way to characterize this. I think Mr. Yim's characterization with those words you just voiced are generally right.

I do think—once again, we do find ourselves juxtaposed against the need to secure some of the information we have and to communicate it so that it can be used by appropriate authorities and not alarm or unnecessarily excite the general public. This is a matter of great judgment at times and can be second-guessed and criticized.

As you said, you gave us credit for doing the best that we possibly can, and we are certainly trying to do that. We will learn, using Mr. Yim's construct here, more about how to communicate specificity out to the larger country than we have in the past.

However, the point of protection of the information probably revolves around the degree to which we can be specific and, at the same time, make sure that we don't further endanger our public by giving away to those who would strike us some kind of information that would allow them then to find a seam or a gap and hit us where we did not expect.

Mr. SHAYS. I understand it is a fine line. But I would suggest this to you, that it was known from almost day 1 that we were having a problem with flights from Europe. We knew it, the terrorists knew it, and the general public was hearing about it kind of indirectly.

And I would just suggest to you that some of what we knew, since the terrorists knew and the government knew, the only thing you can argue is that we wouldn't want to disclose sources and methods. But I don't think you necessarily have to disclose sources and methods to disclose information to the public that would then get them to decide whether or not they want to do something.

I just make this point to you. If, in fact, we thought that large—we were reading it in the newspaper and the newspapers were correct, but it wasn't coming from Homeland Security that large public gatherings were a very real target, then unlike the way I responded publicly, which I would do differently, I think the public would at least need to know that they should make choices, that we think we protected this large public gathering, that we are confident of what we have in place, but you need to know it is a target, and so when you go, you go with some risk—if it is to raise the flag, show you are brave, whatever, but it might tell a parent, maybe they are not going to send their 14-year-old child. And then I want to tell you why I think this is important.

If, in fact, something does happen, you have more credibility the next time. I will tell you, there will be hell to pay if the public isn't warned about something that everybody else knew about in government. Then they will never believe you.

I will just illustrate it this way. When we were warning right after September 11th that we could deal with smallpox, that we had all of the resources necessary to deal with it, I knew that was simply a lie. It was not true. When I confronted—and I will say it more generally, I just simply knew it was not true.

When I spoke to the individual involved, he said we were trying to make the public feel more comfortable and to lower their anxiety. My comment to him was, though, if there was an outbreak and there was this lack of ability to deal with it, they will never believe

you forever, and then—no matter what the government says. So I guess truth in this process is important too.

And let me just close by saying, first, is there any panelist that wants to make a comment? Is there anything that you felt we should have asked that was not asked that you want to put on the record? Anything based on what you have heard said today that you want to put on record?

Mr. YIM. Just a 10-second comment, if I could, Mr. Chairman.

I think we should err on the public's right-to-know side, because the public has a great appetite for information. I have a great appetite for information. If I am not going to get it from a credible source, I may get it from a source with much less reliable information. I would rather receive it from the Department of Homeland Security than receive it from the Internet.

Mr. SHAYS. OK.

Any other comments?

General, you are great to be here. Thank you for participating in this panel. It has been very helpful. And we know that you clearly want to make this system work better. I believe in the system, the process, I know it has to work better though.

Mr. Reese, thank you as well. Mr. Yim, thank you.

We are going to announce our second panel: Mr. Charles D. Connor, senior vice president, communication and marketing, American Red Cross; Mr. Michael Wermuth, senior policy analyst, RAND Corp.; Dr. James J. Carafano, senior research fellow, defense and homeland security, Heritage Foundation; and Mr. Kenneth B. Allen, executive director, Partnership for Public Warning.

All four of you, if you would, stay standing.

[Witnesses sworn.]

Mr. SHAYS. Note for the record, our four witnesses have responded in the affirmative.

You have all been here for the questions and responses and statements of the first panel. Feel free to incorporate that in your statement; feel free to depart from your statement. That will be part of the permanent record. And I want to let you know that we really thank you. We think this is a very significant issue, and we appreciate your participation in our trying to understand it better.

We will start, as you are sitting, with you, Mr. Connor, first.

STATEMENTS OF CHARLES D. CONNOR, SENIOR VICE RESIDENT, COMMUNICATIONS & MARKETING, AMERICAN RED CROSS; MICHAEL WERMUTH, SENIOR POLICY ANALYST, RAND CORP.; DR. JAMES JAY CARAFANO, SENIOR RESEARCH FELLOW, DEFENSE AND HOMELAND SECURITY, HERITAGE FOUNDATION; AND KENNETH B. ALLEN, EXECUTIVE DIRECTOR, PARTNERSHIP FOR PUBLIC WARNING

Mr. CONNOR. Thank you, Mr. Chairman and members of the subcommittee, for your gracious invitation to testify this morning. My name is Chuck Connor, and I serve as senior vice president of communication and marketing at the American Red Cross national headquarters here in Washington.

The American Red Cross is a nationwide network of nearly 900 chapters and 36 blood services regions dedicated to saving lives

and helping people prevent, prepare for and respond to emergencies.

With 1.2 million volunteers and 32,000 employees, the Red Cross annually mobilizes relief to families affected by nearly 70,000 disasters. We also train almost 12 million people each year in life-saving skills. The Red Cross is the largest supplier of blood and blood products to more than 3,000 hospitals across the Nation. We also assist victims of international disasters and conflicts at locations worldwide.

One of our most important partnerships is government at every level—Federal, State and local. Government relies on the American Red Cross to address the huge challenges of public preparedness, particularly in the all-hazards environment we spoke of today. We believe that everything the Red Cross can do in this important area relieves some of the burden on government agencies and first responders.

As the Department of Homeland Security has assumed the huge responsibility for domestic security, it has correctly focused on operational procedures. Conversely, it is our responsibility at the Red Cross to prepare the American public.

In January, Red Cross president and CEO, Marty Evans, issued a strong wake-up call to the American public to get prepared. Despite growing concerns about terrorism and man-made disasters, Americans have generally failed to take the most basic steps to ensure their own safety.

According to a study the American Red Cross commissioned last year, close to 60 percent of Americans, fully 175 million of our fellow citizens, are entirely unprepared for a disaster of any description. In February 2003, the Red Cross launched the Together We Prepare Campaign. This program challenges individuals and communities to take responsibility for their safety and that of their families at home, in school, and in businesses and neighborhoods.

By following five basic steps we can all move toward greater safety. Those five steps are: make a plan, build a kit, get trained, volunteer, and give blood. Mr. Chairman, please mark your calendars, our next blood drive in the House is scheduled for April 15th.

We believe that the more empowered and self-sufficient you and I feel, the more immediately effective we can be in a crisis situation. The bottom line, regardless of the responsibilities of government, in the end, all of us must take charge of our own destinies.

The strategic direction of the Red Cross is to be America's partner and a leader in mobilizing communities to help people prevent, prepare for and respond to disasters and other life-threatening emergencies. A critical part of this effort includes public education regarding the meaning of each alert level within the Homeland Security Advisory System, and the immediate actions required to ensure safety and security.

As you know, the White House issued Homeland Security Directive 3 in March 2002, which established the five threat conditions for a possible terrorist attack. General explanations were given for preparedness activities for each level, but these were intended mainly for government agencies.

However, across the country, there arose questions of, what does a condition yellow mean to me or my family? What does this mean for my business or my children's school?

Working with the Office of Homeland Security at the time, the Red Cross developed and released specific disaster readiness guidelines for individuals, families, neighborhoods, schools, and businesses. Each color-coded threat category was further expanded to provide recommendations for each of these different audiences. These Red Cross-developed guidelines have been incorporated into the Department's own public communications.

As part of our expanding preparedness and response role, we are continuing to keep America informed of the Department's terrorist threat level recommendation and the appropriate actions to take if the level is raised or lowered. And I believe you will see the chart on the wall there, which is germane to what we are talking about here.

Once notified of a status level change, the Red Cross implements procedures and protocols to ensure that the organization can provide a swift, efficient and supportive response in case of an incident.

Similarly, the public looks to the Red Cross as a primary source of emergency preparedness information. When a change in status takes place, the Red Cross communicates practical emergency preparedness information to the public through national news releases and the communication resources of our Nationwide Disaster Services Network.

Preparedness information empowers all of us who use it to be more responsible for our own security and that of our family. This vital education effort befits our stature as America's premier disaster response organization.

In a world where the forces of nature and man too often collide, the Red Cross is truly a beacon, showing Americans the way to safety. We owe it to ourselves, our families, our communities to prepare for the unexpected.

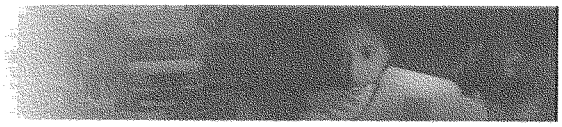
Thank you again, Mr. Chairman, for this opportunity to appear before your panel. I would be pleased to answer questions later.

Mr. SHAYS. Thank you, Mr. Connor.

[The prepared statement of Mr. Connor follows:]

American Red Cross

Together, we can save a life



Testimony of

Charles D. Connor
Senior Vice President, Communication & Marketing
American Red Cross

March 16, 2004

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

Homeland Security Advisory System:
Threat Codes and Public Response

Testimony of
Charles D. Connor
Senior Vice President, Communication & Marketing
American Red Cross
March 16, 2004
House Committee on Government Reform
Subcommittee on National Security, Emerging Threats, and International Relations
Homeland Security Advisory System: Threat Codes and Public Response

Thank you, Mr. Chairman and members of the subcommittee, for your gracious invitation to testify this morning. My name is Chuck Connor and I serve as Senior Vice President of Communications and Marketing at the American Red Cross national headquarters.

The timing of this hearing is most appropriate—Every year since 1943, March has been designated "American Red Cross Month" by the President of the United States to highlight the work of an organization that was founded in 1881 by Clara Barton and chartered by the Congress in 1905 to provide humanitarian services to the United States in times of need. This year, President George W. Bush signed the Presidential Proclamation, continuing this proud tradition. As a result, March has become a time for the Red Cross to commemorate its past accomplishments and to look forward to future goals.

Our dedication to helping make families and communities safer at home and around the world is continuous. Governed by volunteers and supported by charitable donations, the American Red Cross is a nationwide network of nearly 900 chapters and 36 Blood Services regions dedicated to saving lives and helping people prevent, prepare for and respond to emergencies. With 1.2 million volunteers and 32,000 employees, the Red Cross annually mobilizes relief to families affected by nearly 70,000 disasters, trains almost 12 million people in lifesaving skills and exchanges more than a million emergency messages between U.S. military service personnel and their families. The Red Cross is the largest supplier of blood and blood products to more than 3,000 hospitals across the nation and also assists victims of international disasters and conflicts at locations worldwide.

As the Department of Homeland Security (DHS) marked its one-year anniversary a few weeks ago, the Red Cross was recognized for its pivotal role in keeping the nation prepared. As a valuable partner with Homeland Security, the Red Cross continues to help prepare Americans for emergency situations by teaching lifesaving skills, recruiting volunteers and providing valuable preparedness information to individuals, families, schools and workplaces.

In fact, the strong relationship that exists between DHS and the Red Cross has been mentioned on numerous occasions by Secretary Ridge, most recently as an integral partner in disaster preparedness and response.

We are the only non-governmental agency assigned a lead role in the Federal Response Plan coordinated under FEMA and DHS. We are the lead agency for Emergency Support Function #6 -- Mass Care - the shelter, feeding and clothing of disaster victims - and we're a support agency to the Department of Health and Human Services for Emergency Support Function #8 - Health and Medical Services. That's the provision of blood, first aid, basic health care and mental health counseling. As the Federal Response plan is rolled into the new, more comprehensive National Response Plan, Red Cross anticipates an expanded role.

Furthermore, the Red Cross has a position on the Interagency Incident Management Group (IIMG) as the subject matter expert for Mass Care and serves as the only non-governmental organization with an assigned staffing position. At the first sign of an increased threat, the IIMG is stood up to provide policy recommendations to Secretary Ridge. For example, the Red Cross staffed the IIMG during last summer's northeast blackout, Hurricane Isabel, on New Year's Eve and during the recent 'Unified Defense 04" national terrorism training exercise.

We also commend the dedicated efforts of our President, our partners at DHS, and each of you for the significant actions that have been undertaken to strengthen our nation's homeland security.

The importance of partnerships in our work cannot be overstated. Going it alone is no longer an option as the frequency, scope and scale of disasters—both natural and human-made—is on the rise. One of our most important partnerships is the government at every level—federal, state and local. The government relies on us to address the huge challenges of public preparedness, particularly in an all-hazards environment. And, the Red Cross cannot be effective unless we're at the table working collaboratively to make America safer. Stated differently, every time we move forward to prepare the public, we relieve the burden on government.

We are all partners in this endeavor—government, the Red Cross, the private sector, and each and every American. All of us in this room and beyond need to prepare ourselves for whatever may come. The federal government cannot do that for us—necessity dictates that it address the nation's capabilities and response strategies from the top down. That's where the Red Cross comes in.

As the Department of Homeland Security has assumed the mammoth responsibility for domestic security, it has focused on operational preparedness. It has been marshalling resources, modeling terrorist scenarios and their likely implications, focusing on the needs of the first responder community—police, firemen, and EMTs—as they should.

But, while the Department oversees massive efforts to prepare governments and public agencies at all levels for every type of disaster, it's our responsibility at the Red Cross to prepare the general public. And we take that responsibility very seriously.

Before I address the specific focus of this hearing—the threat alert system—I would like to briefly expand upon the importance of public preparedness—the theme for Red Cross Month 2004—and the role of the Red Cross.

In January, Red Cross President and CEO Marty Evans issued a strong wake up call to the American public to remember the importance of being prepared. Despite growing concerns about terrorism and human-made disasters, in addition to the onslaught of fires, tornadoes, floods and other natural disasters that the United States faces every year, Americans continue to go unprepared. Amazingly, there are 175 million of our fellow citizens who are basically asleep at the switch when it comes to their own, and their family's, safety and security.

Last year reminds us all that we live in unpredictable times. Not only did we observe the second anniversary of a devastating terrorist attack, but we also had to face our vulnerability to the forces of nature. An extraordinary string of more than 516 tornadoes wiped out large swaths of the Midwest and Southeast - killing 39 people in a single month. Hurricane Isabel battered the East coast in September. And, wildfires and mudslides ravaged whole communities in Southern California in October. It was tragic to see an entire community burned to the ground.

Add to that a rash of power outages in the Northeast in August and the tens of thousands of single-family house fires across the nation over the course of the year, and you get a sense of how busy we've been at the Red Cross. Most of these disasters never make the news; we call them our "silent" disasters. With over half the U.S. population living in coastal communities and nearly a third in the top nine metropolitan areas, the risk of catastrophic and mass casualty disasters increases annually. And that's ***without*** adding in the threat of terrorism. To highlight the myriad of disasters that impacted our nation last year and to focus the public's attention on the continuing importance of preparedness, we will be releasing *America's Disasters 2003—A Call to Action* in the coming weeks with valuable information and statistics.

As Admiral Evans noted in her remarks, we are a nation of resilient, optimistic individuals. We have not let the increased threat of danger deter us from living our lives, and we applaud and share that spirit.

But, what concerns us is the lack of reasonable preparedness on the part of the general public. According to a study the Red Cross commissioned last year, close to 60 percent of Americans are wholly unprepared for a disaster of any description. They don't have a family emergency plan, nor are they aware of school, workplace and community emergency procedures. They have not stocked emergency supplies, nor have they sought even basic first-aid and CPR training. They're not giving blood, nor are they donating their time or money to emergency support services like the American Red Cross.

In February 2003, the Red Cross launched the *Together We Prepare* campaign, challenging individuals and communities to take responsibility for their safety and that of

their families in their homes, schools, businesses and neighborhoods. By following five basic steps, we can all move toward greater safety. Those five steps are:

- Make a plan—Design a Family (Home) Disaster Plan. Work with neighbors and co-workers to create Community and Workplace Disaster Plans.

- Build a kit—Assemble Disaster Supply Kits, which contain items that people may need (1) if confined to their home or place of business for an extended period or (2) if they are told to evacuate on short notice.

- Get trained—Learn to save lives. The Red Cross offers classes year round to individuals and businesses on first aid, CPR, and use of automated external defibrillators, or AEDs.

- Volunteer—Give of yourself. Supporting the Red Cross mission, whether sharing your time or money, means that they will be there to respond immediately whenever the need arises.

- Give blood—Become a regular and frequent blood donor to ensure a blood supply that meets all needs, all of the time. It is critical that the Red Cross maintain at least a 5- to 7-day blood supply. To do so, more Americans need to become first time and repeat donors. Only five percent of the eligible population donates blood. Having current donors donate more frequently is not sufficient to meet that need. So mark your calendars—our next blood drive in the House of Representatives is scheduled for April 15.

We introduced the *Together We Prepare* program to empower people to shoulder the responsibility for their own safety and security by laying out the five pro-active steps that individuals and families can take to prepare for any emergency.

That's the critical point, actually. The more empowered and self-sufficient you and I feel, the more immediately effective we can be in a crisis situation. We become less of a burden to the 9-1-1 emergency call system, and our state and local public health and emergency responders. It makes sense—if you and your family have a plan, it goes into action in a disaster. You're not fumbling around looking for help and guidance. You're in charge of your own destiny.

The strategic direction of the Red Cross is to be America's partner and a leader in mobilizing communities to help people prevent, prepare for and respond to disasters and other life-threatening emergencies. This nationwide education effort focuses on personal and family preparedness for disasters of all types and magnitudes—whether at home, at school, or in the workplace. A critical part of this effort includes public education regarding the meaning of each alert level within the Homeland Security Advisory System and the immediate actions required to ensure safety and security.

As you know, the White House issued Homeland Security Directive #3 in March 2002, which established five threat conditions for possible terrorist attack:

Green—Low
Blue—Guarded
Yellow—Elevated
Orange—High
Red—Severe

General explanations were given for preparedness activities for each level, but these were intended mainly for government agencies. However, across the country, questions of "What does a condition 'yellow' mean to me or my family?" or "What does this mean for my business or my children's school?" Working with the Office of Homeland Security at that time, the Red Cross developed specific disaster readiness guidelines for individuals, families, neighborhoods, schools and businesses, and released a complementary set of guidelines. Each color-coded threat category was further expanded to provide recommended actions for each of these give different constituencies:

Individuals
Families
Neighborhoods
Schools
Businesses

As part of our expanding preparedness and response role, we are continuing to keep America informed of the Department's Terrorism Threat Level recommendations and the appropriate actions to take if the level is raised or lowered. We are also working with the Centers for Disease Control (CDC) on the most effective means of providing terrorism risk information.

Through our nationwide, community-based network of chapters and blood services regions, and supported by resources at the regional and national level, we have forged many collaborative partnerships with federal, state, and local agencies. Once notified of a status level change, the Red Cross implements procedures and protocols to ensure the organization can provide a swift, efficient, and supportive response in the case of an incident.

Similarly, the Red Cross is looked upon by the public as a primary source of emergency preparedness information. When a change in status takes place, the Red Cross communicates this change and critical emergency preparedness information, and its meaning, to the public through national news releases and the communication resources of our nationwide disaster services network.

Preparedness information, once taken to heart, empowers all who use it to be more responsible for their own security and that of their family. This preparedness education effort belies our stature as America's premiere disaster response organization.

For information about any Red Cross programs or opportunities to support Red Cross, you can log on to www.redcross.org or call 1-866-GET-INFO. Taking a step toward your own safety and security is as easy as picking up the phone... signing up at the next company blood drive... storing some water and non-perishables in the basement. So, why don't we all do it?

In a world where the forces of nature and man too often collide, the Red Cross is a beacon showing people the way to safety. We owe it to ourselves, our families, our communities to prepare for the unexpected. That's our challenge to America today—don't let disaster take you or your family by surprise again! Like the Red Cross, have a plan, get involved, and join with us.

Thank you again, Mr. Chairman, for this opportunity to appear before this distinguished panel. I would be pleased to answer your questions.

American Red Cross

Together, we can save a life

Homeland Security Advisory System Recommendations

Individual

Risk of Attack	Recommended Actions
SEVERE *(Red)*	• *Complete recommended actions at lower levels* • Listen to radio/TV for current information/instructions • Be alert to suspicious activity and report it to proper authorities immediately • Contact business to determine status of work day • Adhere to any travel restrictions announced by local governmental authorities • Be prepared to shelter in place or evacuate if instructed to do so by local governmental authorities • Provide volunteer services only as requested
HIGH *(Orange)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Review your personal disaster plan • Exercise caution when traveling • Have shelter in place materials on hand and review procedure in Terrorism: Preparing for the Unexpected brochure • If a need is announced, donate blood at designated blood collection center • Prior to volunteering, contact agency to determine their needs
ELEVATED *(Yellow)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Ensure disaster supplies kit is stocked and ready • Check telephone numbers and e-mail addresses in your personal communication plan and update as necessary • Develop alternate routes to/from work/school and practice them • Continue to provide volunteer services
GUARDED *(Blue)*	• *Complete recommended actions at lower level* • Be alert to suspicious activity and report it to proper authorities • Review stored disaster supplies and replace items that are outdated • Develop emergency communication plan with family/neighbors/friends • Provide volunteer services and take advantage of additional volunteer training opportunities
LOW *(Green)*	• Obtain copy of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter • Develop a personal disaster plan and disaster supplies kit using Red Cross brochures Your Family Disaster Plan and Your Family Disaster Supplies Kit • Examine volunteer opportunities in you community; choose an agency to volunteer with and receive initial training • Take a Red Cross CPR/AED and first aid course

Your local American Red Cross chapter has materials available to assist you in developing preparedness capabilities.

ARC 1462 (Rev. 8- 2002)

American Red Cross

Together, we can save a life

Homeland Security Advisory System Recommendations

Family

Risk of Attack	Recommended Actions
SEVERE *(Red)*	• *Complete recommended actions at lower levels* • Listen to radio/TV for current information/instructions • Be alert to suspicious activity and report it to proper authorities immediately • Contact business/school to determine status of work/school day • Adhere to any travel restrictions announced by local governmental authorities • Be prepared to shelter in place or evacuate if instructed to do so by local governmental authorities • Discuss children's fears concerning possible/actual terrorist attacks
HIGH *(Orange)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Review disaster plan with all family members • Ensure communication plan is understood/practiced by all family members • Exercise caution when traveling • Have shelter in place materials on hand and understand procedure • Discuss children's fears concerning possible terrorist attacks • If a need is announced, donate blood at designated blood collection center
ELEVATED *(Yellow)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Ensure disaster supplies kit is stocked and ready • Check telephone numbers and e-mail addresses in your family emergency communication plan and update as necessary • If not known to you, contact school to determine their emergency notification and evacuation plans for children • Develop alternate routes to/from school/work and practice them
GUARDED *(Blue)*	• *Complete recommended actions at lower level* • Be alert to suspicious activity and report it to proper authorities • Review stored disaster supplies and replace items that are outdated • Develop an emergency communication plan that all family members understand • Establish an alternate meeting place away from home with family/friends
LOW *(Green)*	• Obtain copy of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter • Develop a personal disaster plan and disaster supplies kit using Red Cross brochures Your Family Disaster Plan and Your Family Disaster Supplies Kit • Take a Red Cross CPR/AED and first aid course

Your local American Red Cross chapter has materials available to assist you in developing preparedness capabilities.

ARC 1463 (Rev. 8- 2002)

American Red Cross

Together, we can save a life

Homeland Security Advisory System Recommendations

Neighborhood

Risk of Attack	Recommended Actions
SEVERE *(Red)*	• *Complete recommended actions at lower levels* • Listen to radio/TV for current information/instructions • Be alert to suspicious activity and report it to proper authorities immediately • Adhere to any travel restrictions announced by local governmental authorities • Be prepared to shelter in place/evacuate and assist neighbors who are elderly or have special needs to do the same
HIGH *(Orange)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Check on neighbors who are elderly or have special needs to ensure they are okay. Review disaster plan with them • If a need is announced, contact nearest blood collection agency and offer to organize a neighborhood blood drive
ELEVATED *(Yellow)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Have neighborhood meeting in order to identify neighbors who are elderly or have special needs. Assist them in development of a personal disaster plan and disaster supplies kit if requested.
GUARDED *(Blue)*	• *Complete recommended actions at lower level* • Be alert to suspicious activity and report it to proper authorities • Ask the local Red Cross chapter to offer a presentation called "Preparing for the Unexpected" at an upcoming neighborhood meeting
LOW *(Green)*	• Have neighborhood meeting to discuss emergency plans and establish a 'Neighborhood Watch' • Obtain copies of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter and distribute at neighborhood meeting • Promote or arrange for people in the neighborhood to take a Red Cross CPR/AED and first aid course

Your local American Red Cross chapter has materials available to assist you in developing preparedness capabilities.

ARC 1464 (Rev. 8-2002)

American Red Cross

Together, we can save a life

Homeland Security Advisory System Recommendations

Schools

Risk of Attack	Recommended Actions
SEVERE *(Red)*	• *Complete recommended actions at lower levels* • Listen to radio/TV for current information/instructions • Be alert to suspicious activity and report it to proper authorities immediately • Close school if recommended to do so by appropriate authorities • 100% identification check (i.e.-driver's license retained at front office) and escort of anyone entering school other than students, staff and faculty • Continue offering lessons from Masters of Disaster "Facing Fear: Helping Young People Deal with Terrorism and Tragic Events" curriculum • Ensure mental health counselors available for students, staff and faculty
HIGH *(Orange)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Review emergency plans • Offer Masters of Disaster "Facing Fear: Helping Young People Deal with Terrorism and Tragic Events" lessons in grades K-12 • Prepare to handle inquiries from anxious parents and media • Discuss children's fears concerning possible terrorist attacks
ELEVATED *(Yellow)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to the proper authorities • Ensure all emergency supplies stocked and ready • Obtain copies of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter and send it home with students in grades K-12, staff and faculty
GUARDED *(Blue)*	• *Complete recommended actions at lower level* • Be alert to suspicious activity and report it to proper authorities • Conduct safety training/emergency drills following the school's written emergency plan for all grades • Ensure emergency communication plan updated and needed equipment is purchased • Continue offering lessons from 'Masters of Disaster" curriculum for grades K-8 regarding emergency preparedness for natural disasters
LOW *(Green)*	• Use Red Cross Emergency Management Guide for Business and Industry to develop written emergency plans to address all hazards including plans to maintain the safety of students, staff, and faculty, as well as an emergency communication plan to notify parents in times of emergency. Disseminate relevant information to families of children, staff and faculty. • Initiate offering "Masters of Disaster" curriculum for grades K-8 regarding emergency preparedness for natural disasters • Ensure selected staff members take a Red Cross CPR/AED and first aid course

Your local American Red Cross chapter has materials available to assist you in developing preparedness capabilities.

ARC 1465 (Rev. 8-2002)

American Red Cross

Together, we can save a life

Homeland Security Advisory System Recommendations

Businesses

Risk of Attack	Recommended Actions
SEVERE *(Red)*	• *Complete recommended actions at lower levels* • Listen to radio/TV for current information/instructions • Be alert to suspicious activity and report it to proper authorities immediately • Work with local community leaders, emergency management, government agencies, community organizations, and utilities to meet immediate needs of the community • Determine need to close business based on circumstances and in accordance with written emergency plan • Be prepared to work with a dispersed or smaller work force • Ensure mental health counselors available for employees
HIGH *(Orange)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Review emergency plans to include continuity of operations and media materials on hand • Determine need to restrict access to business or provide private security firm support/reinforcement • Contact vendors/suppliers to confirm their emergency response plan procedures • If a need is announced, contact nearest blood collection agency and offer to organize a blood drive
ELEVATED *(Yellow)*	• *Complete recommended actions at lower levels* • Be alert to suspicious activity and report it to proper authorities • Contact private security firm for security risk assessment and to determine availability of support/reinforcement • Contact voluntary organizations you support to determine how you can provide assistance in case of emergency
GUARDED *(Blue)*	• *Complete recommended actions at lower level* • Be alert to suspicious activity and report it to proper authorities • Dialogue with community leaders, emergency management, government agencies, community organizations and utilities about disaster preparedness • Ensure emergency communication plan updated to include purchase of needed equipment. • Ask the local Red Cross chapter to provide a "Terrorism: Preparing for the Unexpected" presentation at your workplace for employees
LOW *(Green)*	• Use Red Cross Emergency Management Guide for Business and Industry to develop written emergency plans to address all hazards. Include an emergency communication plan to notify employees of activities; designate an off-site 'report to' location in case of evacuation. • Develop continuity of operations plan to include designating alternate work facility/location for business • Arrange for staff to take a Red Cross CPR/AED and first aid course • Obtain copies of Terrorism: Preparing for the Unexpected and Preparing Your Business for the Unthinkable brochures from your local Red Cross chapter for distribution to all employees/management as appropriate.

Your local American Red Cross chapter has materials available to assist you in developing preparedness capabilities.

ARC 1466 (Rev. 8- 2002)

Mr. SHAYS. Mr. Wermuth.

Mr. WERMUTH. Thank you, Mr. Chairman, committee members, for the opportunity to be here today to address this important issue.

Mr. Chairman, according to my count, this is the fourth time I have had the pleasure of being before this committee in that many years. I would also say that before September 11th, I could have counted on both hands the number of people who were providing national leadership on this issue, and of course, the chairman ranks among those people before September 11th.

My remarks today are going to be focused on relevant research and related activities in connection with the congressionally mandated advisory panel to assess domestic response capability for terrorism involving weapons of mass destruction, also known as the Gilmore Commission.

In accordance with its statutory mandates, the advisory panel delivered its fifth and final report to the President and the Congress on December 15th of last year. The strategic visions, themes and recommendations in that report were motivated by the unanimous view of the panel, that its final report should attempt to define a future state of security against terrorism, one that the panel chose to call America's New Normalcy.

In developing that report, panel members all agreed at the outset that it could not postulate as part of its vision a return to a pre-September 11th normal. It was the panel members' intention to articulate a vision of the future that subjects terrorism to a logical place in the array of threats from other sources that the American people face every day, from natural diseases and other illnesses to crime to traffic and other accidents, to mention just a few.

That report focuses on conceptualizing a strategic vision for the Nation that in the future has achieved in both appearance and reality an acceptable level of capabilities to cope with the uncertain and ambiguous threat of terrorism as part of dealing with all hazards. In developing that strategic vision, the advisory panel was guided by the recognition that the threat of terrorism can never be completely eliminated and that no level of resources can prevent the United States from being attacked in the future.

The panel believes that the Nation is achieving a critical understanding of the risk posed to America by terrorism, an understanding that derives from America's inherent strengths, the strength in our Constitutional form of government and, in particular, the strength of our people.

As a group of American citizens with broad experience in government at all levels and in the private sector, the panel members can see from those national strengths an ability to respond to the threat of terrorism with firm resolve and through concrete actions across the full spectrum of awareness, prevention, preparedness, response and recovery.

Its goal was to articulate a strategy to achieve a steady state 5 years into the future, a vision shaped by a broad and well-grounded American perspective on the threat of terrorism and focused particularly, because of this panel's mandate, on State and local response entities.

As part of that vision, the panel depicts a desirable state 5 years in the future in a number of specific areas, including, among them, State, local and private sector empowerment; intelligence, information sharing; and enhanced critical infrastructure protection.

Of course, a true national alert system will have an impact certainly in those four areas; and potentially in what the panel addressed. But as you have heard from other witnesses, the Homeland Security Advisory System, any true alert system or warning system, however you would like to couch it, is only one piece of a much more involved and complex process of intelligence collection, analysis and dissemination, and information sharing. As was mentioned by the previous panel of witnesses, the actual status of response capabilities, the assessment of vulnerabilities, which are part and parcel of what the Department of Homeland Security is doing, as well as those at the State and local level and the private sector, and the responsibility and the authority to act.

After the panel described a future vision that included the words, "The national warning system has been refined to provide more geographically and sector-specific information, based on the actual or potential threats, as its vision of the future." It went on, in a following section that it called a Roadmap for the Future, to articulate a specific recommendation based on the following conclusions.

The panel said, "The Homeland Security Advisory System has become largely 'marganilized,'" was the term that they used. "This may be attributed to a lack of understanding of its intended use as well as the absence of a well orchestrated plan to guide its implementations at all levels of government and within the public. The Governor of Hawaii chose to maintain a blue level in February when the Federal Government raised its level to orange. And the Governor of Arizona announced that his State would likely do the same thing based on particular threats."

Organizations surveyed by RAND for the panel had a number of suggestions for improving the Homeland Security Advisory System. Between 60 and 70 percent of State and local organizations suggested providing additional information about the threat type of incident likely to occur, where the threat is likely to occur, and during what time period, to help guide them in responding to the change in threat.

And I have included, for the committee's information, an actual extract of that survey of some 1,200 State and local response organizations, as well as the tabular information on how they responded based on their own disciplines.

The panel specifically said, "We recommend that DHS revise the Homeland Security Advisory System to include using, one, a National Alert System to notify emergency responders about threats specific to their jurisdiction; two, providing training to emergency responders about what preventive actions are necessary; and three, creating a process for providing specific guidance to potentially affected regions or sectors when threats are changed." All of that just affirms what you have heard from other witnesses this morning.

But several points are really worthy of consideration here. First, an alert process of this type is neither a total solution nor a single point of failure. Second, it is, by its own title, advisory. It does not require anything. Most importantly, most importantly, any alert

system will only be as effective as the intelligence upon which it is based, making that function especially critical. And without delving into continuing deficiencies in the whole intelligence and information collection, analysis and dissemination, I respectfully call the panel's attention to the extensive discussion of that subject contained in the advisory panel's fifth report.

Mr. Chairman, State and local governments, as you well know, and as other members of the subcommittee know, have a threshold responsibility for public safety and health. And they must do things that they determine are best for their own jurisdictions within their own existing resource constraints.

With better assessments, with better alerts, based in large measures on more comprehensive and focused threat information, they will be able to make more well informed decisions.

As the committee has already heard this morning, there have been changes in recent days. Over the end of the year holiday period, the flights from Europe that the chairman talked about earlier, all of those, in our opinion, are steps in the right direction. I would even venture to say that perhaps the advisory panel might not have been as specific in its recommendation now as it was in the fall of last year, because there are improvements that are headed in the right direction.

But the Federal Government still needs to do a better job. It needs to do better about engaging States and localities and the private sector in part of that process. The Terrorist Threat Integration Center [TTIC], may—and I stress "may"—prove to be a valuable tool in that direction, but only time will tell.

Some States and even some major cities have taken more upon themselves to be able to make valid risk assessments based on information that they derive from a lot of sources, and the private sector is becoming more involved as well.

So, in conclusion, I would say that progress is being made. DHS has indicated a new amount of flexibility and innovation in the way that they are now handling the advisory system. There are probably some other fairly significant things that could be done. I did not include any specific recommendations beyond the panel's recommendation in my testimony, but I do have an opinion or two about maybe some specific things that could be done if anyone would like to ask for that during the question-and-answer period.

Mr. Chairman and members, again, thanks for the opportunity to participate. I look forward to your questions.

Mr. SHAYS. Thank you, Mr. Wermuth, thank you very much.

[The prepared statement of Mr. Wermuth follows:]

TESTIMONY

Improving Terrorism Warnings – The Homeland Security Advisory System

MICHAEL A. WERMUTH

CT-220

March 2004

Testimony presented to the House Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations on March 16, 2004

Published 2004 by the RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Statement of Michael A. Wermuth[1]
Senior Policy Analyst
The RAND Corporation
and
Executive Project Director
Advisory Panel to Access Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

Before the Committee on Government Reform, Subcommittee On National Security, Emerging Threats, and International Relations
U.S. House of Representatives

March 16, 2004

Mr. Chairman and subcommittee Members, thank you for giving me the opportunity to appear before you today, to address the important issue of ways to improve terrorism alerts.

My remarks today will be focused primarily on relevant research dedicated to, and the resulting related recommendations of, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the "Gilmore Commission")(established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105thCongress, 2nd Session)(October 17, 1998), as amended).

Fifth Report to the President and the Congress

Overview

In accordance with its statutory mandate, the Advisory Panel delivered its *Fifth Annual Report to the President and the Congress* (the *"Fifth Report"*) on December 15, 2003. The

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

strategic vision, themes, and recommendations in that report were motivated by the unanimous view of the panel that its final report should attempt to define a future state of security against terrorism—one that the panel chose to call "America's New Normalcy."

In developing that report, panel members all agreed at the outset that it could not postulate, as part of its vision, a return to a pre-September 11 "normal." The threats from terrorism are now recognized to be a condition that we must face far into the future. It was the panel members' firm intention to articulate a vision of the future that subjects terrorism to a logical place in the array of threats from other sources that the American people face every day—from natural diseases and other illnesses to crime and traffic and other accidents, to mention a few. The panel firmly believes that terrorism must be put in this context of the other risks we face, and that resources should be prioritized and allocated to that variety of risks in logical fashion.

The report attempts to project a future—five-year—equilibrium state of well-established and sustained measures to combat terrorism. It focuses on conceptualizing a *strategic vision* for the nation that, in the future, has achieved in both appearance and reality an acceptable level of capabilities to cope with the uncertain and ambiguous threat of terrorism as part of dealing with all hazards. The report also makes specific findings and recommendations on process and structure that must be addressed to move from general strategies to specific accomplishments—including the issue under review today by this subcommittee.

In seeking to develop a strategic vision of the future of homeland security, the Advisory Panel was guided by the recognition that the threat of terrorism can never be completely eliminated and that no level of resources can prevent the United States from being attacked in the future. At the same time, the panel believes that the nation is achieving a critical understanding

of the risks posed to America by terrorism, an understanding that derives from America's inherent strengths—the strength in our Constitutional form of government and particularly the strength of our people.

As a group of American citizens with broad experience in government at all levels and in the private sector, the panel members could see in those national strengths an ability to respond to the threat of terrorism with firm resolve and through concrete actions across the full spectrum of awareness, prevention, preparedness, response, and recovery—areas already familiar to a society that has successfully responded to a wide array of natural and man-made disasters. Its goal was to articulate a strategy to achieve a "steady state" in the next five years—a vision shaped by a broad and well-grounded American perspective on the threat of terrorism and supported by a profound increase and sustainment of our preparedness *especially at the State and local levels*.

Alert System as Part of a Larger Process

As part of that future vision, the panel depicts a desirable steady state five years in the future in several specific areas:

- State, Local, and Private Sector Empowerment
- Intelligence
- Information Sharing
- Training, Exercising, Equipping, and Related Standards
- Enhanced Critical Infrastructure Protection
- Research and Development, and Related Standards
- Role of the Military

A national alert system will obviously have implications in several of these functional areas, especially the first three and in critical infrastructure protection. It is, however, only one piece of a much more involved and complex process of intelligence collection, analysis and dissemination; information sharing; the status of response capabilities; the assessment of

vulnerabilities; and the responsibility and authority to act. Here is what the panel specifically said, for example, in its future vision with respect to intelligence:

> *The improvements in both threat and vulnerability assessments have enabled DHS to produce overall national risk assessments for critical target sets (such as infrastructures and national icons) and to aid State and local governments in high-risk target areas in performing site- and community-specific risk assessments, including real-time risk assessments that respond to new actionable intelligence. These data are beginning to guide the allocation of preparedness funding but not to the exclusion of low-threat areas. The national warning system has been refined to provide more geographically specific information based on the actual or potential threats.*[2]

The Specific Recommendation

After having articulated its vision for the future, the panel then turned to what it titled as a following section "A Roadmap to the Future." In that section, the panel recommended ways in which a future of the type that it envisioned might become reality. There, the panel addresses the Homeland Security Alert System as follows:

> The Homeland Security Advisory System has become largely marginalized. This may be attributed to a lack of understanding of its intended use as well as the absence of a well-orchestrated plan to guide its implementation at all levels of government. The Governor of Hawaii chose to maintain a blue level in February 2003 when the Federal government raised the level to orange, and the Governor of Arizona announced that his State might do the same based on the particular threat or lack thereof to Arizona.[3] Organizations surveyed by RAND for the panel had a number of suggestions for improving the Homeland Security Advisory System. Between 60 and 70 percent of State and local organizations suggested providing additional information about the threat (type of incident likely to occur, where the threat is likely to occur, and during what time period) to help guide them in responding to changes in the threat level.[4]
>
> **We recommend that DHS revise the Homeland Security Advisory System to include (1) using a regional alert system to notify emergency responders about threats specific to their jurisdiction/State; (2) providing training to emergency responders about what preventive actions are necessary at different threat**

---

[2] *Fifth Report*, page 16.
[3] See Hhttp://www.bizjournals.com/pacific/stories/2003/02/24/story4.htmlH, February 7, 2003; Hhttp://www.azcentral.com/arizonarepublic/news/articles/0601homeland01.htmlH.
[4] See the related survey question and the resulting tabulation attached (from the Advisory Panel *Fifth Report*, page D-7-2).

levels; and (3) creating a process for providing specific guidance to potentially affected regions when threat levels are changed.[5]

Having said that, Mr. Chairman and Members, several points are worthy of consideration. First, the alert process is neither a single solution nor is it itself a single point of failure. Second, it is by its own title only advice. It is not a requirement to do anything; it is not really even a specific request to do things. Most important, any alert system will only be as effective as the intelligence upon which it is based, making that function especially critical in this context. Without delving into continuing deficiencies in intelligence collection, analysis, and dissemination in this hearing, I would respectfully call to the attention of the Chairman and subcommittee Members the extensive discussion on that subject in the Advisory Panel's *Fifth Report.* Clearly, there will always be a massive amount of intelligence and other information from a wide variety of sources to be processed at any given point in time by intelligence, enforcement, and responses entities. Separating true "signal from background noise" will continue to be a daunting challenge, unless and until collection sources and methods improve dramatically.

The Role of States, Localities, and the Private Sector

Mr. Chairman, it is a verity to say that State and local governments have a fundamental and threshold responsibility for public safety and health. Those entities must do that in ways that they determine best for their own jurisdiction within existing resource constraints. In the terrorism context, not all States and not all local jurisdictions, even those of similar size, will necessary be "equal" in terms of risk—in this framework, a consideration of threat *and* vulnerability. With better risks assessments, based in large measure on more comprehensive and focused threat information from the Federal level, specific States and local governments will be

[5] *Fifth Report*, page 27.

able to make more well-informed and effective decisions on measures to take when alerts are issued.

State and local jurisdictions have, in recent months, complained that raising the national alert level caused them to expend inordinate additional resources for law enforcement overtime and other increased security measures. Given the lack of more comprehensive or focused threat information, it is easy to understand how such a reaction may be viewed as a political necessity—the public will not understand, absent better explanations, why their own State or locality does not do something "more" when the national alert level goes from Yellow to Orange.

The private sector likewise has an important role but also has a requirement for better threat information in order to be able to make its own cost and operationally effective decisions as a means of insuring against catastrophic losses and ensuring the safety of its workforce. It will not do, however, for corporate governance to sit back and expect governments—at whatever level—to give them all the answers or to provide all the resources.

Recent Developments

The Federal government is getting better at analyzing and disseminating threat information, although much more needs to be done to make this process more effective. The Terrorist Threat Integration Center (TTIC) may—I stress may—prove to be a valuable asset in "moving the ball down the field." Time will tell.

Many States and localities continue to get better in this process every day. Examples of how that process is working fairly well are New York City, the Los Angeles Operational Area,[6] and the State of California. There are a number of others.

The private sector, especially those in critical infrastructure sectors, is becoming more engaged and starting to recognize their own responsibility as part of the process.[7]

[6] A consortium of 76 county and municipal jurisdictions.

Most important, DHS has, in just the last 90 days, changed—in certain instances fairly dramatically—the way it is determining and issuing heightened alerts. Over the 2003 end of the year holiday period, DHS initially raised the alert from Yellow to Orange nationwide—prudently, I would suggest, based on certain credible threat information that was not geographically or sector specific. After a few days, the nationwide alert was once again lowered, but certain localities and sectors were advised to maintain a heightened (Orange) alert status.

A similar process was used when various international flights were cancelled or postponed around Christmas and New Years, and again in January and early February of this year. Those situations did not even involve raising the level for the entire aviation sector.

Conclusion

Progress is being made. DHS is showing flexibility and innovation in the way they are now handling alerts. States, localities, and the private sector are, in my opinion, starting to understand the ambiguity of threats from terrorists and learning to adapt in a variety of ways. I would venture to say that the Advisory Panel would be somewhat more comfortable with the alert process today than it was when it decided to make its *Fifth Report* recommendation on revising the Homeland Security Advisory System in the fall of last year.

Mr. Chairman and Members, again my thanks for inviting me to participate in this important hearing. I welcome your comments and questions.

---

[7] The Advisory Panel recently endorsed one such effort along these lines. See its recommendation on page 30 of the *Fifth Report*, and the related information on the "Business Roundtable's Principles of Corporate Governance," at Appendix N of that report. More information is also available at Hhttp://www.businessroundtable.org/pdf/984.pdfH.

ATTACHMENT—Extract of RAND Survey of Federal Preparedness Programs for Combating Terrorism and Related Results

83. In your opinion, what modifications, if any, would improve the usefulness of the Homeland Security Advisory System for your organization?

(Mark All That Apply)

1 ☐ Use a regional alert system to notify emergency responders about threats specific to their jurisdiction or region

2 ☐ Provide more detailed information through existing communications channels (not the media) as to what type of incident is likely to occur

3 ☐ Provide more detailed information as to where the threat is likely to occur

4 ☐ Provide more detailed information as to during what period of time the threat is likely to occur

5 ☐ Provide training to emergency responders as to what protective actions are necessary at different threat levels

6 ☐ After an increase in threat-level, have the DHS follow-up on what additional actions ought to be undertaken

7 ☐ Other *(please specify)*: _____

_____

8 ☐ **No improvements are necessary to the Homeland Security Advisory System.**

_____

Table 7B. Suggestions for Improving the Usefulness of the Homeland Security Advisory System With Respect to Threat Information Provided

	PERCENT OF ALL ORGANIZATIONS		
	"Provide more detailed information through existing communications channels as to the type of incident likely to occur"	"Provide more detailed information as to where the threat is likely to occur"	"Provide more detailed information as to during what period of time the threat is likely to occur"
Local Response Organizations			
Law Enforcement	71 (5)	77 (5)	65 (6)
Local/Regional EMS	75 (5)	67 (5)	61 (5)
Local OEM	75 (5)	73 (6)	62 (6)
Paid/Combo Fire	67 (7)	80 (4)	69 (5)
Volunteer Fire	69 (8)	59 (9)	49 (9)
State Organizations			
State EMS	72 (5)	65 (5)	66 (5)
State OEM	76 (6)	88 (5)	76 (6)
Health Organizations			
Hospital	75 (5)	60 (8)	63 (8)
Local Public Health	–	–	–
State Public Health	–	–	–

Standard error of the estimate is shown in parentheses. Local and State public health not asked this question. (Question 83)

Mr. SHAYS. And, Dr. Carafano, thank you.

Dr. CARAFANO. Thank you, Mr. Chairman. Thank you for inviting me to speak on this important topic.

I have a lengthy statement for the record which I will submit. I would like to briefly summarize the high points of that, which are why I think this is an important subject; the good things I think which are going on, which I don't think have been touched on enough; some concerns about the current system; and then, I think, a look to the future of what we really need to think about for the long term.

I think it's worth just reviewing and why this is important is four reasons: First and foremost is, I think the HSAS could be a key tool for welding the disparate national, Federal, State and local systems we have into a national system, which I truly think is the Federal role, is getting the resources where they need to be, when they need to be, for what they think needs to be done to protect American citizens.

The second is, I do think that a properly run system can have an effect in terms of preventing, deterring and mitigating terrorist acts. I think that is an important fact.

The third one, which has already been touched on, is there are enormous physical implications for this. It is widely reported it costs the Federal Government $1 billion a week to let the system—the Conference of Mayors says it costs about $7 million dollars for local jurisdictions to do this. So every time we change the level, the physical implications are really large, and those need to be taken into account.

And, fourth, I think we really need to look at the long-term psychological impact that this system will have on the Nation. I strongly encourage further research in that area to determine how Americans are really going to react to this system over the long term.

Just very quickly in terms of the good things that are going on, that I think deserves to be mentioned. The Homeland Security Council is playing an increasingly important role. They meet each time the level is changed. I think there is good coordination, at least from the outside, across Federal agencies in terms of coordinating Federal efforts to respond to the changing alerts. I think that is important.

I think at the deputies level behind the scene, there is an improving increase in coordination. I think that is good.

I think the Homeland Security Operations Center that the Department of Homeland Security has established, is an important asset. It plays an important role in managing the implementation of the system. It is a credit to the Department that they have stood it up, and the role that it plays. And I do think the announcement that Secretary Ridge made of the Homeland Security Information Network, which was mentioned in the last panel, is important and most important because I think it will provide a collaborative tool at a classified level that allows key people at Federal, State and local levels to communicate with each other, which in the end is really important to making the advisory part of this system important.

I do have several concerns. On the Federal level, my primary concern is with the TTIC, the Terrorist Threat Integration Center, and that I think in the future the TTIC should play an increasingly important role in implementing HSAS, in determining when it should be implemented and how it should be implemented. As I talked about before, I am concerned that TTIC is not under the Department of Homeland Security, I don't think that is what the intent of the Homeland Security Act of 2002—I don't think it allows the Secretary to actually fulfill his role.

I mentioned a number of recommendations in the report. I think in the end the IA portion of IAPA in TTIC need to be fully integrated. I think they need to be under DHS. I think the Secretary of DHS needs the legislative authority over the TTIC similar to the kinds of things that the JCS has over who can participate in the joint staff, that were implemented in the Goldwater-Nichols reforms.

I do think that the problem with the system is at the State and local and public level. I understand what DHS has said, but the perception is that the HSAS is the key risk management communication tool to the Nation. And the general consensus is that it lacks useful guidance to actually be that. I mean, you can say what you want, but the research shows that if a warning is credible, specific, understandable and actionable, it is not a warning.

I would recommend delinking the color code from the warnings that we give to State and local and the public. I think, as mentioned before, the State and local warnings need to be regional and functional in nature.

As I mentioned, I think DHS has been moving in that direction. After we changed back from code orange at Christmas, they kept a specific alert on for the airline industry and certain airports. I think that is a sign that they are moving in the right direction.

I think the other key piece to this is, we really need national performance standards, because State and local governments are never going to be able to act appropriately unless they know what is expected of them. And I am very supportive of the Cox-Turner Bill. I think that would be a step in the right direction, in putting in a requirement for these standards to be in place, because I think they are a key part of what we need to do to have a good system.

The public system, I think we need to move to a simple, two-tiered system, a watch-and-warning system similar to what we do for weather alerts. People are already conditioned to that. I mean, we need a simple standard. We need to tell people what we can when we can. We need to provide specific directions and specific actions; otherwise, these warnings are simply not meaningful.

I also think we need to have realistic expectations about what we can expect. The research shows that, by and large, unless people are conditioned to a disaster, if they have had experience in a forest fire or earthquake or something, that they tend not to prepare. And so we can put out all the warnings that we want, but unless we have a really serious education system in this country, it is unlikely that people are going to do much with these warnings.

And even if we do have an extensive education system, it is really questionable what kind of large impact it is going to have in terms of raising public preparedness. And I just—I—as we look to

the future, one of the most important things you need to think about is the back end of the system. We don't spend near enough time on that. We are talking about getting alerts to people, but what we need to do is start training the next generation of leaders at the State and local level and private industry, who know how to react to these alerts.

One of the things I did in preparing for this testimony is, I screened about 100 Web sites from State and local governments and various industries, and the results are uniformly disappointing. Most people take the Federal color code system, and they just put that page up on their Web site. They say, here is what to do. So we are not training the next generation of leaders who can really react to nuanced warnings officially. And I have a series of recommendations in my testimony which I will be happy to go into.

With that, I will conclude my statement. Thank you.

Mr. SHAYS. Thank you, Doctor.

[The prepared statement of Dr. Carafano follows:]

Statement of Dr. James Jay Carafano
Senior Research Fellow
The Heritage Foundation

Before the House of Representatives Committee on Government Reform

Subcommittee on National Security, Emerging Threats and International Threats

The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2003, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2003 income came from the following sources:

Individuals	52%
Foundations	19%
Corporations	8%
Investment Income	18%
Publication Sales and Other	3%

The top five corporate givers provided The Heritage Foundation with 5% of its 2003 income. The Heritage Foundation's books are audited annually by the national accounting firm of Deloitte & Touche. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Chairman Shays, Ranking Member Kucinich, and other distinguished members, I am honored you asked me to testify before the committee today. This hearing focuses on what I believe to be one of the most critical components of our emerging national homeland security system: the means for alerting the nation about potential terrorist acts.

One of the most important actions taken by President Bush's administration in the wake of the September 11 attacks on New York City and Washington was establishing a national homeland security strategy. In turn, the strategy defined the six critical missions required to protect U.S. citizens from the threat of transnational terrorism.[1]

The first critical mission area is intelligence and early warning. It includes activities related to detecting terrorists and disseminating threat information and warning.

[1]White House, National Strategy for Homeland Security, 2002, pp. 15-46.

Central to the success of this mission is the development of programs that promote intelligence sharing across the public and private sectors. Effective intelligence sharing is a prerequisite for exploiting the full potential of national capabilities to respond to potential terrorist threats.

The Homeland Security Advisory System (HSAS) is an important component of the intelligence and early warning mission area. The HSAS employs a series of color codes to designate various levels of national preparedness in anticipation of a terrorist attack. Associated with each threat condition are a range of suggested protective measures (such as implementing various contingency plans), with federal, state, and local agencies responsible for developing and implementing their own specific response activities.[2] Since the system has been established, the HSAS threat condition has been raised five times over the last two years.

Getting the HSAS exactly right is critical for four reasons.

First, the Administration envisions the HSAS serving as one of its key tools for integrating federal, state, local, and private-sector responses. Thus, it is potentially a vital tool for wielding these disparate capabilities into a true national preparedness and response system.

- *Second,* if effectively employed, the HSAS may help prevent, deter, or mitigate the effects of a terrorist attack.
- *Third,* the HSAS has significant fiscal implications. The $10 million requested for funding the system in FY 2005 is not an issue of concern. On the other hand, implementation of the HSAS could have a significant impact on future requirements for supplemental funding. Increased security resulting from changing the alert status requires an estimated $1 billion per week at the federal level. The additional costs incurred by state and local governments and the private sector, as well as the impact on the economy overall, such as reducing consumer confidence or affecting business travel and tourism, are more difficult to estimate, but no doubt significant.[3]
- *Fourth,* how the HSAS is employed may have a significant psychological impact on the nation. It is not clear what the long-term mental health impact may be or how frequent and ambiguous changes in threat condition may undermine the system's responsiveness.

My research explores these issues from the perspective of the impact of the HSAS on executing the national strategy and how changes in alert status affect the overall state of national preparedness. In my testimony I would like to cover three points: 1) the positive aspects of the present system, 2) concerns over how the HSAS is currently

---

[2]Presidential Homeland Security Directive–3, March 2002, at *www.whitehouse.gov/news/releases/2002/03/20020312-5.html.*

[3]For example, the U.S. Conference of Mayors estimates the cost at approximately $70 million per week. New York City spends about $5 million per week when the alert level is raised. Boston estimated its costs at about $100,000 per day.

organized, and 3) what long-term issues must be addressed to ensure that the HSAS can effectively serve the nation for years to come.

The Nation on Watch

The HSAS was established by presidential directive in March 2002. The U.S. Attorney General assumed overall responsibility for implementing the system.[4] Subsequently, the Homeland Security Act of 2002 placed responsibility for intelligence and early warning activities squarely on the shoulders of the Secretary of the Department of Homeland Security (DHS). According to the legislation, it is the responsibility of the DHS Assistant Secretary for Information Analysis and Infrastructure Protection (IAIP):

> (1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to--(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland.[5]

Section 201 of the law also assigns IAIP responsibility for administering the HSAS.

I would like to start off by commending Secretary Ridge on the work that he has done in implementing the HSAS, both at the Office of Homeland Security and as DHS secretary. The war on terrorism is likely to be a long, protracted conflict, and the DHS has the difficult task of being on watch right now against possible terrorist threats and building a robust homeland security that must stand for decades. The DHS has achieved a lot given the short time frame of its existence and the magnitude of the challenge it faces. With regard to the HSAS, there are clearly some things that have gone right.

It is worth noting that the Homeland Security Council (HSC) and the council staff have played an important role. When the HSAS threat condition is elevated, the HSC convenes to ensure that the federal response is integrated and appropriate. At the deputies level, behind the scenes a steady stream of policy directives and strategy planning documents suggests ongoing and improving coordination under the direction of the HSC staff. Particularly commendable was the rapid development and implementation of domestic security measures (Operation Liberty Shield) resulting from the increase in threat level during Operation Iraqi Freedom.

The HSC must always play a central part in the implementation of the HSAS to ensure that federal agencies undertake protective measures commensurate with changes in alert level and the nature of the threat that prompted the need for heightened security

---

[4]Presidential Homeland Security Directive–3, March 2002, at *www.whitehouse.gov/news/releases/2002/03/20020312-5.html.*
[5]Public Law 107-296, Sec. 201.

measures. Indeed, at the national level the HSAS appears to be achieving its stated goal on ensuring the coordinated employment of protective measures across the federal government.

Also noteworthy is the development of the Homeland Security Operations Center (HSOC) in the DHS. The center is responsible for consolidating information and putting out warnings. This consolidation has been long-overdue and contributes to the Department of Homeland Security's ability to see the "big picture" and manage implementation of the HSAS.

The February 24 announcement of the establishment of the Homeland Security Information Network was also welcome news. HSIN will link states, territories, and major urban areas to the HSOC through the Joint Regional Information Exchange System (JRIES). Initially, the system will be limited to sensitive-but-unclassified information, but in the future it is intended to carry secret information to the state level. A collaborative tool such as HSIN is essential for establishing the interactive communications necessary to support implementation of the HSAS.

Additionally, the DHS has undertaken programs to make average citizens more aware of their role in how to prepare and respond to terrorist attacks. The DHS Web site *Ready.gov* provides appropriate, clear, and jargon-free advice on how to respond to chemical, nuclear, biological and radiological dangers.

Concerns and Recommendations

That said, there are areas relating to implementation of the HSAS that raise issues that Congress should carefully consider.

In particular, it is becoming increasing clear that the management of the Terrorist Threat Integration Center (TTIC) will be critical to the long-term success of the HSAS. Established by President Bush in 2003, the TTIC is staffed by an interagency group responsible for gathering, assessing, and disseminating all terrorist-related information to federal agencies. The Administration intends for TTIC to be the place where all the dots get connected and the right information gets to the right people, at the right time. Over the long term, it is likely that the TTIC will be providing the key intelligence assessments that determine changes in the HSAS.[6]

Currently, the Director of Central Intelligence provides oversight of TTIC, and most of the TTIC staff are from the Central Intelligence Agency. The DHS plays only a subordinate role. Policies on operations and the functions and duties of DHS personnel, and other participating agencies as well, are governed by an interagency memorandum of understanding.

---

[6]For concerns over the TTIC's current operations, see Second Report of the Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security*, 2003, p. 3.

Establishing TTIC separate from the DHS is problematic. The current arrangement appears to conflict with the intent of the Homeland Security Act of 2002 and raises concerns over whether such an approach will optimize intelligence sharing overall and the implementation of HSAS specifically. It is deeply troubling that the DHS, as the primary consumer of intelligence for providing domestic security, does not have primary control over the mechanisms for fusing and disbursing information.[7]

The current arrangement leaves the DHS as little more than just another intelligence end user, competing with other members of the national security community to ensure that its priority requirements are met and that it has the information it needs to manage the HSAS.

The Congress should consider measures to strengthen the role of the DHS in TTIC. The best course would be to merge TTIC and the intelligence functions of the DHS Information Analysis and Infrastructure Protection Directorate (IAIP) into a single interagency staff under the supervision of the DHS. In addition, the DHS secretary should have authority over all TTIC-related appropriations. Finally, the DHS should have authority to approve, evaluate, and establish the education and experience requirements for all TTIC staff, much as the Pentagon's Chairman of the Joint Chiefs of Staff has legislative authority to designate qualified personnel from the military services to attend the joint staff.

A second major concern is the "one-size-fits-all" nature of the national alert system, amply demonstrated when recent changes in the HSAS brought America its first "orange" Christmas—the second-highest danger level. Currently, when the HSAS is raised to orange, the whole nation ratchets up security—even in areas where no credible threat is made. This is because the current system does little or nothing to inform state and local governments as well as the American public of specific threats. As Dan Goure, a national security specialist with the Arlington, Va.-based Lexington Institute, concluded, "We have a better system for rating movies."[8]

The limitation of the current system is its all-inclusive nature. During the Cold War, the Pentagon established DEFCON (defense condition) levels to ramp up the readiness of its forces to respond to global contingencies based on changes in the nature of the Soviet threat. At the same time, civil defense systems were developed to alert local authorities and the general public of impending attacks. One system was designed to enhance levels of preparedness, the other to alert public safety officials and the public of imminent emergencies.[9] The HSAS attempts to efficiently combine both these attributes in a single system. Given the large and diverse population and infrastructure of the United States, this is a daunting and perhaps unachievable task.

---

[7]James Jay Carafano and Ha Nguyen, "Better Intelligence Sharing for Visa Issuance and Monitoring: An Imperative for Homeland Security," Heritage Foundation *Backgrounder* No. 1699, October 27, 2003, at *www.heritage.org/Research/HomelandDefense/BG1699.cfm*.

[8]James Jay Carafano and Ha Nguyen, "Warning: We Need a Better Warning System," Commentary, January 8, 2004, at *www.heritage.org/Press/Commentary/ed010804a.cfm*.

[9]Gary A. Kreps, "The Federal Emergency Management System in the United States: Past and Present," paper presented at the 12th World Congress of Sociology, Madrid, Spain, July 1990.

On the other hand, we should not scrap the current system entirely. It appears to work well at the federal level, where assets are under centralized control and deployed by people with unfettered access to classified intelligence. Washington needs an integrated system to add or subtract from the levels of security at our borders, at sea, and around key assets. The HSAS threat conditions are evolving into an appropriate instrument to accomplish that goal.

Application of the HSAS to state and local governments, as well as the private sector, is more problematic. A survey of various state and local response organizations, done by the Gilmore Commission, showed overwhelmingly that these organizations want more information on the type of attack, where it is likely to occur, and when.[10] Currently, few have the classified intelligence and the sophisticated analytical capabilities to evaluate threats. Lacking concrete assessments, many states, counties, and cities typically react in two ways: do nothing or pile on layers of possibly unneeded security that generate exorbitant overtime costs and other expenditures.

That is not to say that the nation requires a standardized system that solicits uniform responses from every state and local government. In fact, just the opposite is needed. Research suggests that diversity is natural and desirable. Public safety and emergency response entities are more effective by adapting their operations to local conditions.[11] The HSAS needs to be flexible enough to serve all their needs.

Of even greater concern is the impact of shifts in the threat level on average citizens. Many appear perplexed by changes in threat condition. Though the HSAS is intended to serve a variety of purposes, it is perceived by many as primarily a warning system for the general public. That's a problem. The HSAS does not meet all the expectations of an effective public alert system.

Public alerts must be credible, specific, understandable, and actionable by individuals.[12] Arguably, the change in color code, which dominates the public perception of what the HSAS represents, is none of these. For example, when the national alert level is changed, local officials may take no publicly discernable action because they have no specific information of threats in their area. In February 2003, when the federal government changed the national threat condition to code orange, the Governor of Hawaii chose to maintain a blue level of alert. The Governor of Arizona suggested that

---

[10]Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty*, Fifth Annual Report to the President and the Congress, Vol. 5, December 15, 2003, p. D-7-2, at *www.rand.org/nsrd/terrpanel/volume_v/volume_v.pdf.*

[11]Russell. R. Dynes *et al.*, "Disaster Analysis: Local Emergency Management Offices and Arrangements," Final Report, No. 34., University of Delaware, Disaster Research Center, 1986.

[12]Kathleen J. Turner *et al.*, *Facing the Unexpected: Disaster Preparedness and Response in the United States* (Washington, D.C.: Joseph Henry Press, 2001), p. 30.

Arizona might do the same, depending on threats to the state[13] For average citizens, these responses are incongruous, raising questions about the overall credibility of the HSAS.

The lack of specificity over the nature of the alert and the absence of clear guidance on what actions need to be taken by individual citizens is problematical as well. The American Red Cross, recognizing the public confusion over the color-coded system, has issued its own guidelines for preparedness by the private sector.[14] This advice, and the recommendations given in the DHS *Ready.gov* Web site as well, include practical measures that should be taken every day to ensure public safety and prepare for all kinds of natural and technological (i.e., man-made) disasters. They do not, however, suggest significant changes in behavior when the threat status shifts from one color to another. Thus, even citizens who have studied the Red Cross guidance provided might well be puzzled over how to react to the HSAS alerts.

Additionally, there is a real question over whether any national alert system will have a significant effect on enhancing public preparedness. A considerable body of research suggests that many individuals change patterns of behavior or take precautionary measures in preparation for disasters only after they have had some personal experience with that threat. Additionally, the perceived need for preparedness recedes as the event becomes more remote.[15] Given that few Americans have experienced, or are likely to experience, a terrorist attack, such findings do not bode well for the effectiveness of the HSAS as a means of risk communication to the general public. Certainly, at the least, significant additional and tailored pre-alert education and continuous reinforcement will be needed to convince a significant number of Americans to take common-sense precautions in anticipation of a terrorist attack over threat periods that may span several years between major attacks.

While color-coded alert may not spur greater preparedness, it could have unintended adverse psychological consequences, fostering a "fortress America" mentality or increasing anxiety among some individuals. Since age, socioeconomic, and sociodemographic factors can significantly condition preparedness and public response to warnings,[16] significant additional research may be needed to determine the long-term mental-health impact of the HSAS and its capacity to reach a growing and increasingly diverse U.S. population.

Responsible voices, including former Virginia Governor James Gilmore, who chaired a prestigious national commission on terrorism, along with Representatives Christopher Cox, R-Calif., and Jim Turner, D-Texas, have called for revising the alert system. The report also concluded that the Homeland Security Advisory System has become largely marginalized. This panel believed that "this may be attributed to a lack of

---

[13] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty*, p. 27.
[14] American Red Cross Homeland Security Advisory System Recommendations for Individuals, Families, Neighborhoods, Schools, and Businesses, at *www.redcross.org/services/disaster/beprepared/hsas.html.*
[15] Kathleen J. Turner *et al.*, *Facing the Unexpected: Disaster Preparedness and Response in the United States* (Washington, D.C.: Joseph Henry Press, 2001), pp. 34-43.
[16] *Ibid.*, pp. 167-188.

understanding of its intended use as well as the absence of a well-orchestrated plan to guide its implementation at all level of government."[17] The Gilmore Commission goes on to make a series of useful suggestions for improving the HSAS.[18]

As a minimum, I recommend the following solutions:

- *That the public color-coded portion of the Homeland Security Advisory System be scrapped.* Rather than a complex, vague, multi-tiered system, a simple two-tiered system similar to that used by the National Weather Service,[19] to which the public is by and large already conditioned to respond, might be more appropriate.
- *Public alerts, when appropriate, should be issued in brief, simple, and clearly worded watch or warning reports that average people can understand.* Officials should tell people what they can, when they can, then let them make their own choices on how to respond. These reports must contain specific threats and specific actions that should be taken. An objective system would probably merge terrorist alerts into an "all hazards" alert system with common formats and methods of dissemination.
- *Replace the national alert to state and local governments with regional alerts and specific warnings for different types of industries and infrastructure.* In fact, the DHS is already moving in this direction. As the department has become more sophisticated in analyzing threats and communicating information, it has been issuing more audience-tailored warnings. For example, after the DHS lowered the national threat level on January 9, 2004, it continued higher levels of security for commercial aviation and specific air routes.[20] This practice will no doubt become easier and more routine once the DHS completes its comprehensive risk-level ranking of all areas in the country. Hopefully, the ranking will address criteria such as population, threat assessment, number of important sites, and level of vulnerability, and then classify areas as low, medium, or high risk.
- *Establish standards of preparedness and response for state and local authorities.* National performance standards will provide a guide to help state and local governments determine what they need to do to counter terrorist threats and what help they should expect from the federal government.[21] In turn, these assessments will assist in establishing appropriate security measures for each of the HSAS threat conditions.

---

[17] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty*, p. 27.
[18] For concerns and recommendations on revising the system, see *ibid.*, pp. 27, D-1, and D-7-2.
[19] In the National Weather Service system, the first level warning, a "watch," indicates that conditions are for severe weather. The second level is a "warning," indicating severe weather is imminent or underway.
[20] Jamey Loy, testimony before the House Select Committee on Homeland Security, February 4, 2004, p. 2.
[21] James Jay Carafano, "Homeland Security Grant Bill Needs Revision, But a Step in the Right Direction," Heritage Foundation *Executive Memorandum* No. 909, January 8, 2004, at *www.heritage.org/Research/HomelandDefense/EM909.cfm*.

With more specific alerts, DHS, in cooperation with other federal agencies and state and local authorities, will be better able to apply scarce resources to address the higher threats. Congress should consider providing additional appropriations in the FY2005 budget to support revamping the HSAS.

Looking to the Long Term

Finally, I would like to briefly discuss the issues that must be addressed to ensure that the HSAS evolves into an integrated component of a true national preparedness and response system and remains effective for decades.

A legitimate concern with regard to the HSAS is that overuse will lead to apathy among civilians. This is known as the Cry Wolf Syndrome, a subject that engenders some controversy. Some argue that the syndrome is a myth. In particular, they contend that the response of the "internal" audience (e.g., public officials and emergency responders) to alerts can actually be strengthened by frequent alarms. Using the system provides an opportunity to test readiness and refine procedures. On the other hand, other research suggests that the public "external" audience (individual citizens) can be adversely affected by alarms that are not followed by the appearance of an actual threat.

Instances of the cry-wolf scenario have been documented. For example, at a Seton Hall University dorm in 2000, 18 false fire alarms had caused students to ignore the fire alarms. As a result, when a real fire did break out, students continued to ignore the alarms and three people died in the blaze.[22]

According to a research paper entitled "The Warning Process: Toward an Understanding of False Alarms" and a survey conducted by Eve Gruntfest and Kim Carsell of the University of Colorado at Colorado Springs, most people who issue public safety alerts have a fear of false alarms that directly impacts their decision to issue warnings to the public. In fact, 54 percent of such responders to the survey said that fear of false alarms delays their decision to notify the public.[23]

In contrast, there are numerous experiences where alerts of "imminent" threats that did not materialize subsequently did not lead to degradation in responsiveness. For example, during World War II, when air raid sirens sounded in London, German bombers were headed toward the city. However, increasingly as the Battle of Britain progressed, British air defenses would drive off the air attacks or make them less effective. Yet citizens responded with alacrity to each alert. Similarly, residents in tornado-prone areas routinely react to severe-weather warnings, even when funnel clouds have not appeared overhead for years.

In each of those instances, the public had a clear understanding of the threat and of how to respond to it. In contrast, the United States may see long periods when terrorist

---

[22] Eve Gruntfest and Kim Carsell, *The Warning Process: Toward an Understanding of False Alarms*, at *http://web.uccs.edu/geogenvs/ecg/falsealarms/understandingfalsealarms.html.*
[23] *Ibid.*

dangers represent "potential" rather than imminent dangers. Thus, the HSAS could be more prone to degraded public response over time.

The fact that al-Qaeda operatives took five to seven years to plan and execute the September 11 terrorist strikes is a cause for concern. It could well be a half-dozen years before the HSAS faces its next great test. There is a compelling requirement for additional research to determine the long-term prospects for the HSAS to remain an effective public alert system with regard to intermittent terrorist threats.

More work is also needed to explore how modern information technologies can be used to enhance the public portions of the HSAS. Currently, the government relies on an emergency broadcast system that interrupts broadcast television, radio, and cable programs to inform the public of emergency events.[24] The system is not sufficiently robust, however, to meet the needs of HSAS, nor does it exploit the Internet and multi-media and telecommunications capabilities of the information age. Additional research is required to determine how best to leverage all these capacities, as well as the costs and benefits of integrating HSAS with other alert systems such as the AMBER alerts employed by various states and the National Weather Service advisory system.

Finally, and perhaps most important, more attention needs to be given to the capacity of the emerging national preparedness system to best exploit the warnings that may be provided by an effective HSAS. Particular focus should be placed on human capital and leader development programs that will be required to train the next generation of homeland security professionals, public safety leaders, and government officials.[25] After all, it will be the actions of these men and women, not the alerts themselves, that will determine whether the nation is safer in the years to come.

Currently, the nation lacks an overall homeland security training and education strategy. The advanced degree program offered by the DHS through the U.S. Naval Post-Graduate School is one admirable initiative, but it is not enough. Other professional development opportunities for emerging senior leaders are also needed. The Massachusetts Institute of Technology, for example, conducts a program called Seminar XXI for the federal government. Seminar XXI provides a year-long series of lectures and workshops for mid-grade professionals on international affairs. A similar program targeted on homeland security might be equally useful. In the same manner, the national community might benefit from the establishment of a national homeland security university modeled on the military's war college system.

Finally, any national leader development effort will have to include a plethora of state and local leaders. The nation's network of junior colleges, which have become the

---

[24] Partnership for Public Warning, "The Emergency Alert System (EAS): An Assessment," PPW Report 2004-1, February 2004.

[25] For an overview of homeland security training and education programs, see James Jay Carafano, "Homeland Security and the Trouble with Training," CSBA *Backgrounder*, October 3, 2002, at *www.csbaonline.org/4Publications/Archive/B.20021003.Homeland_Security_/B.20021003.Homeland_Security_.htm*.

hub of continuing adult education throughout the country, may provide the best venue for offering appropriate leader development opportunities.

Over the long term, the capacity of the national homeland security system to exploit the advantages of intelligence and early warning will be more dependent on the quality of the decisions made by its leaders and the programs they implement than on the structure of the HSAS. The nation would be well served if equal attention was paid to both sides of the equation.

I, again, thank the committee for the opportunity to testify on this vital subject and I look forward to your comments and questions.

Mr. SHAYS. Mr. Allen.

Mr. ALLEN. Thank you, Mr. Chairman, members of the committee. My name is Kenneth Allen. I am the executive director of the Partnership for Public Warning. I appreciate this opportunity to appear before the subcommittee to talk about the Homeland Security Advisory System, but most of all, I want to talk about the public.

The objective of a public warning system is to provide people at risk with timely and accurate information so that they can take protective action. Effective public warnings can save lives, reduce property losses and speed economic recovery.

Public warning empowers citizens by providing them with the information they need during times of emergency to make informed decisions and take protective actions. Four years ago, the President's National Science and Technology Council issued a report concluding that many in our society are at risk because we do not have an effective national public warning system. That message was confirmed on September 11, 2001.

On that terrible day, not a single national public warning system was ever activated. The Partnership for Public Warning was established in January 2002 by concerned emergency management officials from around the country. Because public warning is an issue that encompasses all levels of government and relies upon a private-sector infrastructure, PPW was created as a nonprofit, public-private partnership.

We are the only national organization addressing the issue of public warning. And let me emphasize that many of our members and many of the proponents of the creation of PPW were the local and State officials and emergency managers involved in this issue. In fact, the chairman of our board is the director of the Florida Management Agency, so we are truly a public-private partnership.

Less than 3 months after our creation, the government proposed the Homeland Security Advisory System. We provided comments on the initial proposal and have continued to monitor it and evaluate the system.

In June 2000, we hosted a 4-day workshop with experts from government, industry and academia to look at the proposed system. The most significant finding was the one that the chairman noted earlier, this is not a complete warning system. It is merely a threat advisory system. It tells us that something may happen, but it doesn't tell us what, where or when.

The best description I have heard of the HSAS is that it is America's "mood ring," and even a mood ring probably comes with more specific actions such that if it is black, you need to get help. We need to address that issue.

As a result of the workshop, we provided recommendations in 2002 to the Office of Homeland Security. Last November, as people began to look at the HSAS and Secretary Ridge talked about making changes, we decided that someone ought to ask the public and local and State government what they thought about it; and we initiated our own request for public comment.

The comments we received included the following points: The current system is too vague. It is inconsistent with existing alert and warning scales. It would be more effective if it used standard

terminology and message formats. When there is a change in the threat level, State and local officials should be notified before the public is notified. One color does not fit all. Advisories should be tailored to specific geographic regions, industry sectors and other potential targets.

A terrorist warning system should be developed to complement the advisory system. It should be linked to existing alert and systems such as the emergency alert system, and NOAA weather radio. And most of all, we should employ a multitude of technologies to reach people when there is a risk.

After almost 2 years of operation under the HSAS, I think it is clear from the record and this hearing that changes are needed. A more useful system, an effective system, can and should be developed.

We are not here today to criticize those who developed the HSAS. This is a complex and difficult challenge; and we believe that the system in place has been a good first step, and the Department of Homeland Security is to be commended on its efforts. It is time for us to work together, however, on a more effective solution.

In my testimony, I have some of the elements of an effective public warning system. Applying those elements to the HSAS, we have the following recommendations: one, make the threat advisory scale consistent with other existing threat scales; two, refine the system to provide information on a local, regional and industry-specific basis; three, provide more guidance regarding the protective actions that citizens should take; four, develop a public warning system for terrorist threats to complement the threat advisory scale; five, integrate the HSAS with existing public alert and warning systems and move toward the national public warning capability; and six, collaborate with State and local government, the private sector and the public on the development of a more effective terrorist alerting system.

The last two recommendations are the most important. Americans do not expect their government to preserve and protect them from all risk. The public, however, does expect the government will at least provide timely and effective information on imminent risk. Many, if not most, Americans believe that an effective national warning capability exists. It does not.

Existing national alert and warning systems are fragmented and uncoordinated. Individuals at risk often fail to get timely information, fail to understand or act on the information, and often do not know where to go for additional information.

Those not at risk who receive warnings of little relevance may come to view the system with skepticism if not distrust. The HSAS is an example of this fragmentation. Instead of building upon existing alert and warning capabilities, we have created another system and layered it on top of what we already have.

The solution is a national integrated public warning capability that can be used to alert the public during all types of the emergencies, from terrorism to national disasters to accidents. We have done some work in that area, and I would be glad to talk to the committee if you wish to pursue that.

But our final and most important recommendation is the need for cooperation and partnerships. Protecting our Nation's security

must be a collaborative effort in which government, industry and the public work together. This is especially true if we were to develop an effective Homeland Security Advisory System.

The Federal Government cannot develop an effective system on its own; no organization or individual has all the answers. Moreover, local and State governments, private industry and the public must understand and implement a terrorism warning system. To do so effectively, those stakeholders should be part of the process to design and operate the system.

We urge the Department of Homeland Security to participate in a collaborative forum with all of the stakeholders.

September 11th taught us that the unthinkable can happen. Future tragedies, whether natural or manmade, are not a matter of if but when. Lives can be saved and losses reduced through effective public warning. Americans expect their government to protect them and believe an effective warning capability exists. It doesn't exist today, but we can put it in place quickly if we work together. There is no excuse for further delay. This is an important issue. We commend the committee on its leadership in this area and look forward to working with you. Thank you.

[The prepared statement of Mr. Allen follows:]

PARTNERSHIP FOR
PUBLICWARNING
www.PartnershipForPublicWarning.org

Embargoed until
10:00 AM
March 16, 2004

TESTIMONY BEFORE THE
HOUSE OF REPRESENTATIVES SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS
COMMITTEE ON GOVERNMENT REFORM

"THE HOMELAND SECURITY ADVISORY SYSTEM: THREAT CODES & PUBLIC RESPONSES"

March 16, 2004

Mr. Chairman and Members of the Committee:

My name is Kenneth Allen, and I am executive director of the Partnership for Public Warning (PPW). William Craig Fugate, chairman of the PPW Board of Trustees, regrets that he cannot be here today. However, Mr. Fugate is director of the Florida Division of Emergency Management, and his legislature is currently in session. On behalf of the Partnership, I appreciate this opportunity to appear before the subcommittee to discuss the Homeland Security Advisory System (HSAS).

Timely and effective public warnings can save lives, reduce property losses and speed economic recovery. Public warning empowers citizens by providing them with the information they need during times of emergency to make informed decisions and take protective actions. The objective of a public warning system is to provide people at risk with timely and accurate information regardless of their location, the time of day or night or any special needs.

Four years ago, the President's National Science and Technology Council issued a report which concluded that many in our society are at risk because we do not have an effective means of warning them about impending emergencies such as natural hazards, chemical spills and other accidents. On September 11, 2001, we learned that we did not have the capability to warn citizens of terrorist attacks. On that terrible day, not a single national warning system was activated.

The Partnership for Public Warning was established in January 2002 by concerned emergency management officials from around the country. Recognizing that public warning is an issue that encompasses all levels of government and relies upon a private

7515 Colshire Drive M/S N655
McLean, VA 22102
TEL: (703) 883-2745
FAX: (703) 883-3689

sector infrastructure, PPW was created as a non-profit, public-private partnership. PPW provides a collaborative, consensus-based forum where government and industry are working together to develop the standards, processes, policies and educational materials needed to create an effective alert and warning capability. PPW is the only national organization dedicated to working on public warning issues.

Less than three months after the Partnership for Public Warning was established, the Federal Register of March 18, 2002 included a notice describing the then-proposed Homeland Security Advisory System. In addition to responding to that initial request for comments, the Partnership has continued to monitor and evaluate the HSAS. I am therefore pleased to discuss this important issue with the committee.

On April 25, 2002, the Partnership for Public Warning submitted written comments that discussed the nature of public warnings and identified significant issues that should be considered in the development of any alert or warning system for terrorism.

Believing that this issue deserved more attention than was possible during a 30-day comment period, the Partnership convened a four-day workshop where emergency management and warning experts from government and industry reviewed and discussed the proposed system. Participants included experts from the social sciences, physical sciences, emergency management community, public warning and communications industries and federal law enforcement. The conclusions and recommendations that emerged from this workshop were provided to Governor Tom Ridge, Director of the Office of Homeland Security in a July 5, 2002 letter.

In November 2003, the Partnership solicited public comments on the operation of the Homeland Security Advisory System. These comments were provided to the Department of Homeland Security in a December 30, 2003 letter to Frank Libutti, Undersecretary for Information Analysis and Infrastructure Protection. Copies of all three reports have been provided to this committee and are available on the PPW web site at www.PartnershipforPublicWarning.org. I would like to review our initial recommendations, summarize the most recent public comments, answer the specific questions raised by the committee and provide some thoughts on how to move forward.

The most important point that emerged from the PPW workshop in 2002 was the conclusion that the Homeland Security Advisory System is a "*threat assessment system*" and not a complete warning system. The five colors can tell the public that something may happen, but it does not identify what or where – it does not warn citizens when an attack is imminent. The best description I have heard is that the HSAS is "America's mood ring." Based on this conclusion, the experts who participated in the June 2002 workshop made the following recommendations:

1. **Develop clear standards for deciding on changes in threat condition and for reviewing suggested changes. Have these standards reviewed by experts in the**

Administration and private sector. Publicize the existence of such standards. Build credibility for the process.

2. **Base the threat-level scale on the probability/imminence of a terrorist attack. Do not include potential gravity or risk. If the risk is not high, express this information separately.**

3. **Develop ways to be more specific about what is likely to happen, where, when, over what time period and how likely it is. Be clear about the risks and the actions required to reduce the risks. People are unlikely to take actions that expend their limited resources without credible, specific information.**

4. **Consider changing the name of HSAS to accurately describe it as a threat assessment system and indicate that the advisory (warning) system is being developed.**

5. **Recognize that effective warning is an ongoing evolutionary process that involves consistent use of terminology, thoughtful planning, training, and meaningful public education. The need for an ongoing long-term commitment and continual reevaluation and quality improvement is shown clearly by decades of experience in developing warning systems to prevent/reduce a variety of natural and social problems.**

6. **Move towards development of a national, all-hazards warning system. Americans must respond to more natural hazards and accidents each year than to acts of terrorism. Unifying the terminology and approach will provide better response to warnings about terrorism.**

7. **Use the power of existing emergency response plans, practices and procedures to engage State and local governments in the development and use of the HSAS. Emergency response to disasters (including warnings) usually starts at the local "incident" level. The state's role is to supply resource requests from local government. The federal role is to back up state response.**

8. **Recognize that actions taken outside the federal government will be based in part on actions taken by the federal government, because the federal government is the primary source of information on terrorism.**

The above recommendations were based on many years of social research and the experience of emergency management experts and authorities. We believe that these recommendations remain valid today.

It has now been almost two years since the Homeland Security Advisory System was put into place. It is an appropriate time to evaluate the effectiveness of that system.

We note that Secretary Ridge and other senior DHS officials have acknowledged that the HSAS needs to be refined. We also note that several Congressional committees have expressed similar concerns. As part of the FY 2004 budget process, the House and Senate Appropriations Committees have directed DHS to provide a report on how to improve the system.

The Partnership for Public Warning felt that it would be useful to ask local and state governments – and the public – for their comments on the HSAS. Towards that end, PPW initiated a request for public comments last November. The comments we received including the following points:

- **The current system is too vague. It does not provide sufficient information to enable the public to understand the nature of the threat. Emergency managers and the public are unclear as to what protective actions should be taken.**

- **The HSAS is inconsistent with existing alert and warning scales such as the current FBI 4-tiered Threat Level System, the DOD THREATCON and the numerous threat scales used by other federal agencies. This multiplicity of different scales can create confusion in the minds of the public.**

- **The HSAS would be more effective if it used standard terminology and message formats – similar to those being developed for other warning systems.**

- **When there is a change in the threat level, state and local officials should be notified before the public. A standard, minimum time should be established between the notification to the proper authorities and notification to the public.**

- **One color does not fit all. Advisories should be tailored to specific geographic regions, industry sectors and other potential targets. Models or templates should be developed to guide this tailoring process.**

- **The HSAS is merely a threat advisory system; in its current incarnation it cannot be used to warn the public of an imminent terrorist attack. A terrorist warning system should be developed and it should be linked to existing alert and warning dissemination systems such as the Emergency Alert System and NOAA Weather Radio.**

- **The federal government should develop a terrorist alert and warning system that is not dependent solely upon the news media for dissemination of information to the public. Such a system should employ a multitude of distribution channels and technologies.**

The commentors who responded to the PPW request also provided a number of specific recommendations for improving the Homeland Security Advisory System. These recommendations ranged from getting rid of the system to reducing the number of colors and eliminating the colors in favor of a threat scale consistent with other existing systems.

Before I provide our suggestions as to how we can move forward, I would like to address the specific questions raised by the committee.

What process is used to determine the Homeland Security Advisory System threat level?

The Partnership for Public Warning is not in a position to answer this question, as we are not involved in the process for determining the threat level.

However, as we have noted in our previous comments on the HSAS, public credibility will be significantly enhanced if there is a well described and understood process for changing the threat level and releasing information. The research into public warnings has demonstrated that one of the most important factors in an effective public warning is the credibility of the warning source. When people understand, believe and trust the source of a warning, they are more likely to take the appropriate protective actions.

Clearly, much of the information used to assess the threat level is classified and cannot be released to the public. However, there is no need to do so if there is a clear and codified process for assessing threats and making decisions about the correct threat level. At a minimum, this codified process would include the process by which data is evaluated, the criteria to be used for increasing or decreasing the threat level, the organizations and people involved in the decision making process and the methods and protocols for disseminating information.

What are the specific means of communication used to disseminate threat level information to federal agencies, state and local authorities, private industry and the public?

It is our understanding that there are a number of specific channels for disseminating threat information to government agencies and key industry sectors. Our primary interest is in how threat information is disseminated to the public.

Currently, changes in the threat level and information regarding specific threats are disseminated to the public via press release. Although the media does an excellent job of distributing the information, not everyone is listening to the radio or television. While as many as 22% of the population may be listening to the radio at any given time of the day, fewer than 1% are listening in the middle of the night. The average television set is in use only 31% of the day, and most of us turn the television off when we go to sleep.

Relying upon the media may not be a problem if the purpose of the HSAS is solely to advise the public that something may happen at some indeterminate point in the future.

Most people will eventually read a newspaper or listen to the radio or television. Sooner or later almost everyone will hear the news.

However, if there is the danger of an imminent attack, and there is a need to warn the public immediately, the HSAS will not be effective. This is especially true if the threat emerges in the middle of the night – when few people are listening to the radio or television.

As we have previously suggested, there needs to be a public warning component developed to complement the threat advisory system. Moreover, the warning system should be linked to existing dissemination systems such as the Emergency Alert System and NOAA Weather Radio. In the longer term, there is a need to develop a comprehensive and integrated national public warning capability that uses multiple technologies --- computers, telephones, cell phones, PDAs, etc. – to deliver warnings to the public.

<u>What types of information are passed to federal agencies, state and local governments, private industry and the public?</u>

PPW does not know what information is passed to federal agencies, state and local governments and private industry. We are aware of the information that is shared with the public.

To date, whenever the threat level has been raised, the public has been provided with very general information that there may be some type of threat to the United States. In most instances, there has been little specific information as to the exact nature of the threat or where it is most probable. The public has also been provided with only general suggestions about what to do. These suggestions range from being more vigilant to putting together a home survival kit. We believe that more specific information needs to be provided. Moreover, as a result of the research that has been done, we know what makes an effective warning.

The first objective of a warning is to get people's attention – to get them to realize that something is happening (or about to happen) that is important enough to be worthy of some of their time and thought. This is easiest when there is a clear, perceivable threat such as an approaching tornado or hurricane. When the threat is less perceptible, such as a toxic cloud or a potential terrorist attack, sufficient information must be provided just to get people's attention. Once you have their attention, they will seek information in order to decide whether the event will affect them and what, if any, action to take. If official information is not available, they will get it from less authoritative sources, or discount the threat, reasoning that if the threat were really serious, the government would provide additional information. The public wants specific information and details upon which to base decisions. The more detail that is provided, the greater the chance that the public will pay attention and consider options. It is important to remember that a warning is intruding into people's lives, seizing their attention, and urging them to modify deeply embedded behaviors.

Intermediaries and the general public will be seeking as much information about an event as possible. While not every piece of information will be equally relevant to every person, among the information that should be considered as part of any public warning is the following:

- **Hazard information**
  - **Type of hazard**
  - **When**
  - **Where**
  - **Intensity**
  - **Duration**
  - **Source that identified the hazard**
- **Vulnerability**
  - **Demographic characteristics (static and dynamic)**
  - **Population density**
  - **Population profile**
  - **Access to escape routes**
  - **Environmental characteristics**
  - **Infrastructure**
- **Risk**
  - **Probability**
  - **Projected numbers of individuals affected**
  - **Types of impacts**
- **Possible actions**
  - **Ways to reduce impact**
  - **Protective actions**
  - **Recovery actions**
- **Additional Information**
  - **How to obtain**

As noted above, not every member of the public will need all of the above information. Provided below is an example of the type of information that might be sought by a homeowner threatened by an approaching hurricane.

Hurricane Warning Information for Households

Threat Information

Type of event	**Hurricane**
Types of threat	**Storm surge, wind, inland flooding, tornadoes**
Target location	**What are the threats at their location?**
Impact area	**Where else are there threats? Should they change locations?** **Width of threatened coastline**

	Inland extent of surge, wind, and flooding
Magnitude (Intensity)	What is the impact to them? Saffir-Simpson scale Depth of surge/flooding and wind speed at critical locations
Time of onset	Estimated arrival time of tropical storm winds and surge
Duration	How long tropical storm winds and surge will last?
Probability	Expected landfall location and radius of hurricane winds, storm category, arrival time, duration
How vulnerability varies by structure and location	For single family structures, multi-family structures, mobile homes

Recommended Actions

Protection for persons	Evacuation Sheltering in-place
Protection for property	Strengthen building envelope (install shutters) Secure contents (bookcases, refrigerators) Turn off utilities (gas, electric power, water)
Further information	Contact point for further information (EAS station, NOAA Weather Radio) Contact point for assistance in protective response Environmental cues Social sources/conditions

Clearly, the warning process for a hurricane, or any other hazard, requires communicating a great deal of information quickly and concisely. This is best achieved when the population has been given previous training and education.

One essential characteristic of an effective public warning system is the use of uniform terminology for all hazards and consistent messages. Disasters have many similarities, regardless of whether the cause is a natural hazard, accident or act of terrorism. This is true because the mechanisms that harm people and property, such as fire, building collapse, toxic chemical release, or floods, are the same regardless of how these mechanisms are triggered. Alerting people at risk to an impending disaster, or notifying them about an ongoing disaster, involves the same kinds of activities no matter what the cause of the disaster. The goal in each case is to get people's attention, to provide information about what is happening, and to get them to take appropriate action. Effective

warnings must be communicated clearly and succinctly. Unfortunately, there is frequently little similarity in the warning terminology used by different government organizations.

Even at the community level, it is not uncommon to find that each type of emergency event employs different terms and warning scales. As a result, people at risk may not recognize or understand a warning when it is heard. It is far more effective to use consistent terminology and warning scales. People at risk would understand warnings much better if the terminology were standard for all types of hazards.

In developing standard terminology it is important to use:

- **Easily understandable "trigger words"**
- **Words that are simple and memorable to the great majority of people**
- **Words that are transferable across different hazards**
- **Words that translate into other languages with similar meanings**
- **Words that can be used in many different media such as a 10-character mobile pager, a 12-character cell phone, a 60-character short messaging appliance, a newspaper article, a half-hour television documentary.**

By using standard words, training and education are facilitated. This would alleviate the problems associated with having multiple threat scales, or scales that people rarely hear about. For example, on September 10, 2002, National Public Radio interviewed tourists at the Washington Monument about that day's increase in the Homeland Security Advisory Scale to level "Orange." Few of them knew that the level had changed, and none could identify what it meant. One man stated, "No, I'm not [aware of the HSAS change or level]. I mean, I barely get the pollution and the heat colors. Last week the kids were talking about purple. Like, I've never heard of purple." Another commented, "I'd rather see it high, low, medium, you know? It'd be easier to understand." The use of different terminologies for each warning system makes it difficult for the individual citizen to remember how each system uses the terms and hinders our ability to move easily from one system to another.

<u>What actions should federal agencies, state and local governments, private industry and the general public take once a threat level has increased from yellow (elevated) to orange (high)?</u>

The warning process consists of those with information communicating with individuals at risk and others, such as emergency responders, in advance of or during a hazardous event, with the intent that those at risk will take appropriate action to reduce casualties and losses. The goal of a warning is to prevent hazards from becoming disasters. The success of a warning is measured by what actions people take.

A warning prompts people to take immediate actions that save lives, reduce injuries and protect property. Terrorist attacks and other hazards, both natural and man-made, create disasters when they kill and injure people, destroy and damage property, and cause further economic and emotional problems by instilling a sense of unease and uncertainty into society. Such losses can and have been reduced when people receive an alert of what is likely to happen soon, or notification of what is happening and advice about what to do in response to the hazard. With such knowledge, those at risk can take appropriate action to get out of harm's way, to reduce losses, to reduce uncertainty and to speed recovery. Thus, a warning must provide the information and motivation for people to take informed action.

As we have already noted, the Homeland Security Advisory System is not a warning system – it is merely a threat advisory system. Moreover, the public has been provided with minimal guidance as to what specific actions to take and, in some instances, conflicting guidance. When the threat level was raised over the most recent holiday season, the public was advised to conduct business as usual and continue to make their holiday visits and trips. Such a message creates conflict in the minds of the public between the credibility of the threat and the need to take protective actions – if the threat is credible and serious, why are no changes in behavior warranted?

Having said that, the Partnership for Public Warning is not in a position to list those actions the public should take when the threat level is raised to orange (high). We believe the specific actions to be taken should be a function of the nature of the threat, its probability, risk and location. This requires greater specificity in the threat advisory system and the information that is disseminated to the public.

Our nation is at risk from terrorist attacks. We need an effective alert and warning system to communicate with the public and provide them the information they need to protect their lives and property. Creating such a system is not an easy task. The Homeland Security Advisory System has been a good first step towards a terrorist threat system and we commend the Department of Homeland Security for its efforts.

After almost two years of operational experience with the HSAS, it is clear that changes are needed. A more useful and effective system can be developed. The Partnership for Public Warning has the following recommendations for creating a more effective system.

<u>Moving Towards an Effective Public Warning System</u>

The Partnership for Public Warning supports the development of a truly effective system for warning the public about terrorist threats and attacks. A first step is understanding that developing an effective public warning system is a complex process that requires the integration and management of many different elements. Selecting a technology to disseminate warnings is often the easiest issue to address, as there are many

excellent technologies and systems available. Moreover, a comprehensive public warning system will employ not just one, but a multitude of technologies.

The key elements of the public warning process include:

1. **Data collection and analysis**

   Development or collection of data regarding a potential hazard and the analysis of that data by experts as to the potential risk associated with the hazard.

2. **Deciding to issue a warning**

   Review of the data and the expert analysis by the appropriate authorities and the reaching of a decision to issue a warning to the public.

3. **Framing the warning**

   Creating a warning message for the public that includes pertinent information such as the nature of the hazard, the risk, the affected area and the protective actions that are recommended.

4. **Disseminating the warning**

   Distribution of the warning through all appropriate and available channels. This could include sirens, the Emergency Alert System, the media and specialized warning services such as telephone dial-out. The warning is also disseminated to those with special needs (e.g. blind, deaf, non-English speaking).

5. **Public Reception**

   Members of the public at risk hear the alert and understand the warning.

6. **Validation**

   Before taking action, most members of the public will seek to validate the warning by going to alternate information sources to see if the same message is being sent.

7. **Take Action**

   Members of the public take appropriate protective action to protect themselves, their families and their property.

The above is a simplified overview of the warning process. Developing a successful warning strategy requires three things:

- **Planning**

  Long before an emergency occurs, the appropriate officials should develop plans for when and how to issue public warnings. Key elements in any plan include the criteria for issuing a warning, the officials with the authority to issue a warning, standard terminology and the methods of distribution.

- **Public Education**

  Just as important as the plan is the education of the public. Information needs to be provided to the public that explains how they will be warned, what the warnings mean (e.g. if a siren goes off is it calling the volunteer firemen to the station or signaling that citizens should stay in their houses?) and where to get additional information, especially if the power is off.

- **Testing and Evaluation**

  An effective warning system will be tested on a regular basis, both to make sure the system works and that individuals targeted for the warning understand the purpose and the message. Evaluation of the system by emergency managers, government officials, the media, private sector and the public can be invaluable in identifying ways to improve the communication of warning messages.

With regard to the Homeland Security Advisory System, we have the following recommendations.

1. **The threat advisory scale should be made more consistent with other existing threat scales.**

2. **The system should be refined to provide information on a local, regional and industry-specific sector basis (better targeting).**

3. **More detail should be provided regarding the protective actions that citizens should take at each threat level.**

4. **A public *warning* system for terrorist threats needs to be developed to complement the threat advisory scale.**

5. **The HSAS should be integrated with existing public alert and warning systems, and a national, all-hazard public warning capability should be developed.**

6. **The Department of Homeland Security should collaborate with local and state governments, the private sector, the non-profit community and the public to refine and operate the Homeland Security Advisory System.**

The last two recommendations are the most important.

Americans do not expect their government to preserve and protect them from all these risks. However, because of government's duty to promote the public welfare, and its unmatched ability to gather, analyze, and disseminate risk information, Americans do expect government to give them significant warning so they can act to limit damage to themselves, their property and their communities. Indeed, event post-mortems more often focus on the adequacy of warning than on the prudence of the public's response. For government, there is no escape from public judgment on its performance in warning those who subsequently become victims.

The public, reasonably, has a right to expect that government, if it cannot protect them, will at least effectively communicate to them critical advice and information on imminent risks. Many, if not most, Americans believe that an effective national public warning capability exists. It does not. While current warning systems are saving lives, they are not as effective as they can or should be.

Existing national alert and warning systems are fragmented and uncoordinated. With few exceptions, existing systems are unable to target only those people at risk, provide inconsistent messages, lack coordination, and are often not interoperable. Each program has its own scale for measuring risk and its own method for reaching those at risk. Existing systems also fail to reach many people at risk while warning and alarming many who are not at risk. As a result, individuals at risk fail to get timely information, fail to understand or act on the information and often do not know where to go for additional information. Those not at risk who receive warnings of little relevance may come to view the system with skepticism, if not distrust.

The Homeland Security Advisory System is an example of this fragmentation. Instead of building upon existing alert and warning capabilities, we have created another system with its own threat scale and distribution channels.

The Partnership for Public Warning believes that the answer is a national, integrated public warning capability that can be used to alert the public in all types of emergencies, from terrorism to natural disasters and accidents. The Homeland Security Advisory System should be part of a national all-hazard public warning capability that will provide citizens at risk during times of emergency with timely and useful information to enable them to take appropriate actions to save lives and property. Such a capability will:

- **Support multiple warning sources (President, federal officials, state officials, local officials and authorized private officials (e.g. nuclear plant));**
- **Take advantage of existing national assets such as Weather Radio and the Emergency Alert System;**
- **Enable local emergency managers to provide more effective public warnings;**
- **Ensure that only authorized officials may enter alerts and warnings;**
- **Be secure, redundant and available 24/7;**
- **Be based on an open, non-proprietary architecture;**
- **Employ uniform alert and warning terminology that is clearly understood by recipients regardless of geographic location;**
- **Support multiple languages and users with physical disabilities;**
- **Employ multiple distribution channels employing multiple technologies (e.g. telephones, cell phones, PDA's, personal computers, TV's, radios and other consumer electronics);**
- **Involve all public and private stakeholders in its development and operation.**

Creating this national capability is not a technology problem. We already have the technologies necessary to warn people in any location, at any time of day or night or in any language. The need is for standards, policies, procedures, and public education. An effective national public alert and warning capability can be developed relatively quickly for only a few million dollars. The Partnership for Public Warning has already begun work towards this capability. In addition to a recent assessment of the Emergency Alert System, PPW has promoted the development of the first-ever standard message format for warning – the Common Alerting Protocol. This protocol is about to be issued as a standard and is already in use in a number of jurisdictions.

For further information on what it will take to create a national alert and warning capability, I draw your attention to PPW's "*National Strategy for Integrated Public Warning Policy and Capability.*" This document sets forth a vision and a road map for creating an effective national, all-hazard alert and warning capability. We have also released a plan that identifies the specific actions needed to implement the strategy. Terrorism alerts should be an integral part of this national capability.

Perhaps the single most important recommendation is the need for cooperation and partnerships.

Protecting our nation's security must be a collaborative effort in which government, industry and the public work together. This is especially true if we are to develop an effective Homeland Security Advisory System. Despite its best efforts, the government cannot protect us from all threats, and no citizen would expect otherwise. It is therefore essential that there be an effective system for the government to communicate with us about the nature of the threats, the risks and what we can do to protect our families and ourselves.

The Federal government cannot develop an effective system on its own. Neither it – nor any other organization or individual – has all the answers. Moreover, local and state governments, private industry and the public must understand and implement a terrorism warning system. To do so effectively, these stakeholders should be part of the process to design that system. We urge the Department of Homeland Security to participate in a collaborative forum with local and state governments, the private sector and the public to create a system that is understood and supported by all sectors of our society. The Partnership for Public Warning has offered to assist the Department of Homeland Security in this endeavor, and we reiterate that offer today. Let us work together to develop a truly effective national alert and warning system.

September 11th taught us that the unthinkable can happen. Future tragedies – whether natural or man-made – are not a matter of if, but when. Lives can be saved and losses reduced through effective public warning. Americans expect their government to protect them and believe an effective warning capability exists. Although such a capability does not exist today, it can be put in place quickly if we work together. There is no excuse for further delay.

Public warning is an important issue, and we applaud the committee's interest in the Homeland Security Advisory System. We look forward to working with you on this vital issue.

Thank you.

Mr. SHAYS. I thank the gentleman.

One of my staff in hearing the issue of, you know, we are taking steps in the right direction, said it is hard to be satisfied with steps in the right direction. As former Senator Nunn points out, a gazelle being chased by a hungry cougar is taking steps in the right direction. Survival is a matter of velocity, speed, not vector direction. And I guess it is a combination of a lot of things, but interesting.

Mr. SCHROCK. How do I top that? Thank you all for being here. I want to start with Colonel Carafano. You mentioned that the TTIC, you thought it should fall under the Department of Homeland Security, but as a DOD function. Its product and analysis is integrated with the DHS Homeland Security Advisory System. If Secretary Ridge consults with his council before raising or lowering color codes, why yank it out of DOD?

Dr. CARAFANO. TTIC, now as I understand it, is statutorily run by the Director of Central Intelligence, and it is actually—it is an interagency group, obviously. It has DHS members. It's mostly CIA members. I think they're going to potentially go to about 250, and over half of those will be CIA. I think the intent of the Homeland Security Act of 2002 is that the Secretary of Homeland Security is responsible for the integration and dissemination of terrorist threat information.

It just seems to me that unless we have somebody that we can put a finger in the chest and say, "You are responsible for this," unless he is in charge of the resources of the organization and the membership of the organization, what the organization does, that we haven't truly met the intent of the law. And I know Mike has a different interpretation on who ought to have the rose pinned on him for this. I will let him chime in.

Mr. SCHROCK. Colonel Wermuth.

Mr. WERMUTH. Jim and I have had this discussion before.

Mr. SCHROCK. Obviously.

Mr. WERMUTH. I think the TTIC is appropriately placed somewhere other than within a single department. In the first place, the Department of Homeland Security doesn't own everything, even at the Federal level. More importantly, it's our experience in studying issues like this that when an entity becomes part of a single department, that's how it's viewed. It's part of that department. It doesn't tend to be viewed as something that can provide services outside the department, and clearly, the Department of Justice, Department of Health and Human Services, DOD itself and other Federal entities, much less States and localities, need some of the product that is generated from an organization like a TTIC.

So I would suggest that a TTIC-like entity does need to be placed not directly under a particular department of the Federal Government but more freestanding to do the broader strategic approach to fusing intelligence information, if you will, fusing it and analyzing it and disseminating it.

At the same time, Jim is absolutely right that the Department of Homeland Security needs more capability to take that information, maybe to take information from a lot of other sources, and process it, analyze it and disseminate it and make it actionable within DHS's own mission, which is of course to provide better alerts, better warnings, better advisories across this entire spec-

trum to States, localities, the private sector and perhaps the public at large. It's the level that, from my perspective, it's the level you're talking about. We need a broader, strategic, accountable organization like the TTIC; DHS needs an operational organization to do the same kinds of stuff for the execution of its own mission, both.

Dr. CARAFANO. If I could just add one point, one point on which we both agree is—I think it's a great recommendation in the commission report—there should be strong State and local representation in the TTIC so when we implement these alerts, we have people who understand what State and local people do and we can translate that quickly into language that State and local people can act on. I think that's a good recommendation.

Mr. SCHROCK. Mr. Allen, Colonel Wermuth talked about marginalization in the Gilmore Commission report, that the Advisory Panel states, "The Homeland Security Advisory System has become largely marginalized." Do you all believe that, and what actions should DHS take to make this system more credible?

Mr. WERMUTH. Well, for the reasons that the panel stated in much more detail than I did in the testimony, it has become marginalized because people now are not necessarily taking it seriously or taking different kinds of action that you might anticipate that they would take, for whatever reason, whether it's resource considerations or just local politics. I mean, there are reasons why States and localities might decide to choose to do something or not to do something just based on political realities.

I said in my remarks I didn't have any specific recommendations beyond what the panelists said, but now I'll offer one in response to Congressman Schrock's question.

I think we need two systems or maybe two components of a system, and it has been talked about here already, but we need a system that is a warning system for the people who have, as I referred to it in my remarks, the authority and the responsibility to take action. We need a system that is directed to States and localities and those elements of the private sector that are involved in critical infrastructure protection that really provides a more targeted, more focused, more specific level of threat information for those entities to take specific action.

Then it would seem we need a more general system—and Jim talked about this as well—that is directed to the public, that says to the public—he said two tiers; I might suggest three, a lower and a medium and a high one—that would say, at the low end, "You, the general public, are not expected to do anything." We have governments and the private sector that are taking actions in connection with certain things, one that is a little bit higher than that, that says, "You need to be more aware of your surroundings and, perhaps, take some specific actions," and a third level that says, "Gee, at this level, you really need to consider not traveling, doing things, you know, to be more observant, more vigilant of your surroundings."

But it seems like this broad five-tiered system that applies to everybody—all of the witnesses this morning have agreed—that's probably not a good idea, that there has to be more specific things focused on the segments of our society that have both the authority

and the responsibility to act, governments and those elements of the private sector that we've identified, the public at large, and I'm not sure you can devise a single system that would apply across that spectrum.

Now, having said that, we ought to tell the public if we have different processes, and we probably will eventually have different processes. As some different processes have already started being applied, let's tell the public about those, so it doesn't look like we're telling governments and selected people one thing and telling the public something else. Let's describe all of the processes to our public and let them take that information on board and do what they will with it, but it doesn't seem to be helpful to expect the public always to react to a change in threat levels when it really doesn't affect the entire public.

Mr. ALLEN. If I could just add to that, I would agree. One of the lessons of the risk communication is that different audiences respond differently to different warnings, and we are not—this is not one audience. State and local officials are one. Private industry officials are another. The public is another. Even the media is an important audience we should be dealing with, and we need to recognize and develop a system that can communicate with each of those effectively.

Second of all, and again, I will reiterate this again, we need to integrate this with other systems. We have between 10 and 20 different threat scales in this country for different hazards. Even in terrorism, the FBI has a four-tiered level, and we had DOD Threatcon. It's very confusing for folks to know which system applies.

Third, collaboration. Let's let State and local governments work with DHS and the private sector to develop a system that works for all of us.

And fourth and finally and a point that you made earlier is, we need public education. When we grew up in the 1950's and we had all of those civil defense programs and we practiced getting under the desk, we knew what to do in the event of an emergency.

When the Iron Curtain came down, somehow we lost sight of all of that, and it's time, perhaps, to spend a little bit of effort teaching the public simple things such as what does a siren mean if you hear one go off. In different parts of the country, it means different things. So public education is a key part of what we need to do.

Mr. SCHROCK. Let's follow on to HSAS for a minute. Since the creation of the HSAS, a number of issues have arisen and two, I think, that stand out: the vagueness of the warnings and the system's lack of protective measures. And various recommendations have been to refine the system, adding specificity to the alerts, and developing protective measures for the public.

Mr. Allen kind of touched on this, but how can we add more specificity about the nature of the threat when alert levels rise, and why don't we have recommended, standardized protective measures for State and local governments, private businesses and the public?

As Mr. Allen said, a siren going off in my hometown means there's a fire. In Kansas, it could mean a hurricane—I mean, a tornado. So how can we put that all together? Because there are so

many things out there, nobody knows what to believe. Consequently, everybody ignores everything.

Mr. ALLEN. You're absolutely right. And of course, in some places, a siren means gather all of the volunteer firemen.

Mr. SCHROCK. True.

Mr. ALLEN. Clearly you don't want to reveal sources of intelligence, and I don't think anybody is asking for that, but there are a couple of ways to deal with the issue. One is to create a codified process that the public understands. In other words, that we understand and the State and local officials understand how decisions are being made about raising or lowering the threat levels, what are the protocols and criteria used in that process, what are the protocols for communicating with people.

Right now the raising and lowering of the threat level is a black box to most in the public. We don't know what goes on inside that black box. We don't know what goes into that decision, and then we aren't sure what's going to be communicated and when. So you can deal with a lot of the problem by providing more information right up front about how decisions are made, how and when they are going to be communicated.

And then as you get down the road, you do need to put a process in place to share information with the public. We know from history that people generally do not panic, that they would prefer to have more information than less information. And most of all, as somebody said, let's not underestimate the intelligence of the American public, and let's share with them as much as we can.

Mr. SCHROCK. Thank you, Mr. Chairman.

Mr. SHAYS. Thank you.

Mr. Ruppersberger.

Mr. RUPPERSBERGER. I'd like to get more into the TTIC issue and where the information goes. Are you familiar with the analysis and coordination centers that certain States have developed? It just so happened last week I visited the Maryland analysis and coordination center, and I think, from my observations, it's working very well, because what you have there, it's more like a strike force concept. You don't have to worry about the bureaucracy and who is in charge, but you have FBI. You have CIA. You have NSA. You have State and local. You have Customs. You have Immigration. You have all of these groups. And what has been effective, I think, is that it's up and down. Information is flowing up and down.

Now, how would you analyze that—and that was really put together, I believe, out of necessity, because there was a lot of frustration, especially on the local level, that information was not coming from the hierarchy of the Federal level. How would you analyze that operation? And I understand Maryland's operation, I think, was one of the first, but it's being looked at and being implemented in other States. How would you analyze that as it relates to TTIC?

Mr. WERMUTH. I would say that certainly Maryland's effort is great. California, of course, has one that they call their California Terrorist Integration Center. The city of New York, of course, is another example of how a major municipality is handling the issue.

I would just say that all of those are important pieces of this entire process. A lot of them have been developed, as you said, Congressman, as a matter of necessity, because States and localities

felt like they were not getting enough information, and they had to do a better job at either the State or local level for coordinating it. But it goes back to the recommendation that the advisory panel made about the Terrorist Threat Integration Center. That's why it's important from the panel's perspective, why, in our view, the Terrorist Threat Integration Center, the Federal-level entity that looks at this strategically, has to have representation from organizations like the Maryland analysis center, like the California center, like New York, embedded into their staff on a day-to-day basis so that you have this complete perspective, not only from the Federal level but also from the State and local level.

Mr. RUPPERSBERGER. But do you see a duplication of effort occurring between that and this group?

Mr. WERMUTH. Not at all, because when you divide this, if you will, in military terms—strategic, operational and tactical—you need all of the elements. And the New York operation is tactical. The Maryland operation tends to be both operational and tactical, because it's working with the Maryland community. Same thing in California.

So all of these are complementary efforts. It's my same opinion about the TTIC being separate and independent so that it serves all of the customers, but other entities needing their other capability at the operational level inside departments. The Department of Treasury just formed a new intelligence and analysis center for money operations, for financial transactions by terrorists. I think all of those things are important, not duplicative but complementary depending on what the level of activity that you're talking about, tactical, operational or strategic.

Mr. RUPPERSBERGER. Let's get—yes?

Dr. CARAFANO. If I could follow on that. I really think the State and local analysis centers are essential, and they're really the missing piece of the puzzle and the piece that will allow us to get away from the blunt instrument we now have. Because what you need is—if you have these analysis centers that can really take the information and interpret it to understand what should be done in that local situation, then DHS can move away from the blunt instrument, and they can pass more focused analysis to the regional and the functional areas, and then they can do their analysis to interpret if it's applicable for them.

So I think these are complementary with TTIC, and I think something like HSIN, the Homeland Security Information Network, which could provide a bridge between TTIC and DHS and these other organizations so they can talk collaboratively, will really allow us to have a much, much more nuanced system.

Mr. RUPPERSBERGER. You said that you think those systems like the one that I visited in Maryland are very good, but there are some concerns about TTIC. What would your recommendation be? Is it because you don't have one boss, because you have a combination of FBI, CIA? And yet, in the analysis center, you have the whole group together. What would your recommendation be to make it more effective so that Secretary Ridge could be in a position to make the proper recommendations and get the right intelligence?

Dr. CARAFANO. First of all, I think TTIC will always have to be an interagency organization. It should never be anything but an interagency organization.

Mr. RUPPERSBERGER. Yes. I agree.

Dr. CARAFANO. And second, I think you have to have one guy in charge, you have to have one guy responsible, and I really think that should be the Secretary of Homeland Security.

My third recommendation would be to then give him the tools to ensure that the other pieces of the Federal system cooperate appropriately, and the model I would use is what we use for the Joint Chiefs of Staff. When we passed the Goldwater-Nichols Act and said the Joint—the chairman gets to decide who is on his staff, and you have certain education requirements. You have certain experience requirements. You have certain accreditation requirements, and then he has certain budgeting authority.

So if he has all the tools to make the other Federal agencies, then I think you've built a system for the long term and, most importantly, you have a chest that you can put your finger in and say, "This is the guy that's responsible for bringing it all together, connecting the dots and telling everybody what they need to know and when they need to know it."

Mr. WERMUTH. The only point of disagreement there is in the placement of the TTIC, as I mentioned earlier. The Advisory Panel believes the TTIC ought to be separate and independent from my Department. And in fact, if you want to pin the rose on a single person, this panel recommended that what it calls the National Counterterrorism Center, that we think probably will help serve as a model for the TTIC, really ought to report not to the Director of Central Intelligence but directly to the White House. So clearly you can pin a rose directly on an individual there, the guy in charge of all of the Federal——

Mr. RUPPERSBERGER. Where is the funding going to come from, the White House? You're going to have to have the resources. Where are the resources going to come from?

Mr. WERMUTH. You might very well have to have a separate appropriation for an organization like this. You could do it as part of intelligence authorizations. Because it's an interagency organization, it could also be part and parcel—as it is right now, with the TTIC—it could be part and parcel of other agency appropriations that help to fund an entity like that.

Mr. RUPPERSBERGER. Let's get to the—is the light still green?

Mr. SHAYS. We did another one.

Mr. RUPPERSBERGER. The issue as far as—is it information coming in and not properly analyzed? Is it information that's there and not getting to the right people? Let's focus on what the real issue is with TTIC.

Mr. WERMUTH. It's all of the above. Before the TTIC, before other perhaps similar types of interagency entities, various agencies were collecting information, analyzing information in some cases, disseminating information without either having a willingness to share or having an understanding of what needed to be shared with other entities.

Mr. RUPPERSBERGER. Let me get back to my original question because of the time.

Why is the coordination centers—why do they seem to be working very well while there are still issues with TTIC? Would you analyze the two and why you feel one is working better than the other right now?

Dr. CARAFANO. I think, quite honestly, if you talk to most State and local governments, they will say that there's more information going into the system than coming out. And there are lots of reasons for that, connectivity, security clearances. How do we share information? It's a learning process. I'd be reticent to say there's one reason why we're not communicating down as well as I think we're communicating up, and I think that all of these things are really going to have to be addressed before you see a marked improvement.

Mr. RUPPERSBERGER. Let me get to another area. I was a former county executive, during September 11, and went through sending our police officers into overtime to synagogues and FBI buildings, Social Security buildings, those type of things. I see the U.S. Conference of Mayors reported last year that it cost U.S. cities approximately $70 million per week in extra overtime, security, personnel costs, and I think the Heritage Foundation estimates that it costs the Federal Government $1 billion per week.

Do we need—what would you recommend as far as a procedure, as it related to geography and specificity? Now, again, I know that there is a lot of different intelligence, there is a lot of chatter, but in the end, our intelligence is pretty strong in a lot of areas. The issue of specificity and locale, for instance transportation versus an issue involving an airplane issue or whatever it is, that we need to continually—when we hear the chatter, when things go up—to throw it out to the whole country. And that is No. 1.

And second, then what would the recommendation be, if we could get to a geographical issue or specificity, how would you implement that? Through code colors or what?

Mr. ALLEN. I don't have the specific answer for you, because I think it's going to depend on the region and the sector. Industry sectors might——

Mr. RUPPERSBERGER. My question is for the whole country, is it—do you think it would work to declare a certain area in the East Coast and not declare California? Because then all of a sudden——

Mr. ALLEN. I think it would work the same way the State Department can advise you that certain nations of the world are unsafe to travel in or travel to them at your own risk. I think if we develop a specific system targeted at specific geographic and industrial sectors and we educate the public as to what it means—I mean, I think a lot of this comes from the confusion on the part of the public as was discussed here. What does it mean when the threat level goes up? Does it mean everyone is affected the same? I think we can develop a much more effective system that's targeted at the specific threats because——

Mr. RUPPERSBERGER. Automatically, all local jurisdictions and most States, they are spending millions of dollars that maybe we don't have to spend.

Mr. ALLEN. Well, one of the things we heard today, for example, is that DHS does try to communicate with State and local governments, and where they have specific information, as I understood,

what they were saying was, "After we send out the general notice, we will call those where we have specific information." So maybe it's a matter of putting a protocol in place that if you're a local community and you don't get a call within the hour, you know that there is no specific threat targeted at your jurisdiction.

Mr. RUPPERSBERGER. But most people will cover themselves by doubling up and pulling the people in overtime. It happens. Believe me, that's reality. The numbers are there.

Mr. ALLEN. It is reality, but remember, no system is going to be mandatory, but each community and each citizen, all we can do is provide them with as much information as possible to make informed decisions.

Mr. RUPPERSBERGER. You can keep talking. I can't. But the specificity—I'm just asking—well, fine if we can. It depends on who the chairman is. He's a good chairman.

What I'm getting to, is it realistic to think that we could come up with a plan that would deal with the issue of specificity, geography so that if in fact we know—and we can have, our intelligence is a lot more specific in certain arenas—that California, as an example, doesn't have to spend overtime when in fact you might need to do that on the East Coast, that's kind of what I'm—is there—do you all feel that there's a possibility to come up with a system like that? Would that be confusing? Would that—because once it goes, believe me, all—you know how elected officials always want to be re-elected. They are going to make sure they cover their bases.

Mr. WERMUTH. It will never be perfect but better than it is now. Because of the ambiguity of terrorist threats, you'll never be able to devise a 100 percent system, but we can do it better and less costly at the State and local level, absolutely.

Dr. CARAFANO. I would just like to say, I think it's important to de-link in the minds of the public and the State and local governments the HHS color-coded system from what they do every day. I think it works fine at the Federal level because you're coordinating centralized agencies, but I think we need to get people to think we're organizing the Federal Government effort; and for State and local governments and the public, we need to provide them watches and warnings that are applicable to them, and I do think that is an achievable system.

Mr. ALLEN. I agree, it is achievable. Collaboration and education are the two key components, but we can do that.

Mr. RUPPERSBERGER. OK.

Mr. SHAYS. I thank you, gentlemen. I'm going to ask all of you this question, including you, Mr. Connor, but I'm going to also have a specific question for you, Mr. Connor. I want to know how you transform from a threat assessment to a real warning system. I mean, I know we've been talking about it and it's in your testimony, but I want you to give me the first and second, say, the third most important steps DHS can do. I want you to think about that, and first ask you, Mr. Connor, you had mentioned in your testimony the work of the Red Cross in preparedness lessens the burden on Government agencies and first responders and yet the organization relies primarily on charitable donations to perform this important work in support of Government at all levels.

I want to know, what additional resources do you need to continue to be successful in your effort to prepare the American public and to respond to the 70,000 disasters in any given year?

Mr. CONNOR. Yes, Mr. Chairman. The Red Cross, through its nearly 900 community based chapters nationwide, is on the scene with first responders immediately following disasters, both natural and manmade, and as part of the first-response community, we provide direct support to fire, police, EMS, and we are integrated into State and local disaster preparations and training. Yet we are unable currently to apply directly for first-responder funding to meet these requirements we discussed. We must rely currently on local municipalities to include us in their grant applications.

Mr. SHAYS. And why is that?

Mr. CONNOR. Pardon me, sir?

Mr. SHAYS. Why is that?

Mr. CONNOR. I am advised that this is currently, if I'm not mistaken, the DHS interpretation of the statute. They've had—they have a narrow interpretation of first responder, and it is, as I understand it, fire, police and EMS, if I'm correct in that. And so they are the entities that have the eligibility to apply directly for grants and not Red Cross, currently.

Mr. SHAYS. How do you describe your relationship with the Federal Government?

Mr. CONNOR. We are a Federal instrumentality. The President appoints our chairman. We have several Cabinet members who are ex officio members of our board of Governors but we are not a Federal agency. We rely, almost to the 100 percent extent, on donations of that nature.

Mr. SHAYS. Yet you have an actual specific role to play when disasters——

Mr. CONNOR. We do. We are listed, if I may—we are in the National Response Plan, and we have the role for mass care, which is spelled out in the Federal——

Mr. SHAYS. And of course, you wouldn't want to change that, but the issue is, should you be allowed to——

Mr. CONNOR. Correct. Our point is, we have a lot of work to do. We are committed to be partners with DHS at the national level and the local level. We really want to do this. It takes resources. And to the extent we could be eligible for grants directly, that would be helpful——

Mr. SHAYS. So the issue is not that you would get a grant but at least that you would be eligible——

Mr. CONNOR. That's correct. That's correct.

Mr. SHAYS. No. That makes sense.

Mr. CONNOR. Thank you.

Mr. SHAYS. Let me have all of you, including Mr. Connor, let's start with you, Mr. Allen—I mean, first off, we basically all agree here that we have a threat assessment, but we don't really have a warning system yet, and that's the nodding of heads—can't be recorded, is all yes. OK.

Now, so how do we move from threat assessment to a real warning system? Tell me the first few steps. Give me two. You can give me one. You can give me four.

Mr. ALLEN. Can I give you an example, Mr. Chairman? Let's say that there is a threat that there's going to be an anthrax attack or a dirty bomb here in the Washington, DC area, and the government has elevated the level to severe, and then they get more information that it is a real likelihood that something is going to happen. In a warning system, some of the steps you would go through in the decisionmaking process, the first might be to notch it up by notifying the local officials to keep an eye out for this sort of behavior or to watch this sort of activity and provide them specific information to the extent you can.

But let's say, again, that, at some level, you're going to go and say you have to notify the public. Currently, there is no capability within the HSAS or within the DHS threat system to provide an actual public warning to the public. In other words, if they were going to notify us, there's not even a linkage between the HSAS and the NOAA weather radio or the Emergency Alert System, our two national warning systems to get information out. There should, at a minimum, be a linkage—if there's going to be a public warning, that we have a process and a procedure to notify citizens over television and radio via EAS and NOAA weather radio. We do not have that.

Second of all, we need to have decided in advance what are we going to tell citizens to do. It's no good warning them if you don't tell them what you're going to do. Do you want them to shelter in place? Do you want them to evacuate? So we need a plan prior to any of this happening.

But the first step would be to develop that linkage between the threat assessment and the threat warning and the systems that we already have in place to communicate with the public in times of emergency. That would be the first step. And there's a lot more we could do, but let's keep it simple.

Mr. SHAYS. Thank you. We intend, as this committee, to write a report on what we're going to recommend to DHS because—and we are going to use a good deal of what we've learned from the first and second panel. You've provided some rich information. I do want to encourage you to feel free to continue to dialog with the committee, all of you, in terms of recommendations. That would be helpful.

Doctor.

Dr. CARAFANO. I would establish a public system, a two-tiered system of watches and warnings. In order to issue a watch or a warning, you would have——

Mr. SHAYS. Let's start again. You're talking too quickly.

Dr. CARAFANO. I would establish a public system that would consist of a two-tiered system of watches and warnings, and in order to issue a watch or a warning, you would have to provide information that was credible, specific, understandable and actionable. If you couldn't meet those four criteria, then issue a press release or something else.

Mr. SHAYS. I'm going to come back to your comment. I'm going to give you a specific example, and tell me what you would want the public to know.

Mr. WERMUTH. There needs to be some distinctions made between threat assessments and warnings. Unfortunately, the lexicon, even within the Federal Government, about what really is a

true threat assessment is different depending on which agency you talk to; so in the first place, we need better definitions. But I would offer that we need various types of threat assessments to start with, strategic threat assessments, who are our enemies, what are their motivations, what are their capabilities. And then with that information, you can make some more strategic decisions about the application of resources.

Warnings, on the other hand—and I think Jim and I agree here. In fact, I think from what I've heard, all of us would agree warnings have to do with actionable intelligence, something that causes you to say not only is there this threat but it is this specific and here is what you ought to be doing, perhaps within a range of various activities depending on who your sector is.

So to me, a threat assessment is something at a higher level. A true warning system has to be based on something more current, more actionable, more tactical, if you will, than broader threat assessments about who our enemies are and what they intend to do and what they have the capabilities to do, so that then you can overlay that with your vulnerabilities in performing a good risk analysis for the application of resources and other kinds of activities.

Mr. SHAYS. I'm going to come back, Mr. Wermuth, and want to know how specific they would have to be in an example I'll give you.

Mr. Connor.

Mr. CONNOR. Mr. Chairman, the Red Cross's emphasis is on preparing the public for all hazards, kinds of affairs, and we understand this debate, and we think it's properly left in the Federal arena. Whatever the outcome is, we want to be helpful to DHS in whatever system is——

Mr. SHAYS. Well, let me ask you this, though, do you think the public needs to be warned about potential terrorist threats, or do you think it should just be threat assessment?

Mr. CONNOR. Mr. Chairman, I don't think that is a question for the Red Cross.

Mr. SHAYS. Fair enough. I'm comfortable. So now, let me give you a specific example. Let's just suppose that we believe that the Europeans aren't doing a good enough job of making sure terrorists are able to get onto airplanes. Let's assume that they may use a biological agent on the plane and that we think that is a very real possibility. Let's also assume that we're concerned about a dirty bomb being detonated when a large group of people are gathering and that we surmise that it may be in 5 to 12 cities.

And we have decided to respond by warning all the officials about this concern. We are asking the Europeans to put marshals on airplanes. We are asking them to do a better job of checking. Let's assume that we are going into our cities to try to determine whether there is in fact any hint of radioactive material and that we are particularly guarding those larger events.

Let's also assume that we have such a concern that there might be an outbreak, that we even have sharpshooters at large public gatherings.

Now, tell me, if I'm being told that and that's what I know as well as a Member of Congress, what do you think the public has the right to know?

Mr. ALLEN. Mr. Chairman, well, you didn't pick an easy example.

Mr. SHAYS. I thought I picked a damn realistic one.

Mr. ALLEN. But a very realistic one. From the point of view of the partnership, we would err on the side of telling the public more information than less, enough to let them make informed decisions about whether or not they want to go to a large crowd gathering.

Mr. SHAYS. Or travel at your own risk.

Mr. ALLEN. Or travel at your own risk.

We would also hope that the decision on releasing that information or not is made collaboratively in a process in which State and local government officials also have a right to play a role and that it's just not DHS and the Federal Government making that decision.

But we think that—we believe that it's the basic precept of our society. The public has a right to know, and unless there's a reason from an intelligence perspective not to, we would err in sharing it with the citizens and letting them make their own decisions.

Dr. CARAFANO. I think everything you just stated would be the perfect basis for a usable warning to the general public, certainly much, much more useful than going from one color to another. Everything that you describe, there are things where individuals can take actionable things on their own behalf to protect themselves, and I think that would be a foundation for a perfectly valid announcement.

And I would add, I think DHS's press announcement where they talked about concerns about airlines in late February and stuff, I think that came closer to the kind of thing that we would be looking for, but I don't think there's anything that you just said that wouldn't be perfectly appropriate in an announcement.

Mr. WERMUTH. Let me use your examples to explain what I think is the difference between threat announcements or threat analysis and warnings. In the airline example, I think we could and should tell the American people, on a regular basis if necessary, that we know that terrorists are still interested in commercial airliners and that we think some of our European allies are not providing enough security measures at airports to prevent them from getting onto airplanes. That's kind of a threat advisory. Right? People can process that information and make decisions about whether to travel or not.

It rises to a warning level when, as we did around the holiday season and again around the first of February, say we have specific information that terrorists may be trying to board flights out of Heathrow and out of Paris coming in this direction. That rises, to me, to the level of a warning that says, "You may really want to consider not flying on some of those routes, because we have specific actionable intelligence." That's the distinction between the two.

But I would agree with my colleagues here on the panel, that I think the public has a right to know. In the dirty bomb instance, you don't have to tell the people exactly how many people you have as sharpshooters, for example, what kinds of weapons that they

have, but perhaps you ought to say we're concerned enough that we're providing additional security forces that have the authority to interdict potential terrorists, including the possible use of force at arms.

I just think that information is important enough to disseminate to the public and then let them make a decision. They may still decide to go to that sporting event or that public gathering, whatever it happens to be, but tell them enough where they can make an informed decision without necessarily talking about either intelligence sources or methods or for that matter enforcement methods, on the other hand.

Mr. SHAYS. I'm just struck by the fact that you're basically saying what seems to logical to me and so respectful of the public, and yet that was really a real life example. That wasn't a made-up example. That was a real-life example that occurred in the last few months.

Mr. Ruppersberger, I'm going to have a few more questions, so if you want to join in?

Mr. RUPPERSBERGER. I want to get back to TTIC, because I know it's important, and it's just not working as well as it should. Is there anything that you would recommend to us as far as legislation is concerned on how we might be able to fix TTIC?

Mr. WERMUTH. That it be a mandate: full-time representation in the TTIC from State and local entities of the Maryland type, of the California type, of the New York type. Whether you allow States and localities to pay for that or whether you provide direct Federal funding through grants or otherwise, that would allow some of these entities to provide their full-time representation, I don't think that entity is ever going to have the full picture, is ever going to be as effective as it could be, unless it has that kind of representation; and it can't be a quarterly meeting with a few State and local representatives coming to the TTIC and sitting around the table. It has to be full-time, every day.

As one person described it, you'll learn more when you're talking to your colleagues around the coffee pot than you will in exchanging pieces of paper or having advisory meetings.

Mr. RUPPERSBERGER. From a legislation point of view, do you think there's a need for legislation to reform it or to dictate something?

Mr. WERMUTH. It may very well be that it would require very specific legislation or at least broader authority for Federal grants to be used by States and localities, if they choose to do so, to send representation to the TTIC, particularly those States in major metropolitan areas that perhaps are at higher risk, from everybody's viewpoint at higher risk, and we could sit here and name some of those.

Mr. RUPPERSBERGER. Dr. Carafano.

Dr. CARAFANO. I would legislate the requirement for State and local participation in TTIC. I would legislate something similar to the Goldwater-Nichols requirements for JCS for participation in TTIC. I would do all of the funding for TTIC through the DHS so that DHS got basically a go/no-go on how the funds and other agencies participating in TTIC will be spent.

And then finally, I would do a technical amendment to the Homeland Security Act of 2002. I would take TTIC, and I would take the IA portion of IAIP, merge them into one organization and put them under the jurisdiction of the Secretary of Homeland Security.

Mr. SHAYS. Thanks, gentlemen. I'm not going to keep you here much longer, but I need to—this doesn't seem as difficult for me as I think it probably is, because I just start with the basic premise that the public has a right to know. But what I do wrestle with is, then, when don't they have a right to know or when would I cause more harm than good.

Tell me, if you were in the position of having to do not only an assessment, a risk assessment, but a warning, what would become the most difficult tradeoffs for you that would maybe suggest that the public would not have a right to know? And you all have had to have thought about it. I mean, it just—you're in this line of work.

Mr. WERMUTH. That one, of course, is difficult, but all I can do is to say, without having a specific example, there are not many scenarios that I can think of where you wouldn't want to tell the public something. I know the situation you're talking about right after September 11th when the question was asked, "are we prepared for biological attacks," and what the answer was to that question on national television—I think the rationale behind not telling the public in that case is absolutely the wrong rationale. We have to trust the American people to take this information on board and process it. Whether it's natural disasters or emerging natural infectious diseases or a deliberate attack, I think we can tell them what you would, as a citizen, want to know without necessarily disclosing intelligence sources and methods or perhaps all of the steps that governments at all levels are taking to help protect them, because that might disclose things to the bad guys. You have to tell them what the threats are and what that means to them in terms of risk. I think it's wrong to take any other approach.

Mr. ALLEN. General Hughes said that making those decisions about what to share is a balance, and I would agree with him to an extent, but I think the balance needs to be shifted a little bit.

Hopefully, we will never be—have the difficult decisions that I guess they had during World War II in the bombing of Coventry when they decided not to share that information in order not to divulge the source of the intelligence.

Mr. SHAYS. That's a great example, isn't it?

Mr. ALLEN. It is a great example. And the only example I could think of when you wouldn't share it is when the potential loss to the Nation is greater from sharing it than not sharing it, and I truthfully can't conceive in 99 times out of 100 where that would be the case.

So I think that the balance, again, needs to be shifted to the side of informing the public, letting them make their own decisions about their lives and their families.

The President said we're at war on terrorism, but unlike other wars, where we had an ocean between us and the battlefield, it's here, and I think we're all combatants in that war. And I think,

as combatants, we all have a right to know whatever we can to protect ourselves and our communities. So I would err on informing people.

Dr. CARAFANO. I agree. I think that the two concerns are, one, compromising sources or methods and, two, doing something that might facilitate a terrorist attack and might make it easier. I think those would be my two primary concerns.

Mr. SHAYS. You all, again, are such experts, I want to ask you this. Could what happened in Spain happen in the United States?

Mr. WERMUTH. Certainly. It's part and parcel of this entire public information, education process. I think governments at all levels have an obligation to tell people we cannot protect you against everything all of the time. You will never be 100 percent secure in any number of contexts within our society, whether it's within your freedom of travel, whether it's within your ability to communicate with each other through increasingly sophisticated communication systems. We ought to be explaining that to the American people.

It really is the basis of what the Advisory Panel described as its new normalcy. Be straightforward with the American people. We can't protect you against everything. Yes, there are risks with train travel in the United States, but just because we're vulnerable, as this panel would say, doesn't necessarily mean that there is a threat out there that exists to exploit that vulnerability.

Could it happen here? Yes. But that's what makes intelligence collection, analysis and dissemination so critically important. It's not just because we're vulnerable or the things that scare us to death. It's understanding who the enemy is, what their motivations are, what their capabilities are and being able to take action on that depending on what the threatened attack is at any point in time. But to me, the answer to the question is, sure.

Mr. SHAYS. Dr. Carafano.

Dr. CARAFANO. I agree.

Mr. SHAYS. And the answer is, yes, again?

Dr. CARAFANO. Yes. I would agree.

Mr. SHAYS. OK. Mr. Allen, as well, is saying he would agree.

I would also put into perspective we lose about 120 people every day in automobile accidents. It blows me away every time I think about it. You know, the number last year was 440,000, and so we do know there are a lot of things we do at risk. It's just nice to know it, and, I mean, nice—I just think it's important to know it.

Let me ask you, is there anything that we should have asked that we didn't? Is there anything that you would have liked to have responded to that we didn't ask? Anything you want to put on the record?

Mr. CONNOR. Mr. Chairman we would love to put in the record our thanks to Mr. Ruppersberger for his great support of the Red Cross and his statement on the floor of the House last week for March as Red Cross month. Thank you.

Mr. SHAYS. That's probably the most important thing that happened all day today, that you thanked him.

Dr. CARAFANO. I'd just like to reiterate a call that I think we need to pay much more attention to educating the next generation of State and local and Federal leaders on how to do preparedness

better, how to do response better, and it's a serious education challenge that I don't think we've fully taken on.

Mr. ALLEN. I just want to commend the chairman and this committee for addressing this issue, the whole issue of public warning. I think it's because so many people are involved, and nobody has been in charge of it. And somebody needs to pay attention to it, and we commend you for doing so.

Mr. SHAYS. Thank you. We're not going to let up on it, and we do know we have people of good will, but we do think politics is kind of interfering, in some cases, with good judgment, regretfully, and I just think that we just need to keep plugging away at it, and I thank you all for providing us tremendous data and information and opinion. Thank you.

This hearing is now adjourned.

[Whereupon, at 12:48 p.m., the subcommittee was adjourned.]

○