THE HOMELAND SECURITY ADVISORY SYSTEM

HEARING

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 4, 2004

Serial No. 108–35

Printed for the use of the Select Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

22–132 PDF WASHINGTON : 2005

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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, *Ranking Member*
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
STEVEN CASH, *Democrat Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

CONTENTS

Page

STATEMENTS

The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Select Committee on Homeland Security 1
The Honorable Jim Turner, a Representative in Congress From the State of Texas, Ranking Member, Select Committee on Homeland Security
Oral Statement 22
Prepared Statement 7
The Honorable Benjamin L. Cardin, a Representative in Congress From the State of Maryland 36
The Honorable Donna M. Christensen, a Representative in Congress From U.S. Virgin Islands 42
The Honorable Jennifer Dunn, a Representative in Congress From the State of Washington 33
The Honorable Kay Granger, a Representative in Congress From the State of Texas 24
The Honorable Jane Harman, a Representative in Congress From the State of California 25
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas
Oral Statement 46
Prepared Statement 9
The Honorable Nita M. Lowey, a Representative in Congress From the State of New York 44
The Honorable Edward J. Markey, a Representative in Congress From the State of Massachusetts 31
The Honorable Loretta Sanchez, a Representative in Congress From the State of California
Prepared Statement 9
The Honorable John B. Shadegg, a Representative in Congress From the State of Arizona
Prepared Opening Statement 8
The Honorable Christopher Shays, a Representative in Congress From the State Connecticut 38
The Honorable John E. Sweeney, a Representative in Congress From the State of New York 28

WITNESSES

The Honorable James Loy, ADM, Deputy Secretary, Department of Homeland Security
Oral Statement 11
Prepared Statement 14
Mr. John O. Brennan, Director, Terrorist Threat Integration Center
Oral Statement 17
Prepared Statement 18

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

Responses and Questions from The Honorable Loretta Sanchez 63
Responses and Questions from The Minority Staff 64

THE HOMELAND SECURITY ADVISORY SYSTEM

Wednesday, February 4, 2004

HOUSE OF REPRESENTATIVES,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 12:38 p.m., in room 2175, Rayburn House Office Building, Hon. Christopher Cox [chairman of the committee] presiding.

Present: Representatives Cox, Dunn, Shays, Camp, Linder, Shadegg, Gibbons, Granger, Sweeney, Turner, Sanchez, Markey, Frank, Harman, Cardin, Slaughter, DeFazio, Lowey, Norton, McCarthy, Jackson-Lee, Pascrell, Christensen, Etheridge, and Lucas.

Chairman COX. [Presiding.] Good afternoon. A quorum being present, the Homeland Security Committee will come to order.

This committee is meeting today to hear testimony on the Homeland Security Advisory System.

I would like to thank the members in attendance, and thank both our distinguished witnesses—Admiral James Loy, the deputy secretary of Homeland Security, and John Brennan, director of the Terrorist Threat Integration Center—for their willingness to share their expertise with us.

This marks Admiral Loy's first testimony before the Congress in his new capacity as deputy secretary of Homeland Security.

Admiral Loy, we are honored to welcome you and look forward to working closely with you in guiding the department's progress, in meeting its Homeland Security Act mandate.

John Brennan has been with us before, and we welcome you back.

Since September 11, 2001, we have made dramatic, undeniable progress in securing the American territory. Everyone here agrees on that.

The president and the Congress have joined forces to lead a fundamental transformation in the way the Federal Government views the national security and how it should relate to state and local governments, as well as to the private sector, in order to promote the security of the American people and our territory.

The Department of Homeland Security is one important product of that dynamic policy reorientation. While the Terrorist Threat Integration Center was, like the Homeland Security Advisory System itself, called into existence without benefit of congressional action, the Congress are nevertheless delighted to note the constructive work it is doing in bringing together information and analysts to form a comprehensive picture of the terrorist threats we face.

In fact, TTIC is doing such good work, we are inclined to think it might be best internalized in the department and made answerable to the secretary of homeland security. That, however, is discussion for another time.

Today we want to get a better understanding of the Homeland Security Advisory System itself—our color-coded national warning system, it is purpose, how it actually works, and its potential, including how it could be improved.

The system's color-coded warnings have become the primary means by which the Federal Government communicates directly to the public, its bottom-line judgment on the risk of terrorist attack at any given time.

It is our inescapable reminder that the Nation is engaged in a global war on terror and that we ourselves may be at risk of attack.

The president's directive establishing the system puts it plainly, "The higher the threat condition, the greater the risk of a terrorist attack."

Adjusting the threat condition up or down is, in short, a very significant public statement to the American people by their government. As a result, we have learned that raising the national threat level can have direct implications, not only for personal safety, but also it may entail widespread changes in personal behavior, including travel and spending patterns, with corresponding if temporary effects on the nation's economy.

Government and private sector entities, too, must take appropriate measures to increase their security posture every time the threat level is raised. And those measures are costly.

I will get to that in a minute.

They key point is that the reliability and timeliness of the advisory system's national threat warnings must be unquestioned.

I want to stress at the outset the public nature of the color-coded warning system.

The Homeland Security Act provides, in Section 201, that the department's Homeland Security Advisory System responsibilities include, "Exercising primary responsibility for public advisories related to threats to homeland security"—that is Section 201(d)(7)(a) of the Homeland Security Act.

I think it follows that what we use the system's public advisories—that is, its color-coded warnings—to say, we should be willing to say and to explain publicly. Because the Homeland Security Act goes on to note that the department's responsibilities have a second element that need not be public, the responsibility, "in coordination with other agencies of the Federal Government to provide specific warning information and advice about appropriate protective measures and countermeasures to state and local government agencies and authorities to private sector, other entities and the public"—that is Section 201(d)(7)(b) of the act.

So we need to make sure that we use the public threat advisory system to advise the American public of threats that are truly national in scope, or to warn of region or sector-specific threats that we are able and willing to identify and discuss in public, including as a means of diverting or delaying potential attacks.

That is to say, we should not be using the public color-coded threat advisory system to warn of terrorist threats that are not national in scope if we are not willing to discuss them publicly. For them, we should be using the second element of the statutory provision I just quoted.

That brings me back to the cost issue.

Securing the homeland is expensive. Every national terrorist threat warning triggers a massive chain reaction throughout our society. Government officials at all levels, businesses of all sorts and sizes, as well as individual citizens are left with the fundamental question: What does code orange mean for me?

The answer in the absence of specific guidance as to the nature, potential targets and likely timing of the threat has been a nationwide piling on of enhanced security measures, breaking state and local overtime budgets and redirecting their personnel from their other duties. If we can avoid or diminish that effect, we should, and soon.

It is, after all, a fundamental part of the terrorist strategy to destroy our economy and our way of life. We must not, through our well-meaning efforts, give them any help.

All across America, in our public and private institutions, we are spending considerable sums of money to enhance our security, and we must do it wisely.

It is enormously intrusive and unnecessarily expensive to call a heightened state of alert across the Nation when hard intelligence shows that only certain parts of the country or certain sectors of our critical infrastructure are at increased risk.

This committee will soon be marking up H.R. 3266, the Faster and Smarter Funding for First Responders Act, voted unanimously out of our Emergency Preparedness and Response Subcommittee late last year. That bill contains a provision that requires the secretary of homeland security to revise the advisory system so that warnings can be issued to the geographic regions or economic sectors which analysts believe are actually at risk.

The case for such reform is in the numbers. Reports describing code-orange-related expenditures include, just by way of example, a January 23 Los Angeles Times article that cites LAX officials reporting that during the most recent rise to orange, their security costs amounted to more than $3.8 million since December 21st; an Associated Press report that officials in New Orleans spent between $200,000 and $300,000 a week in police overtime because of the latest orange alert; a U.S. Conference of Mayors' survey that shows cities spent about $70 million per week in orange-alert-related expenses.

Phoenix, for example, spent $154,000 on a weekly basis. Los Angeles spent $2.5 million each week. And New York City racked up $5 million each week in additional expenses.

We cannot expect states and localities to sustain such unbudgeted expenditures indefinitely.

To take a closer and more comprehensive look at the incremental costs incurred by Federal, state and local government agencies in responding to the last three code orange alerts, this committee made a bipartisan request for a GAO study. Initial findings reported to the committee last week show that state and local offi-

cials would like to receive more detailed guidance to help them determine what protective measures to take in response to orange alerts.

They also want DHS to provide more information on region and industry-specific threats.

They are right. Responding aimlessly over and over to a generalized warning draws down resources without any assurance of enhancing anyone's safety.

It may over time actually contribute to a degradation of this nation's vigilance, so-called warning fatigue, and so diminish the utility of the Homeland Security Advisory System.

There are encouraging signs. This week and late last month, I think we did a good job of identifying aircraft and routes our analysts believe were subject to heightened risk. Preventive measures were tailored to the apparent threat. In the process, DHS demonstrated its ability to use hard intelligence in directing a clear warning message only to where it was needed.

Responsible suggestions for canceling flights enabled the airlines to respond effectively.

Alerts to the public should, by contrast, be made only where they can be publicly explained or when the increased risk is truly national in its scope.

Keeping the American people at a high level of anxiety is not a sustainable strategy. Throughout most of the heightened alert periods, including increasing the alert level from yellow to orange and back again, the public has been told at the same time to go about their normal everyday lives. The question remains: Why issue, then, a public threat advisory at all?

Great Britain's national alert system, for example, communicates warnings only to law enforcement officials. The general population is never notified because causing alarms to the general population would be counterproductive.

On the other hand, public alerts may serve to delay or deter terrorist attacks and may, therefore, enhance opportunities to prevent them.

We must, in some, strike an appropriate balance between providing meaningful warning where hard intelligence warrants it and causing a senseless, unfocused nationwide response to unspecific threat alerts.

I look forward to our witnesses' views on how best to strike that balance.

The chair now recognizes Mr. Turner, the ranking Democratic member, for any statement he might have.

Mr. TURNER. Thank you, Mr. Chairman.

Secretary Loy, let me congratulate you on your new position and thank you for appearing before our committee today.

As deputy secretary, you have the critical role of managing that department. I guess you have most of the duties that Secretary Ridge has except maybe you do not have to go to all the press conferences.

But we are pleased to have you.

And, Mr. Brennan, welcome back to you.

Both of you are here to talk about a subject that the chairman and I have both had a great deal of interest in: the Homeland Security Advisory System.

I have been able to observe the threat alert system over the last two years and have been able to view it in light of the briefings that we receive regularly regarding the threat. And I think it gives us a unique perspective on the system, being able to compare the threat information with the raising of the alert at the various times that it has been raised in the last couple of years.

And after thinking about ways we might change the system, and observing how I think the public has reacted over time to the warnings, it is my judgment that the color-coded system should be eliminated.

The system that we have today we all know was created very quickly after September 11th. It was our government's first attempt to establish a national system to alert our citizens and our economic sectors about homeland security threats. And while the system may have served some initial purpose, I do not believe that the color codes are serving us well today.

Americans understand that we are fighting a long war on terror, often fought in the shadows and without a clear understanding of when or where we might be attacked. Therefore, our intelligence, law enforcement and other security forces must remain vigilant all the time, not just when the color code is raised.

Specific threat advisories can help target the vigilance of these law enforcement and security forces by increasing their security measure at certain places and during certain times when they receive specific information.

And I think certain sectors of our economy, if given the direct and specific information, can make adjustments that are important.

But the color-coded threat alert system that we have does not meet, in my judgment, our true security needs.

First of all, I think that the color codes send very mixed messages. In December we raised the threat level to orange, and as the chairman said, we told the American people not to change their plans or take any specific actions to protect themselves. I think that leaves the public confused and somewhat agitated with a system that causes them alarm but gives them no specific guidance about what to do.

Constantly raising and lowering this color-coded level is I think making the public numb to the ongoing threat of terrorism.

People need to know that they should be constantly alert. We need a culture of awareness in this country to be alert to suspicious behavior that may be linked to terrorism.

Second, I believe the color-coded system is not providing threat information to the people that need it in order to make and take decisive action.

Our law enforcement, security and emergency personnel do not need a color; they just need the facts.

And if the governors and the mayors of this country need to order additional security measures, they need credible, actionable intelligence from the Federal Government.

The General Accounting Office and the Gilmore Commission both reported that state and local officials are not getting the specific in-

formation they need to do their jobs. They are looking for more help, for more information. It is a constant cry I hear every time that I travel into our communities.

Our state and local officials need to know the details before causing public concern and being asked to spend scarce dollars on unnecessary security measures.

In addition, I believe that the all-or-nothing nature of the current system fails to distinguish between areas and sectors of the economy that we believe are at heightened risk. When the threat level is raised, a wide range of Federal, state, local and private sector protection plans go into effect. Although the intelligence has not suggested that all sectors of our society are specifically threatened. State and local governments spend hundreds of thousands of dollars, perhaps millions, to defend against an unknown threat.

Finally, I think we also need to consider whether the alert system is helping terrorists more than it is helping us. When we raise and lower the threat level, we are also telling Al-Qa'2ida that we are strengthening our defenses. And then again, we tell them that we are lowering our guard when we lower the color.

I think I agree with the chairman that we need to look at our system and question whether or not we are giving our enemies as much information as we are giving ourselves.

Now, I recognize that the administration's in a very difficult dilemma here. Our intelligence agencies gather a lot of information, and very little of it relates to specific attack. And I can say, having received these intelligence briefings, that it is pretty clear to me that this general threat information is continuous and ongoing.

I think we should have a level of security deployed around the country that is appropriate in light of the ongoing and the consistent threat of terrorism that we face.

When we believe there is a greater risk of attack, those who are able to take specific action should be advised and should be given as much information as we possibly can share. But issuing general alerts does not serve a useful purpose and may well be counterproductive.

Another point that I think is worthy of some consideration here, and that is that the very existence of this color-coded system really creates a no-win situation for the department. If the department fails to raise the level of alert and an attack occurs, you will be severely criticized. If, on the other hand, you raise the alert and nothing happens, people are quickly going to say you are crying wolf once again.

And the political reality here is that the political pressure is always there for you to raise the alert level when threat information comes to you that indicates there may be some change.

And so I think the political reality is that political pressure itself may cause an over utilization of the color-coded system.

So I think we would be much better off if we shared with the public and with the communities and geographic areas and sectors what we have specific threat information about. And if we have general information that is more specific and may affect the entire country, let's just share it and tell them what it is. But to simply go through the motions of talking about color codes to me is not

the America that I think we want to know, nor is it giving us the information that we need to have.

Thank you very much, Mr. Chairman.

Chairman COX. Thank you very much.

Under committee rule three, members who were present in the first five minutes can make opening statements of three minutes or reserve their time for questioning.

Does any member wish to make an opening statement?

PREPARED STATEMENT OF THE HONORABLE JIM TURNER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, SELECT COMMITTEE ON HOMELAND SECURITY

Thank you, Mr. Chairman.

Secretary Loy, let me congratulate you on your new position. The Deputy Secretary in any department is the person who makes sure that things get done. In this department, you will have your hands full, and I am pleased to see that you are on the job.

Mr. Brennan, welcome back. Thank you both for being here to discuss the Homeland Security Advisory System.

I have been closely observing the threat alert system closely over the past two years and have received threat briefings when the level has been raised to orange. After thinking about possible changes that could be made to the system, and seeing how the general public has is reacting over time to the warnings, my judgment is that this system should be eliminated.

The system we have today was created quickly after the September 11, 2001 attacks. It was the government's first attempt to establish a national system to alert our citizens and our economic sectors about homeland security threats.

While the system may have initially served a useful purpose, it is not serving us well now.

Americans understand that we are fighting a long war on terror, often fought in the shadows, without a clear understanding of when or how we might be attacked. Therefore, our intelligence, law enforcement, and other security forces must remain vigilant, at **all times.** Specific threat advisories can help to target that vigilance, by increasing security measures in certain places and for certain sectors of the economy.

But the color coded threat alert system we have doesn't meet these security needs.

First, we send very mixed messages. In December, we raised the threat level to ORANGE, but told the American public not to change their plans or take any specific measures to protect themselves. This leaves the public confused and agitated with a system that causes them alarm but gives them no concrete guidance. Constantly raising and lowering the threat level is also making the public numb to the ongoing threat of terrorism. People need to know that they should be constantly alert to suspicious behavior that may be linked to terrorism.

Second, the color coded system is not providing threat information to the people that need it in order to take decisive action.

Our law enforcement, security, and emergency personnel don't need a color, they need the facts. If the governors and mayors of this country need to order additional security measures, they need credible, actionable intelligence from the federal government. However, as the GAO and Gilmore Commission have reported, state and local officials are not getting the specific information they need to do their jobs. They are looking for more help from the Department. Our state and local officials need to know the details before causing public concern and spending scarce dollars on unnecessary security measures.

In addition, the all-or-nothing nature of the current system fails to distinguish between areas and sectors of the economy that we believe are at a heightened risk. When the threat level is raised, a wide range of federal, state, local, and private sector protection plans go into effect, although the intelligence has not suggested that all sectors of our society are specifically threatened. State and local governments spend hundreds of thousands of dollars—perhaps millions—to defend against an amorphous threat.

Finally, we also need to consider whether the alert system is helping the terrorists more than it is helping us. When we raise and lower the threat level, we are also telling Al-Qa'ida when we are strengthening our defenses, and then again when we are lowering our guard. I agree with the Chairman that this alert system may present a roadmap, broadcasting our vulnerabilities to those who would do us harm.

I recognize that the Administration faces a difficult dilemma. Our intelligence agencies gather a great deal of information, and very little of it relates to a specific attack. We should have a level of security deployed around the country that is appropriate in light of the ongoing, consistent threat of terrorism that we face. When we believe there is greater risk of attack, those who are able to take specific action should be advised. But issuing general alerts does not serve a useful purpose and may well be counterproductive.

I urge our witnesses and the Department to reform the threat alert system. We need to create a system that is flexible, gets actionable information quickly to the people that need to take action, and underscores the need for our citizens to remain vigilant in the face of the threats we face.

Thank you, Mr. Chairman, for calling this hearing. I look forward to the testimony of our witnesses today.

PREPARED OPENING STATEMENT OF THE HONORABLE JOHN B. SHADEGG, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARIZONA

I commend Chairman Cox for holding this important hearing and look forward to the testimony of Admiral Loy.

Today we wi11 learn about the steps the Department is taking to improve the Homeland Security Advisory System. It is safe to say that overall homeland security in general has improved since 9/11. Awareness, intelligence sharing, and investment in our first responders have all increased. Likewise, states, localities, police and fire departments are becoming more comfortable with what it means to move from yellow to orange on the Homeland Security Advisory System.

At the same time, there is room for improvement. As you know, my Subcommittee passed the Smarter Faster Funding for First Responders bill on November 20th. That legislation would encourage the Department to make the warnings more specific, by including geographic information and a- description of what kind of industry or business is threatened. I applaud the Chairman and the Ranking Member for supporting that legislation. I believe that it is a step in the right direction, and I look forward to seeing it pass full committee as soon as possible.

I am still concerned, however, that we have not fully explained to the American people what moving from yellow to orange on the Homeland Security Advisory System means. Does that mean that they should fill up their gas tank, or buy reserve water, or give blood?

As the brave men and women on Flight 93 proved, Americans are ready and willing to join the fight against terrorism, but they need more tangible information about what they can do. Leveraging the support of the American public is critical to our future success. I applaud efforts like ready.gov and the citizens corps, but as the Department continues to refine the Homeland Security Advisory System, I strongly encourage a focus on what citizens can do.

PREPARED OPENING STATEMENT OF THE HONORABLE LORETTA SANCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you, Mr. Chairman. I'd like to start by welcoming our witnesses and thanking you both for being here.

Today, we're here to talk about the Homeland Security Advisory System. It is my hope that you are going to report to us that this system has proven to be ineffective that you have instead come up with a far improved method to keep our citizens safe and calm.

The mission of the Department is to protect the public from terrorists. And I am. quite sure it was not the intention of the Department to create a system that keeps us at an elevated state of alert at all times.

There are three main areas that are a source of concern for me that I'm hoping I will hear you address today in terms of the alert system as it stands today.

Those three topics are: (1) the WAY in which we obtain intelligence on terrorist activity; (2) the way we disseminate that information to the public-and in particular to law enforcement; and (3) the expectations of the public once they receive that information.

I've talked with several people in the law enforcement community across California about these issues and the various breakdowns in each area, and it would appear that we still have some real changes to make.

On the issue of intelligence, one only needs to read the papers lately to have real doubts about the quality of the information we are receiving. I'm hoping that Mr. Brennen can speak further about this issue. Have we been successful in our intelligence gathering? Are there areas in which we can make improvements?

As for dissemination of information once we identify threats, I'm told there are real breakdowns in this area, particularly as it relates to the law enforcement community.

I'd be willing to bet that every member on this panel has heard a complaint from local law enforcement that they've gotten a million calls from citizens asking what they should do because the threat level was raised to orange. Then the there are the obvious questions that follow from those law enforcement officers, ″Why wasn't I notified? Why do I have to find out by CNN or a citizen's phone call?″

I am confident that you have some ideas on how we can better communicate with our First Responders.

Finally, the warning itself is far too broad and there is no suggested action to be taken.

It is unfair, even cruel, to tell the public: "You are in more danger than you were yesterday. We have information that you may be attacked. This means someone is trying to kill you. What should you do about it? Nothing really. Go about your normal routine, just be a little extra afraid."

I believe we can do better than saying: "We think that somewhere in this huge country there might be a terrorist attack." How can we expect the public to have any confidence in our ability to protect them? More importantly, how do we expect them to feel safe?

I am interested in digging deeper into these issues, and I am hopeful that you have some ideas about some real changes with regards to the alert system that should replace this one, a tool that will really help protect the public. Thank you, Mr. Chairman.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE FOR IN CONGRESS FROM THE STATE OF TEXAS

Chairman Cox, Ranking Member Turner, I thank you for your efforts and energy in providing today's distinguished witnesses and for organizing this important hearing on the Homeland Security Advisory System. The alert system is of considerable controversy, and the testimony and analysis that will go on record today will allow us to improve the system. Thank you also to Admiral James Loy and to Mr. John Brennan for their time and testimony.

I join my colleague the Ranking Member Turner in his criticism of the Homeland Security Advisory System (HSAS). Philosophically, it does no more than incite fear and anxiety for American citizens. A true "advisory system" would do just that-*advise* citizens rather than send them into a frenzy. Since the HSAS's inception on March 12, 2002, I have advocated the need for a system of relevant and concise instructions for citizens-information that is truly useful in the event of a threatening situation.

On December 31, 2003, I held a Homeland Security Taskforce Meeting in Houston, Texas and met with personnel from the Houston Police Department, School District Police Department, Fire Department, Mental Health Mental Retardation of Harris County, Office of Emergency Management, Health Department, Airport System, and the Houston chapter of the American Red Cross; members of the local branches of the Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency (DEA); and the local academic and church communities to discuss the viability of Houston's threat assessment systems with respect to homeland security. As a Member of this Committee as well as Ranking Member of the House Judiciary Subcommittee on Immigration and Border Control, it was critical that I bring back to my fellow Committee members an urgent initiative to analyze and improve the interoperability and functionality of our local and national First Responder corps. This improvement initiative begins with a threat advisory system that actually gives intelligent and articulable information that first responders can use in such an instance.

Among the issues that we discussed on December 31st were whether the funding levels, equipment availability, depth of personnel, and degree of interoperability between local, state, and federal systems are adequate to facilitate timely emergency response. Overall, some of the responses given were that intelligence-sharing has generally improved; however, other important aspects clearly require immediate attention. Monies that were promised back in 2001 by the federal government have not been received; more hospital beds and medical equipment are needed; and the first responder staff and equipment levels must be increased.

The orange alert issued on December 21st signified a 'high' risk of terror threat. With an improved and more comprehensive advisory system, our local hubs perhaps would have already been prepared! The issues underscored in that Taskforce meeting are of grave importance in a city such as Houston, the fourth largest city in the

nation. We are the home to many critical sites such as ports of entry, power grids, major medical centers, and central business facilities that need to have adequate training, a sufficient number of personnel, necessary equipment, and adequate funding in the event that DHS issues a high alert as we have today. Clearly, we in Congress must hold oversight hearings as to the degree of threat assessment operability and interoperability of our cities? first responder systems and whether our communities across the nation are prepared in addition to today's matter-more focused on the alert system itself.

Relative to suggested improvements to the system that will make it more effective, the Houston Chapter of the American Red Cross offered the following alert language to replace the "orange threat level" indication:

Individuals

- Review your Personal Disaster Plan.
- Ensure your Disaster Supplies Kit is stocked and ready.
- Develop alternate routes to and from work or school and practice them.
- Exercise caution when traveling.
- Have shelter-in-place materials on hand and review the procedure in Terrorism: Preparing for the Unexpected, a Red Cross brochure.

Families

- Review Family Disaster Plan with all family members
- Check items in your Disaster Supplies Kit and replace items that are outdated.
- If not known to you, contact your child's school to determine their emergency notification and evacuation plans.
- Ensure the emergency communication plan is understood and practiced by all family members.
- Discuss children's fears concerning possible terrorist attacks.

Neighborhoods

- Check on neighbors who are elderly or have special needs to ensure they are okay.
- Review their disaster plan with them.
- If a need is announced, contact nearest blood collection agency and offer to organize a neighborhood blood drive.

Schools

- Review the school's emergency plan that was developed using the Red Cross Emergency Guide for Business and Industry.
- Ensure all emergency supplies are stocked and ready.

  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.

Businesses

- Review the emergency plans, including continuity of operations and media materials on hand.
- Ensure that the emergency communication plan is updated and includes the purchase of needed emergency equipment as detailed in the Red Cross Emergency Management Guide for Business and Industry.
- Determine any need to restrict access to the business or provide private security firm support/reinforcement.
- Contact vendors/suppliers to confirm their emergency response plan procedures.

I advocate an advisory system very similar to that which the American Red Cross presents. Because the alerts would be so narrowly focused, they would not cost cities, states, and municipalities the extraneous amount of emergency preparedness dollars that they struggle to produce to respond.

Mr. Chairman and Ranking Member, for the above reasons, I recommend restructuring of the Homeland Security Advisory System. Thank you for assembling this meeting.

Hearing no requests, the chair is pleased to again welcome Admiral Loy.

Thank you again for being with us this afternoon, and thank you for your written testimony, which we have provided to the members in advance.

We would be pleased if you would take five minutes to summarize your testimony.

STATEMENT OF THE HONORABLE JAMES LOY, ADM, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Admiral LOY. Thank you, Mr. Chairman.

Good morning, Mr. Turner.

I would like to thank you as well as the other members of the committee for providing the chance to talk about the Homeland Security Advisory System.

First, let me publicly thank my colleague, John Brennan, sitting next door. Since I arrived on the scene at DHS in early December, I think I have spent more time with John than I have with my family.

TTIC's charter is to be the coordination point for the sharing of information related to terrorist threats for the intelligence community. In our day, every day at DHS starts with a TTIC review of current threat analysis. If it is about the terrorist threat, it goes to TTIC from any point now on the intelligence community compass, including some very new ones, like state, local and private sector information provided to them from DHS.

Armed with this all-source array, TTIC offers the analytic product for those of us charged with operational responsibility.

TTIC, like DHS, is an evolving organization, getting better at its job every day.

John and his team have done an exceptional job in starting up the center and meeting the charter in the law. They have become a key cog in the business of securing our homeland.

On March 11th, 2002, President Bush created the Homeland Security Advisory System, as the chairman said, 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 all Federal agencies except the Department of Defense. And it is encourage for state and local governments and the private sector; 55 of the 56 states and territories have adopted it.

During periods of heightened concern, the framework provides the ability to change the threat condition on a national level while also affording the opportunity to target communications to particular geographic regions, 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 as both the chairman and the ranking member have commented.

With the creation of the department on March 1st, 2003, the advisory system has evolved into a framework that married the analytical assets of the intelligence community with the department's unique responsibility in IAIP, that directorate, to assess the nation's vulnerabilities and implement protective measures.

The system in its various dimensions continues to evolve. And I believe we have reached a threshold in that evolution where the system serves the Nation well.

When all the rhetoric is lifted, it is simply a tool in the system we have designed to secure our homeland. As part of a system that includes other tools and can be used selectively itself, the HSAS has demonstrated its utility on several occasions.

This evolution to date has revealed three basic ways, I believe, to use the system.

First, as a universal baseline, and as a universal adjusting tool, when and where the entire nation is alerted to a changed threat circumstance requiring across-the-board upgrades or downgrades of security activity.

Second, surgically, where the threat conditions can be changed geographically, by economic sector, or even by a combination of both, and if the first use is blunt, and certainly it is, this use is more sophisticated and it requires a more evolved system as exhibited in the just-passed December–January holiday period.

Third, using communication channels developed over the year, we now make adjustments within the existing threat condition to regions or sectors without a threat condition change at all.

All of these approaches are keyed to the best judgments we can make on the threat itself. It is a threat-based risk-managed system. It demands new and different thinking and judgment than has ever been necessary before.

We are getting better at it daily, and we look forward to working with the committee to work even better ideas into the HSAS framework.

We recognize that a decision to change the threat condition has significant economic, physical and psychological impacts on the nation. Therefore, decisions are taken by the secretary only after serious consultation with key colleagues around the Homeland Security Council table.

All the players at that table are now familiar with the range of actions the secretary has available to him. And in the final analysis, the HSAS is simply a communication tool.

We have developed other products to fill out that tool kit. Each can be used to inform a broad or narrow audience, depending on the threat. They range from information bulletins to advisories to conference calls to executive visits. And such products have enabled DHS to use the advisory system in a more targeted and flexible manner.

And as a result of this refined ability to target specific information with specific actions and prevention measures, the threshold for recommending changes to the threat condition has actually become more finely calibrated.

This evolution is best illustrated by the most recent threat period, the change over the December 2003 holiday window. At that time the threat condition was raised from yellow to orange based on a substantial increase in the volume of threat-related reports from credible sources across the board. These were the most specific threat reports that we have seen thus far.

When the threat condition was lowered on January 9th, DHS recommended that several industry sectors and geographic locales continue on a heightened alert status. And 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 the specificity that we saw in the threat stream.

For the first time since the creation of the system, the department lowered the national threat level but recommended maintain-

ing targeted protections for particular industries or geographical locales.

We are simply getting better at the decisionmaking required to meet our mission. In the end, it is about finding and building a flexible, effective system and then making good judgments and taking good decisions in the best interest of the American people.

Mr. Chairman, I had the pleasure of hearing your staff director in your absence and Mr. Turner at a dinner event Monday night. Each spoke about our common work together. It was almost uncanny how both gentlemen seemed to articulate loud and clear the thoughts and discussions we have every day in the department.

They spoke about focus and sacrifice across the board for this country and its citizens and strategic planning. They spoke about how the threat continues unabated and how we must be both offensive to rout out the enemy where he is to be found and equally aggressive in protecting our homeland. They spoke of building partnerships here and abroad and investing in technology as one of the keys to our eventual success—and they were on target on all counts.

Mr. Chairman, this is very hard work, as you have committed. We have immensely dedicated people doing it. And I am proud of the efforts invested in the work accomplished thus far, but we also have very far to go and much more to do. And we must hold on to a sense of urgency about getting that work done.

We at DHS are appreciative of your help, your ideas and your role as our conscience in this business.

This is my 44th year of public service, and the work I am immersed in with my colleagues has never been important to our country. We will get it done and we will get it done well. We will be on time and we will on budget. We will be innovative and we will be creative.

And we are trying hard not to be held back by the bureaucratic baggage of the past.

The American public deserves our very best effort and they will be getting nothing less.

Thank you sir, and I look forward to your questions.

[The statement of Admiral Loy follows:]

PREPARED STATEMENT OF THE HONORABLE JAMES LOY

Good morning, Mr. Chairman and Congressman Turner. I would like to thank you, as well as the other members of the committee, for providing this opportunity for me to join my colleague from TTIC, John Brennan, 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 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-Qa'ida'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-Qa'ida 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 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.

Chairman COX. Thank you, Admiral.

I now welcome our second and final witness, Mr. John Brennan, director of the Terrorist Threat Integration Center. Mr. Brennan is a 23-year veteran of the Central Intelligence Agency. He served as chief of staff to Director Tenet, and just prior to being appointed director of TTIC held the position of deputy executive director at the CIA.

Mr. Brennan, we are very appreciative of your being here today. I was going to say we have your testimony, but, do we have your testimony? We do, in fact, have your written testimony and we want to thank you for that, and also want to add five minutes for you to summarize that testimony.

STATEMENT OF MR. JOHN BRENNAN, DIRECTOR, TERRORIST THREAT INTEGRATION CENTER

Mr. BRENNAN. Thank you very much, Mr. Chairman.

Thank you, Mr. Turner.

It is certainly a pleasure to appear before the committee today to be with my very good colleague, Secretary Loy, who, as he said, we have gotten to know each other quite well over the past many weeks.

I have submitted the written testimony and I look forward to answering your questions. But I would like to start off as we begin the hearing on the Homeland Security Advisory System, making three key points, important points, about the Terrorist Threat Integration Center's role in that system.

The Terrorist Threat Integration Center, which we refer to as TTIC, since its stand-up on 1 May of last year, has played I think an important role supporting the Department of Homeland Security during periods of heightened concern about terrorist attacks.

As you know, TTIC analysts have full, unfettered access to the full array of information available to the U.S. government related to the terrorist threat to the United States.

This access allows the analysts, who come from the Department of Homeland Security, the Central Intelligence Agency, Department of Defense, Department of State, the FBI and other departments and agencies of the government to produce integrated assessments of the terrorist threat facing U.S. interests, both at home and abroad.

As a recent example, in the very late hours of 20 December of last year, TTIC produced a terrorist threat alert and an analytic assessment of the Al-Qa'ida threat to the homeland, including against the aviation industry.

These TTIC products were key factors in the decision made the following day to raise the threat condition level to orange. Language from these TTIC products was provided to the Department of Homeland Security, to Secretary Loy and Secretary Ridge to use both publicly as well as in their interactions with state and local officials.

Second, even when the threat level is not heightened, TTIC has constant, in-depth interaction with the Department of Homeland Security intelligence components, indeed components throughout the Department of Homeland Security involved in the fight against terrorism. At least twice daily, TTIC and Department of Homeland Security officers are involved in a secure video teleconference with their colleagues from throughout the government to review the threat reporting and to look at it in terms of what type of threat it poses to U.S. interests.

In addition to these opportunities, there are also regular interactions between DHS and TTIC officers to include electronic connectivity between TTIC and the Department of Homeland Security. This greatly facilitates the flow of information that is necessary for the Department of Homeland Security to do its work.

Finally, TTIC, the Department of Homeland Security and other elements of the homeland security, law enforcement and intelligence communities engage in regular discussions on the many different factors that are taken into account when determining threat

condition. This integrated effort allows threat information, which the TTIC provides, to be assessed in the context of the assessed capability of a terrorist group, in the context of the vulnerability of potential targets, in the context of extant mitigation and defensive measures that are in place, as well as in the context of the options available to enhance security.

In this manner, Secretary Ridge, Secretary Loy and other senior officials are able to gain a true appreciation of the prevailing threat condition, and then make the informed decisions as appropriate.

I look forward to taking your questions.

[The statement of Mr. Brennan follows:]

PREPARED STATEMENT FOR THE RECORD OF JOHN O. BRENNEN

Good afternoon, Chairman Cox, Ranking Member Turner, and the Members of the House Select Committee on Homeland Security.

I appreciate the opportunity to join the Deputy Secretary of the Department of Homeland Security (DHS) to discuss how terrorist threat-related information supports the Homeland Security Advisory System (HSAS).

As Committee Members well know, U.S. interests at home and abroad remain at risk of terrorist attack. Usama Bin Laden and Al-Qa'ida represent the most significant terrorist threat; however, there are many other known and suspected terrorist individuals and groups with an interest and the capabilities to do us harm. Since the tragic events of September 11, 2001, many steps have been taken to prevent future attacks. One of the most significant steps has been the creation and implementation of a national, color-coded Homeland Security Advisory System.

The HSAS was originally established in March 2002 as a mechanism to inform the public during periods of elevated threats. TTIC supports the HSAS through the provision of terrorist threat-related information and analysis to those charged with administering the process.

TTIC is a multi-agency joint venture that opened for business in May 2003, to integrate terrorist-threat related information, collected domestically or abroad, to form a comprehensive threat picture. On a daily basis, TTIC coordinates terrorist threat assessments with partner agencies, including DHS, Federal Bureau of Investigation, the Central Intelligence Agency, Department of Defense, and Department of State. Assignees from these partner departments and agencies have, of course, been involved in the production of these assessments prior to coordination with their headquarters. Twice daily, these assessments and others are discussed during interagency secure video teleconference meetings to discuss the current threat picture. DHS, TTIC, and others coordinate regularly on a product that combines threat information with actions being taken to protect the Nation against those threats. This multi-agency coordination process is enabling the USG to better know what we know, compare information, and make rational decisions based on a more comprehensive threat picture.

When threat information dictates, TTIC participates in special meetings that are convened to determine whether to recommend to the Secretary of Homeland Security and other senior officials that the Homeland Security Advisory System condition should be adjusted. Last December 2003, for instance, TTIC—in close coordination with our partner entities - published a Holiday threat assessment that facilitated multi-agency discussions resulting in a decision to elevate the national threat level to "orange." TTIC's threat assessments played an important part of the risk evaluation strategy that was used in making decisions related to the threat level.

Another aspect of national preparedness and effective warning of terrorist threats to the U.S. and U.S. interests abroad, is more systematic information sharing across the intelligence, law enforcement, and homeland security communities. Progress has been made toward ensuring that all obligations are met, as detailed in applicable statutes and interagency agreements such as the Homeland Security Act and the Homeland Security Information Sharing Memorandum of Understanding (MOU) of March 2003, signed by Secretary Ridge, Attorney General Ashcroft, and Director of Central Intelligence (DCI) Tenet. On behalf of the DCI, and in close coordination with all partner entities, TTIC is facilitating efforts within the Intelligence Community to provide the Department of Homeland Security access to all information and analytic products required to execute its mission.

Within TTIC, there is connectivity with 14 separate USG networks, allowing for unprecedented, near-real-time information sharing—the key to our support to the

Homeland Security Advisory System. A primary conduit for information sharing across the intelligence, law enforcement, and homeland security communities is a TTIC-sponsored, classified website called TTIC Online. This website currently has over 2,500 users throughout the Federal government, and it is being updated to support collaboration and information sharing at varying levels, from Top Secret to Sensitive-But-Unclassified. The website is also being updated to enable users to search across disparate USG-maintained data sets and to enable account holders from multiple Federal departments and agencies to post relevant information for collective access.

In addition, TTIC is working with DHS and the Federal Bureau of Investigation (FBI) to ensure that all relevant threat information and analysis is expeditiously passed to state and local officials and law enforcement personnel, so that they may re-evaluate and adjust protective measures to prevent a possible attack. This rapid sharing of threat information with those working to disrupt potential terrorist activity is a critical area of emphasis in the national homeland security effort—some call state and local officials and law enforcement personnel our "first responders," but if the information reaches them in time to apply appropriate protective measures, they are really our "first and last defenders." For this reason, TTIC and others across the intelligence, law enforcement, and homeland security communities are working together to implement "write to release" and other innovative business processes to increase the number of sanitized and unclassified products available for rapid dissemination to better enable state, local, private industry, and foreign partners to implement protective measures in the Global War on Terrorism.

In conclusion, through collective effort, we are making daily progress toward improving National preparedness through the HSAS and the effective warning of the Nation.

Chairman COX. I thank you both for your testimony.

Members will now be recognized for questions. We will be observing the five-minute rule with the exception that members that were here within five minutes of the gavel will be able to extend their time of questioning by three minutes.

The chairman recognizes himself for five minutes.

I would like to ask both of you or either of you, depending on how you care to respond, about the difference between the public and the nonpublic aspects of our national response to this heightened alert.

We have, as you both outlined in your testimony, an admirable system, still developing but very far advanced from where it was a few years ago, of sharing information among scores of government agencies at the Federal level and integrating that information also at the state and local level.

The TTIC online example that you provided, for example, is a secure network that can be accessed by many users all over the country. That is working, as I think citizens expect it should, so that our government springs into action, does everything it can to anticipate and prevent and prepare for terrorist attacks in response to actionable intelligence.

What we are also wrestling with here today, though, is the impact on the rest of the country, specifically everybody else who is not part of either law enforcement or intelligence.

The government in any way does not manage a large chemical facility or a nuclear power plant, does not run an airport or an airline, is not responsible for a high-rise office building—just somebody watching TV who is told, "Now, we are at a heightened state of alert."

Why are we asking that person to be at a heightened state of alert? What do we expect that person to do differently? And how do we expect that person to square that message with the simultaneous message, at least what we have seen was a simultaneous

message in our recent experience, that you should go about your business just exactly as you were before?

I ask you this question because in my experience, these warnings are having a chilling effect. I have admittedly episodic evidence, but a lot of it, of, for example, school groups canceling their field trips to other countries that have nothing to do with terrorist attacks on the United States of America. They do not know that. They are just worried, and so they are playing it safe.

Business groups canceling conferences, even sometimes within the United States, in other cities, all manner of tourism being affected from small to large decisions that people make. They are behaving differently because a heightened state of alert means to them a heightened state of anxiety.

What is the payback for that? And how are we going to mitigate those effects of the public warning system?

And if you can in addressing that, also include in your answer the consequence and the way that you deal with this consequence of the fact that in communicating publicly with 280 million Americans we are also communicating very publicly with Al-Qa'ida, or whoever it is that we must thwart.

And I would be happy to hear either of you.

Admiral Loy, you seem ready to begin.

Admiral LOY. I will take a stab at it, sir.

I think first and foremost, Mr. Chairman, we are all, as citizens and as responsible public servants, learning our roles in this very, very new security environment that we all woke up to on 9/11/01.

It is just so fundamentally different from—not that any of us are pining for the good old days of the Cold War. But the notion of what occurred from 1989 to 2001 was almost an interruption, when the wall fell and the Soviet Union imploded, that the whole notion of a complacency gene sort of rose among us.

And I saw that not only in individuals and people but perhaps in organizations and even in nations. And come 9/11/01, that cold pail of water in the face, offered a very different environment, an enormously different environment, an enemy that we do not understand, that we are just beginning to learn about, that we are just beginning to read about, with no flag, no president, no boundaries, no nation-state—all those things that were comfortable to us in the course of the Cold War window.

So as we try to learn our way through that fog, if you will, toward a more clear day when we will really be able to react much more adroitly and specifically to the things at hand, I think the challenges have to be about across-the-board notions.

But for the individual citizen, I think three things are important. I think it is about awareness, it is about preparedness, and it is about recognizing they, too, have a contribution to make, almost in the Rosy the Riveter notion of World War II, because this is really an all-hands evolution. Every citizen has the potential to be involved.

So on the awareness side, vigilance matters. And to make that an impression on the citizens of this country is an enormously important thing for us to do. We have to have every citizen understand it is important to hold the edge associated with this new security environment that we are grappling with.

So that means every citizen is a sensor. They have the opportunity to report things that are out of the ordinary, and they should be doing that.

And the notion of interoperable communications suggests that that citizen should have the capacity to report whatever they see out of the ordinary that makes good sense to them.

Preparedness is simple things as much as a family emergency plan, an emergency kind of support kit that would be appropriate, and finding their way, as a citizen must, in this new normalcy that we are trying to define for ourselves in the new security environment we are grappling with.

Chairman COX. I take it that we do not wish that level of preparedness to evaporate if the threat level is at yellow?

Admiral LOY. Absolutely not, sir.

Chairman COX. So that by ticking up the threat level, we are not telling them at that time to go do an emergency preparedness kit or at that time to start looking for suspicious activity?

Admiral LOY. No sir. If you look, for example, at the department's Web sites associated with such things, you will find counsel to the citizens at large that are directly along the line of both yellow and orange as a set of conditions that demand of them these kind of different behaviors in the security environment that we are all trying to understand.

Chairman COX. Mr. Brennan, do you want to add to this?

Mr. BRENNAN. Mr. Chairman, I would just make reference to the TTIC online, which is the classified Web site that we in TTIC maintain to make information available to the Department of Homeland Security and other Federal departments and agencies.

We are working very closely with the department to in fact try to construct a multilayered and interconnected classification system as far as the flow of information downward.

And so as you pointed out, the Department of Homeland Security has a statutory responsibility for providing the information to the state and local officials. And we, with TTIC online, are working with the department to make sure that there can be that flow of information to the departments so that the department can then take the information and share it as appropriate.

Even though as a classified Web site, we put products on there that are at the unclassified level, or at the sensitive but unclassified level, that can be released. So we are working hand in glove with the department on that effort.

Chairman COX. Well, I will reserve for a later round of questioning similar questions that get at that point, Mr. Brennan, about what state and local law enforcement can do and what specifically we are asking them to do when we change these alert levels. And certainly that access to information is a key starting point.

Mr. Turner?

Mr. TURNER. Thank you, Mr. Chairman.

Admiral Loy, Mr. Brennan, I, as you know, share much of the sentiment that the chairman just shared. I mean, I have many instances of folks saying they have canceled their plans to do things that, frankly, my better logic would say they had no reason to cancel, because they heard we changed the alert system to orange.

I think when we look at our efforts, there is no question that we need a threat advisory system and we need to see it continue to mature, as I think it is doing.

And I even noted on several occasions where Secretary Ridge has himself questioned the system and has made some adjustments already as your information gathering system matures.

But I really think the color codes, while may be useful two years ago when this was all new and we were in our infancy, and if you did not have a way to get the information out and you did not know exactly what you were hearing and how important it was, well, sure.

Let's say, yellow to orange—and I do not know what red means. I never did get a clear understanding of that. I had a lot of different people tell me what they thought it meant. But all I know is that if you said red today, it probably would just create mass panic. I do not know what it means.

But I really do think that you have reached the point where you could abandon these color codes and rely on specific threat advisory information. And if that information needs to go to the public, have a press conference and tell every network what it is we are worried about.

Much of the information, I think we all know, needs to be directed to local law enforcement and to the private sector that may be affected.

And that information sharing has not yet matured to the level it needs to. And we are going to have to, I think, get to the point where we have a greater willingness not only to sharing information among Federal agencies, which we always seem to have to struggle with, but with the Federal, state, and local officials who have a role in protecting the homeland.

But I agree completely, Admiral Loy, with what you said about the need to have the citizens involved. But I just do not believe the color code involves them. Because, clearly, as you stated, we need a culture, if you will, of vigilance in this country.

Every citizen has a role in protecting our homeland and they need to be reminded of that. But more often than not, I think, when the color code goes up, they do what the chairman said and they cancel some travel plans.

And think about it a bit, if you were the youth director at your local church and you had responsibility for 30 children of parents in your church, and you heard the alert system went to orange, your tendency would be to say, "Listen, I better not risk anything here; we better cancel this trip." And that ripples all through the society every time you raise that level.

And I even think it goes on in the department. I think the political reality that I shared a minute ago is very much the case. And I really think the department would be better off if, when you have new information, the key players in the department and the FBI and the White House, if they were talking about, "What is it we have on our hands and what information can we share and how quick can we share it?" rather than sitting around the table and getting on these phone calls that I am sure that take place, saying, "OK, should we go to orange, should we not go to orange?"

It is just basically a judgment that somebody ultimately has to make. And I do not think there is any great precision in it. Because the flow of threat information, as I said earlier, I think we all understand it is fairly regular and continually constant.

And, Admiral, you said we need the citizens to be prepared, and we do. And we probably failed in this regard, because the color coded system has not prompted anybody that I know of to make different preparations for different levels.

And if you ask the average person on the street, when the level went to orange, they might have declined to go take a trip, but I doubt many of them would tell you, "Yes, I made sure I had more water in the basement," or whatever it is that we all think folks are supposed to do when the level goes up.

So I guess my question for you is: Have there been serious discussions within the department about the color codes and whether or not the color codes are really an important element of an effective alert advisory system?

Admiral LOY. Yes, sir. There have been such discussions.

I, too, believe this is a work in progress, and there very well may come the day when categories, as are reflected by the colors, are no longer necessary when our citizenry and our private industry sectors and the state and local governments actually have the capacity and have internalized this new security environment that we are dealing with and are adequately prepared to deal across the spectrum from low threat to high threat as it really does change, perhaps not day to day, but over the course of time.

My sense is that we are not there yet.

There are very valuable levels of activity that are clarified for many of the industries that we are dealing with already. And as we reach out, just as we are speaking, to engage all of those economic sectors with respect to following on the president's homeland security Presidential Directive No. 7 on critical infrastructure, we will be able to at least initially sort activity levels associated with those industrial sectors and geographic places according to a range from low to high of varying activities associated with a threat, if in fact a threat can be understood to be that and communicated to them.

The communications channels we have in place are very strongly now able to communicate that information. But what we are still working very hard on is the delineation of what is different between the activity set associated with yellow, for example, from that of orange.

I have run the Transportation Security Administration for the last couple of years, sir. And I can guarantee you that every airport in this country has a security plan that denotes a variety of activities that change as we go from one threat condition to another.

So for the moment, it is a very good set of anchors along the path to a spectrum perhaps of adjustment that can be made further down the road. I believe they continue to serve a good purpose for us today.

Mr. TURNER. Thank you, Admiral. And I am not telling you I disagree with classifications that apply to sectors. I mean, I can see the wisdom of that.

Admiral LOY. Sure.

Chairman COX. The gentleman's time has expired.

The gentlelady from Texas, Ms. Granger, is recognized for eight minutes.

Ms. GRANGER. Thank you very much.

I appreciate your being here and the work you are doing. And not to beat a dead horse, as we would say in Texas, but let me add my concern about the color-coded system.

A little different, there are some people, yes, who do react. My concern are the people that listen to it and now have become very cynical and very angry—one or the other. And the cynicism will lead them to do nothing differently. And so that is a concern I have.

I am very aware the airports do make a change and are very aware of what they are supposed to do, but others are not, particularly at the local community. So when you go from one color to another, there is concern with what they do, and then of course the cost of doing that. And the local communities are having a real struggle keeping up with additional costs that are not being reimbursed.

Let me move from that to something else.

In the fiscal year 2004 Homeland Security appropriations bill, it required a report on the use of NOAA's radio network, what we call the weather alert system. And I was going to ask if that report has been written. If so, could you summarize the conclusions of the report, and then what steps DHS is taking to use the NOAA system.

Admiral LOY. I apologize, Ms. Granger, I simply do not know where the status of the report is. I will check that out today and call you.

Ms. GRANGER. Great, I would appreciate that very much.

And one of the committee's goals is to ensure that DHS utilizes an alert advisory system. That means it can disseminate local alerts and national alerts. Have you focused on the available technology that is out there already for that alert?

Admiral LOY. Yes ma'am. I think there is a couple of very, very real communications kind of challenges that are part of what we are doing.

One of the things I think we can do dramatically is set standards such that they are associated with grants in the future, such that when the acquisition of communications equipment is procured, it is procured according to the standard such that they have become interoperable.

One of the most dramatic lessons that we learned from 9/11, of course, was at the World Trade Center when this police officer could not talk to that fireman, could not talk to that emergency medical technician because of not having interoperable communications.

It is one of the absolute goals of Secretary Ridge, and we have done some very good work on that to this point. Out science and technology directorate is right on the verge of establishing and issuing those standards such that down the road that kind of procurement process will yield continuing interoperable communications.

Ms. GRANGER. That is extremely important, particularly at the local level if you are talking about from hospital to hospital—all of those first responders.

Admiral LOY. Responders, yes ma'am.

Ms. GRANGER. Thank you very much.

Chairman COX. Does the gentlelady yield back her time?

Ms. GRANGER. I do.

Chairman COX. The gentlelady from California, the ranking member of Intelligence, is recognized for eight minutes.

Ms. HARMAN. Thank you, Mr. Chairman.

Welcome to our witnesses, both of whom are very competent managers and are doing an excellent job.

I want to commend you, Mr. Chairman, for holding this hearing. Among the hearings I know of that this committee has held, this would be up there in terms of the most important.

I also want to commend you and the ranking member for the bipartisan collaboration on this issue. I think it is critically important, as you know, that we engage in oversight activities by our committees on a bipartisan basis, and this is happening in this case.

I also think it is useful for us to be offering constructive criticism to Federal agencies. This is part of what Congress is supposed to do. We pay the bills and the taxpayers expect us to do this.

And, Mr. Chairman, I noticed in your statement, a large amount of constructive criticism, and I applaud you for it, and I frankly agree with the comments that you made.

I think it is useful for us to criticize constructively our Federal Government, and I am sure our witnesses took it in that vein.

And, Admiral Loy, you said that things are evolving, you are operating a work in progress. We all understand that. And so this criticism is intended to help you shape your future steps toward an end that we all share, which is to make our homeland safe.

So, Mr. Chairman, I am happy to be in this room, and I commend this productive activity of the House of Representatives. Today, there are too few activities like this. And so it makes me feel good, and I hope it makes all of us feel good to be part of this one.

I have questions in two areas. One is your point about the public, and the second is more technical questions about the interface between DHS and TTIC.

And let me not forget to mention my valuable visit to TTIC a few weeks ago where I saw Mr. Brennan and his very talented work force. TTIC is a success story in this government. I commend you for your leadership and as important, I commend those from a variety of agencies who work for you for their part in helping make certain that we keep our homeland safe.

Admiral Loy, I look forward to visiting your folks as well sometime soon. I think it would be a very valuable visit for me, both in my role as a member of this committee and as ranking member on the Intelligence Committee.

My question on the warning for the public is this: A year ago, I mentioned to Secretary Ridge, my interest in a program called FLASH. That program is an acronym which I cannot remember, but the idea behind it is to invent a curriculum for our public

schools which would be taught each year in the same week to all the children in the public schools by their regular teachers. And the point of this curriculum, which would become more complex with each year, is that both the teachers and the students would be trained in what to do in the event of a terrorist attack.

I am old enough, and I think you are, too, Admiral Loy, to remember the civil defense drills of the 1950's when I was trained on what to do in my public school, and it was valuable training.

It seems to me that in terms of an effective warning system for the public, making certain that every school kid and every school teacher knows what to do would go a long way toward reducing panic, improving response and giving parents the comfort that their kids will know what to do and be adequately protected.

But, I cannot get to square one on this issue. I have proposed a pilot project. I have offered, you know, five different permutations of how this thing could work.

Secretary Ridge sent me to the Education Department. They responded with a "no".

I think this is dead square in your jurisdiction, and I just want to mention it to you here, ask you if you have any comments about it, and urge you, please, to take back to Secretary Ridge at least one Member's opinion that this would be a very effective way to augment your threat advisory system.

Admiral LOY. My comments would go to be actually very supportive. I think the notion of what Mr. Turner and I spoke about just a moment ago of the holding the edge issue, the not allowing the complacency gene to kick back in place, of truly holding on to the sense of urgency that is associated with this global war on terrorism on the home front and then translating that to a consciousness, if you will, that is pervasive across our citizenry.

I believe it is in the very direct interest of all 280 million of us to have that kind of sense about us in this dramatically different security environment that so many people actually would like to sort of just push away and return to normalcy, whatever normalcy used to be. But we have a new normal normalcy, and this has got to be part of it.

I will, in fact, carry your message back to the secretary. And we have initiated a number of educational notions inside our science and technology directorate which can translate to curriculum elements that would be very profitable.

Ms. HARMAN. Thank you for that answer. I will be following up. Be warned.

I hope we will do something like this, at least on a pilot project basis, in the school system in one or more states to see how it works.

But the curriculum has been developed. A very talented team of people, who happen to be based in California, has developed it and is trying it out, and I really think this will add value to the public piece of the threat warning and homeland security problem.

Turning to the interface between your two organizations: This is also critically important. Some members of this committee—I think all members of this Congress—were surprised when the president suggested that TTIC be stood up. It was not the way we had intended this to go in the way we drafted the homeland security law,

but I, for one, am pleased with how it is going and am very pleased about the connection between the two of you.

My questions just want to probe this a little further, and I will observe my time.

First of all, Mr. Brennan, you mentioned in the past that one of the major strategic issues for you is figuring out where TTIC's counterterrorism job ends and the counterterrorism work of other agencies begin. You convened something called the Water's Edge Panel, and I am curious how that came out. And I do not want this clock to go off here.

I would invite both of you to tell me how you are working together, whether there are any problems with sharing information, sharing technology, interoperability, which was raised before, meeting each other's intelligence needs, or anything else out there that you did not cover in your testimony that this committee should be aware of.

Mr. BRENNAN. I would say that, first of all, there are a series of challenges as opposed to problems.

The challenges as far as bringing together different information systems—in TTIC we have 14 different information systems that come in from all the different departments and agencies. In trying to address the different information security policies, different infrastructure, hardware-software issues—those are challenges that we are overcoming.

So these are things that we are working very compatibly on.

We have, in fact, a joint program office: TTIC, the Department of Homeland Security, and Department of Justice, FBI to address these initiatives in a collective and a collaborative way as opposed to doing it individually.

So again, there are a series of challenges there, but it is something that I think we are able to attack together. And we are making progress every day.

Admiral LOY. I would just wholeheartedly agree.

I think the most important thing in here is that the law clarified the realities of 9/11, clarified intent on the part of all the players.

And at those twice-daily sessions, where each of us has an opportunity to hear John's analytical product be tabled and then the discussion offers the opportunity to come to a collective consensus onto what that threat piece really means, and then offer it forward as something that has really been kicked around among ourselves, us from the standpoint of the operator and the requirements to be met, John from the standpoint of attempting to meet those and helping us understand just what are to the possible is inside the intelligence community flow.

We also have people connections as well as technical connections.

The secunded DHS representatives to TTIC that staff is his world as well as those from across the Federal Government are such that all the players that have a contribution to make are at his disposal to gather and allow the analytical work to be done inside the organization. I think it is going very, very well.

Ms. HARMAN. Well, just keep at it.

My time is up, Mr. Chairman, but I would like to share a secret, and that is that the hard drives that are under the desks of the

talented people at TTIC have names. And their names for the moment are Huey, Dewey, Louie and Fred.

And a little humor goes a long way, but it is important that we keep developing the IT and that we keep it compatible and we keep moving this mission ahead together, and we keep the public trained to understand what they are supposed to do too.

Thank you very much, Mr. Chairman.

Chairman COX. The gentlelady's time has expired.

The gentleman from New York, Mr. Sweeney, is recognized for five minutes.

Mr. SWEENEY. Thank you, Chairman, and I appreciate the recognition. I also appreciate you conducting this hearing. Because I think as my prior colleague, Ms. Harman, just pointed out, this is one of the critical oversight responsibilities we have in Congress. And we oftentimes, I think, have not been as particularly focused as I would like.

I would like to thank Admiral Loy and Director Brennan in advance for their cooperation and their work both here today and prior to this.

You know, the principle piece of legislation this select committee has proposed has a number of very valuable and important components to it. And I think it is reflective of a bipartisan effort on this committee's part to really help you as you evolve this process and construct what is an entirely new concept in American government.

One of the pieces I think is particularly important in that legislation is when we call upon the Department and try to help you establish a sector-by-sector or regional threat assessment system.

There are a lot of reasons why there is great utility to that. There are a lot of reasons why it is important. And I will simply point out as a New Yorker, I know I would expect that my colleague, Congresswoman Lowey, will also follow up with some of this.

But New York, and New York City in particular, have huge costs that cannot be reimbursed right now by the Federal Government. And one of the tangible examples of that is when the rest of the country goes to yellow, New York City pretty much constantly stays at orange.

I will ask Admiral Loy this question—when do you think the Department can move to that kind of more specifically focused threat analysis and threat information system?

Admiral LOY. Mr. Sweeney, I think we are very close to being there. The capabilities that are now important for us get on with are the analytical work necessary in a partnered fashion with the stakeholders of all 13 economic sectors of the Nation and the four key assets inventories that are identified in the president's national strategy for homeland security.

Since the president has now signed HSPD–7, the ball is in our court to do that outreach. A series of meetings were just held this week with respect to internal to DHS. The next one is internal to the department.

And then the template associated with that has to be taken literally to each of those 13 economic sectors to discuss through, understand the requirements on their end, what can be provided on

our end to establish that security paradigm, for lack of a better phrase, that we are all looking for.

Mr. SWEENEY. So as we speak it is evolving and developing.

Admiral LOY. Absolutely. Yes, sir.

Mr. SWEENEY. Within a year is practical or not?

Admiral LOY. Absolutely, it is, sir.

Mr. SWEENEY. OK, good to hear.

Admiral LOY. We should have that done inside a year.

Mr. SWEENEY. Director Brennan, thank you for all of your work and your interaction with my office.

How is the relationship with the FBI Joint Terrorism Task Force going?

Mr. BRENNAN. With the JTTFs that are located nationwide, it is a very strong relationship. We have had interactions, we have had TTIC officers who have been out to the JTTFs and have sat down with the FBI agents and analysts there to review different issues, review information.

We work very closely with the JTTFs through FBI headquarters in terms of the counterterrorism division that has sort of oversight on the terrorism matters.

So it very, very close.

Mr. SWEENEY. Has the FBI retracted or taken back any of its analysts from your operation?

Mr. BRENNAN. Oh, no, sir. In fact we are getting more analysts from FBI. And in fact, I have been very impressed with some of the young FBI analysts in TTIC in terms of their dedication and the quality of their work.

Mr. SWEENEY. Somewhere, there is that misinformation that recently in some sort of in-the-bowels kind of turf war, the FBI removed 70 of their analysts from your shop. We would like to know that, I think, on this committee. And I especially would like to know it as an appropriator who is both on Homeland and on Commerce–Justice–State. So I would like to know that if that happened.

Mr. BRENNAN. I have noticed none of them missing. If I do, I will let you know, sir.

Mr. SWEENEY. Let me ask one final question, and it is really for Admiral Loy: New York Police Commissioner Ray Kelly testified on the record before this committee and the Judiciary Committee last year. Another important part of the principle piece of legislation relates to the formulation and how we are spending money and what you are allowed to do and what you are not allowed to do.

He noted that the personnel costs in New York City are a significant part of the expenses when the threat level is increased. I am wondering, your thoughts. Why shouldn't overtime costs, personnel costs, training costs associated with those increases be reimbursed?

Admiral LOY. Sir, I think the categorization of grants and the ability for state and locals to claim against those dollars over the course of time is the answer to that question. It, too, is something I think that is evolving.

The Congress was generous in the supplemental on all three till I identified $200 million in the aftermath of Liberty Shield as a pool of funds to be claimed against by the locals, state and local elements.

There is about 60 of those billions of dollars that have actually been claimed against as opposed to the $200 million that has been offered.

There is an exchange going on as we speak. We clarified that the 23rd of February was sort of a deadline that we would like to have people let us know what were the costs associated with this last experience at orange over the holiday period. That will give us another data point associated with the role of the Federal Government, as appropriated by the Congress in terms of the capacity to reimburse, and also help us all understand that as, again, we have talked about several times before this afternoon already, this is really an all-hands evolution.

And so to some degree, it is about state and local folks standing up to the task, including the financial end of whatever is appropriate for these evolutions, and the private sector as well.

So in threats to our national security historically, you know, when it was the artillery folks looking over the Folda Gap at each other or whether it was across the demilitarized zone in Korea, the notion there was the clarity with respect to Federal responsibility in taking care of that "for the citizenry" was very, very direct.

This is a very different security environment that we are grappling with in understanding. The rules as they play out, sir, are still literally being forged by the Congress and by the executive branch.

Mr. SWEENEY. And I understand that. I know my time is expired, but I think we need to get specifically focused on the impacts in order to maintain the vigilance we seek here. And I thank you.

And I thank the chairman for his time.

Chairman COX. I thank the gentleman. The gentleman's time has expired.

The gentleman from Massachusetts, Mr. Markey—the proud owner of a Super Bowl trophy, almost, almost personally, derivatively. He is recognized for eight minutes.

Mr. MARKEY. Thank you, Mr. Chairman, very much. It is water on the desert up in Boston, I can promise you. It has been a long drought in every other sport but football.

Mr. Brennan, your job is to remedy the problem that we found before September 11, that there was fragmented dissemination of information across the Federal bureaucracy to state and local governments that did not effectively make it possible to coordinate in a way that could protect against a terrorist attack.

As the Senate office building, Mr. Brennan, remains closed for a second day due to ricin contamination, we have learned that three months ago the White House also was the target of a ricin attack. However, the information reportedly was not shared with congressional leaders until after the discovery of ricin in the Senate earlier this week.

Mr. Brennan, did this information, that is, the information about ricin attack on the White House, did that come to your attention three months ago?

Mr. BRENNAN. Sir, I would have to go back and check the record as far as when it came to my attention. And I can get back to you on that.

Mr. MARKEY. Did you know about the ricin attack on the White House before there was an attack on the Congress?

Mr. BRENNAN. As far as an attack, sir, I do not believe—and I also do not think, sir, this is the appropriate forum for discussion about the nature of particularly the terrorist threats that may exist to the White House. There are other venues.

Mr. MARKEY. Mr. Brennan, this is the forum. We are the committee given responsibility to make sure that the agency, which we have created, is working to protect the American public against attack.

If you had knowledge that there was a potential ricin attack on the White House, and you did not give that information to the Congress, or other relevant high-priority targets of Al-Qa'ida, then that is something that we have to talk about and you have to tell us what is your decisionmaking process as to who is on the list that receives this very important information.

Mr. BRENNAN. Mr. Markey, I would be glad to talk to you about the process. My comment that this is not the appropriate forum is because sometimes with threat information, as you well understand, there is classified information, and this is an open hearing. And so, any type of discussion about the underlying reporting or information regarding that should be kept in appropriate channels.

Mr. MARKEY. OK. Well, let us put it this way: Did you notify the Capitol Police when you found about the ricin attack on the White House?

Mr. BRENNAN. Sir, I would have to go back and I would have to check as far as what action was taken, when such information was known.

Mr. MARKEY. You do not know if you notified?

Mr. BRENNAN. I will have to go back, sir, and check on that. I do not want to give you—.

Mr. MARKEY. Doesn't an attack on the White House, Mr. Brennan, automatically trigger a set of responses in TTIC in terms of notification of other high-priority targets?

Mr. BRENNAN. Sir, I would like to get the facts in front of me first before I respond to your questions as far as what actions were taken.

Mr. MARKEY. To the best of your knowledge, did your agency notify mail processors handling mail bound for Capitol Hill or basically the same post offices that had to be shut down after the anthrax attack here in Washington? Did you notify them?

Mr. BRENNAN. It would have been our responsibility to notify the Federal departments and agencies that have a responsibility to share that information with the nonFederal family.

Mr. MARKEY. Well, I will tell you, Mr. Brennan, that if the White House took upon itself not to share this information with other potential targets in Washington, D.C., then that is a very serious matter.

We know that Al-Qa'ida was targeting either the White House or the capitol dome with the final plane that was pulled down in Pennsylvania. And we know that within that same timeframe, Congress was the subject of anthrax letter attacks, as were the networks and other high-visibility institutions in the United States.

So I believe that if that information was not shared, then there was a very serious mistake which was made.

Mr. BRENNAN. As I said, Mr. Markey, I will look into it and find out what the facts are.

Mr. MARKEY. Well, we cannot thwart—I would just put it on the record that we cannot hope to thwart terrorists who use the U.S. mail system and other means to threaten our homeland security without all the facts.

It is, to me, unnecessary. And as the facts unfold, potentially appalling, that innocent lives could be put at risk if they were not given the fundamental information that there was already a ricin attack that had occurred in Washington, D.C., that protective actions could have been implemented to lessen dramatically the likelihood that that could be a successful attempt.

Mr. BRENNAN. Mr. Markey, I can tell you that the Terrorist Threat Integration Center has looked very carefully at the potential use of CBRN materials by Al-Qa'ida. We have shared information with those respective departments and agencies that have responsibility for guarding against those types of attacks.

And we also have worked with the Department of Homeland Security and the FBI and others to ensure that the appropriate measures are put in place.

And so, as I said, on that particular case, on that particular day, as far as what happened, I will be glad to check the record on this.

Mr. MARKEY. You can understand that two days after this attack unfolds, the fact that you do not know the answer to that question as you sit here is something that in and of itself causes some concern to those of us who are in charge of overseeing the department.

Admiral Loy, you have Secret Service as part of the Department of Homeland Security. When did you learn of the ricin attack?

Admiral LOY. I was not in the department at that time, sir. But I did anticipate that this question might come fro the committee this morning. I touched a base with the director of the Secret Service who advises me that his recollection was that the reports were made constructively inside the executive branch. I did not ask him whether or not they had advised the Congress. I will go ask that question, sir, and get back to you.

Mr. MARKEY. Is that a decision that the White House has the right to make under these existing new share-the-information rules and regulations, that is, can the White House decide, just as a matter of executive branch authority, not to share that information with the Congress or other Federal institutions or other state and local institutions that might also be at threat? Is that a policy?

Admiral LOY. Of course not, sir.

Mr. MARKEY. It is?

Admiral LOY. Of course not, sir.

Mr. MARKEY. Of course not.

So if the Secret Service and the White House decided not to share this information with the Congress, knowing that we were a target just two yeas ago—the staffer over my shoulder here, she was on Cipro for two months—that is a very serious issue to those of us who lived through that. It touched the lives of the people who are here and working with us—and as proxies for all other Americans as well.

So do you think that the system works, Admiral Loy? That is, do you believe that the White House having obtained this information handled it correctly in terms of ensuring that the rest of the vulnerable targets would also be notified?

Admiral LOY. Sir, all I know is the conversations I had with Mr. Basham this morning. I will be delighted to found out who called who when and let you know.

Mr. MARKEY. Well, let me ask it another way: If Congress did not know, do you think the system worked?

Admiral LOY. No.

Mr. MARKEY. The system did not work.

Admiral LOY. Right.

Mr. MARKEY. OK.

Mr. BRENNAN. I might add, Congressman Markey, that there is a representative of the Capitol Police within the Terrorist Threat Integration Center who is fully cleared and authorized for access to information such as this.

Chairman COX. The gentleman's time is expired, but we may return to this on a subsequent round.

The vice chairman of the committee, the gentlelady from Washington, Ms. Dunn, is recognized for five minutes.

Ms. DUNN. Thank you, Mr. Chairman, thank you very much.

And, gentlemen, I apologize for not having been here to hear your earlier testimony and the other questions, so forgive me if I overlap on some questions. I was in another committee meeting.

I wanted to ask you, Mr. Brennan, when we first heard about TTIC, my inclination was to recommend that it be under the Department of Homeland instead of the CIA. Have you had any reason to change your opinion of where TTIC should be located?

Mr. BRENNAN. First of all, Ms. Dunn, TTIC is not within the CIA. We are located right now, temporarily, at the CIA compound.

Ms. DUNN. But you are funded by the CIA, is that correct?

Mr. BRENNAN. We receive funding from the director of central intelligence budget. But in fact we see monies from all the different partner agencies.

So we receive it from CIA, FBI, Department of Homeland Security, Department of Defense and others.

So my view, though, is that we should not reside within in one department or agency because the fight against terrorism is a collaborative fight, and if we are really going to do this well, we need to have an organization or an entity such as TTIC that is able to represent the interests of those different agencies and departments.

Ms. DUNN. But the Department of Homeland Security has that as its primary focus.

Mr. BRENNAN. There are many different departments and agencies in the U.S. government that have a terrorism responsibility. The CIA has responsibility for transnational threats to U.S. interests, including at home.

The Department of Defense has that responsibility, the FBI and others.

So, yes, the Department of Homeland Security has the responsibility for homeland security. But the threat to the homeland from international terrorism is truly international, and TTIC has that

worldwide responsibility to report and analyze on those threats to U.S. interests at home and abroad.

Ms. DUNN. What is your relationship to IAIP? Is that relationship and that coordination satisfactory to you now?

Mr. BRENNAN. It is very close. Information Analysis and Infrastructure Protection Directorate within the department, we have constant interaction with them. The assistant secretary for information analysis, for example, retired General Pat Hughes and I are on the phone constantly. We have daily meetings, several times a day.

The under secretary for IAIP, Frank Libutti, is also someone who I am in regular contact with.

So it is very satisfying. It is improving and growing stronger.

Ms. DUNN. In your opinion, do they have the adequate resources to perform the analysis of function after they get the information?

Mr. BRENNAN. We do not collect the material. But I would defer to Admiral Loy as far as whether or not they have the adequate resources to do their mission.

Admiral LOY. They certainly do, ma'am, and that is growing as part of the department's growth as we speak. Literally, they are physically moving to another building with adequate space to put analysts in seats, if you will. And so the growth is a work in progress as well.

But the notion that John cites I think is the important point here.

DHS is enriching TTIC's ability to do its work by the contributions and the flow of whatever our piece of the information and intelligence-sharing process is that our people at TTIC provide him.

At the same, he enriches our ability to do our work by having this full all-source array of material at his disposal to do his analysis, to create his products from, and then we accept those products back in the other direction for the mission of securing the homeland.

There is a very strong assessment process that I think is appropriate for us to go through as we then attempt to map that threat piece to the economic sectors, regions of the country or individual citizens, whatever might be highlighted in the threat piece that he has provided us.

So at this point, the free standing nature of TTIC as an entity is serving the best interests of the country very, very well.

Ms. DUNN. How does the organization work? Do you have regular meetings? Or do you meet on a needs basis? Or do you do work by e-mail or over your communications devices? Is it hierarchical? Is it that you reach out when you need to to the particular department that you are interested in talking with? How does it work?

Mr. BRENNAN. It works in all the above ways that you mentioned as far as we have regular meetings, we have twice daily secure video conferences with the Department of Homeland Security. We have electronic connectivity as far as sharing information both ways, between ourselves and Department of Homeland Security. We have officers from the department, not just IAIP but also from the various constituent agencies—the Coast Guard, the Secret Service, Customs, others—who actually are resident within TTIC

performing the analytic function and liaising, then, back with their parent agencies.

So it is across the board, both in terms of information sharing, people, interaction meetings. There are regular meetings throughout the week where I, along with the DHS counterparts, get together to review threat information as well as the actions that DHS is taking.

Ms. DUNN. Just to finish my questioning: Is there any area where you believe that communications could be improved with regard to TTIC's relationship with these other agencies of government?

Mr. BRENNAN. I think as we referenced before, this is an evolving process. We have a number of challenges ahead of us as far as stitching together the different types of information systems. We have different metadata standards as far as how reporting comes into the government.

So there are a lot of challenges out there, and I think we are making progress on it, and we need to make further progress.

But I feel good about the progress that has been made to date.

Admiral LOY. Ms. Dunn, if I may, one other thought: The other value of the free-standing nature of TTIC is that, I believe that on down the road we will find valuable other kinds of data and pieces of information that heretofore have probably never been part and parcel of the thought patterns about analyzing the threat to the homeland.

For example, I believe much more can be done with respect to proprietary private sector data—what is in that container coming at us? What does the bill of lading say? What does the manifest say?—and the mixing bowl that TTIC represents by having all those kind of things in the future offered into that cauldron, so to speak, so that the mix is the product that is of greater value to those of us who are trying to secure the homeland, or to those of other executive functions that are trying to do their work overseas.

Projecting down the road, I think this freestanding nature represents a continuing positive opportunity.

Ms. DUNN. Thank you very much, Admiral.

Thank you, Chairman.

Chairman COX. I would just observe, as I yield to the questioner, that TTIC is not, strictly speaking, freestanding, but rather it is under the direction of the director of central intelligence.

And when you talk about something that may well have fruitful ends for homeland security such as further mining private sector data, it is because of, among other things, civil liberties concerns, that many of us in Congress did not want the DCI to be in charge of the intelligence analytical portion of homeland security, that integrating fusion function.

And it is why if somebody is going to be in charge, I would much prefer that it were the secretary of homeland security. As I said in my opening statement, that is a carol for another Christmas.

And so I yield next to the gentleman from Maryland, Mr. Cardin, for eight minutes.

Mr. CARDIN. I thank you very much, Mr. Chairman.

And let me thank both of our witnesses that are here for their service to our country in this very important area.

Admiral Loy, I was listening to your response as to what we expect on the code changes from the different stakeholders, including local governments. And you point out, and I think rightly so, that we all have responsibilities, including local government, to do what is necessary for the security of our country.

I am not exactly clear what we expect, though, when we change the coding from local governments. Do we expect that they will increase their presence of law enforcement in the community? Will they tighten up their port securities, if they have ports? Will they do their critical assets, more police patrolling? And probably all of the above, you will say, and that this is something that is somewhat intuitive, although I think we should have better understanding as to what these code differences mean.

You then point out, though, that the funding for this additional burden is reimbursable under the general funding formula, or grants, that we make available to local governments. And that is at odds with what we are being told by the conference of mayors and our governors.

The chair of the Homeland Security Task Force is the mayor of Baltimore. And I have talked to him frequently.

Mayor O'Malley said: Cities are our front lines in ensuring homeland security. And America's cities need direct homeland security funding. We simply cannot fund robust homeland security on the proceeds of local property taxes and fire hall bingos.

The report that was issued pointed out that most—in some cases 100 percent—of the costs are borne solely by local governments and that there is no funds available under the current system.

Congressman DeFazio has a bill in Congress which has a lot of interest on both sides of the aisle to reimburse directly local governments when we change the code to a higher level for the additional cost.

I guess my question to you is: I would hope there would be some sensitivity to working with Congress to develop a more sensitive funding source to local governments to pay for the extra cost of when the security rise so that we have a national expectation as to what local governments will do but we are also providing the resources in order to carry that out.

Admiral LOY. It think it is a very, very difficult and appropriate question for us all to get on the table and grapple with, sir, until we have that resolution.

There are an existing inventory of grant systems in place as we speak today. Some of them are tailored to specific purposes—state formula grants, emergency management grants, Citizen Corps grants, law enforcement terrorism management grants, and the new grants associated with the urban areas.

And the formulaic approach to that I believe must be much more complex than the simple notion of a base-plus-per-capita kind of formula across the board.

And so the president's budget, for example, this year, when it came up, recognized by doubling the urban security grants, which are about a combination of population in general, the per capita notion, which remains sound; population density, for example, in terms of the likelihood of the targets there; critical infrastructure

associated with that particular area, community or region; and the threat itself in terms of how it is focused toward those things.

And so I believe there remains a challenge for us across the board in a distribution of those monies for the purposes that have been outlined by the Congress and reinforced by the administration.

But there is a nature of changing that formula to recognize, for example, Baltimore as opposed to my hometown of Altoona, Pennsylvania. Maybe there is a greater population density, critical infrastructure inventory, threat notion that is more appropriate there.

Mr. CARDIN. I appreciate that, and I agree with you said.

Our distinguished chairman and ranking member have been working very hard on the funding formula that, as the chairman indicated, will be marked up in the full committee soon, that is sensitive to the points that you raise.

I would point out, though, that I do not think it directly answers the concerns of local governments when we change the alert level in that there is some specific expenses that we anticipate will be incurred when we raise those levels. And the funding formulas really are not geared to dealing with that problem.

And I would hope that we could work together to try to figure out whether there is an appropriate way that we can help provide that assistance to local governments consistent with the national assessment on homeland security.

Admiral LOY. Yes, sir, I look forward to working with you, sir, on such things.

You know, again, the sort of shock value of what 9/11 represented to all of us, in this particular instance, became $200 billion in the supplemental of 2003 as a pool of recognized funds to be dispersed.

As I mentioned earlier, only $60 billion of those $200 billion have actually been claimed against to this point in our time line.

So we are sort of finding, like is often the case in the wake of a national tragedy, the mix between job description on one hand, so to speak, and the resources to do it.

Mr. CARDIN. Of course, that brings up the second problem, and that is getting the money actually out there as quickly as possible. And that is another area that we hope that the legislation we are acting on will help in that regard.

I want to turn to the budget itself because you have mentioned that a couple of times.

I am trying to understand the president's budget, and I am hoping that you may be able to clarify this point.

Interoperability is the one area that is been a very high priority of this committee. And in testimonies before the committee, we have talked about that as a prerequisite to a national system. Yet it looks like the 2005 budget zeros out the specific grant for interoperability. Am I reading that wrong—I hope?

Admiral LOY. I do not know that I have a good enough understanding of it, sir. I will get back to you with that specific question.

Certainly the intention with respect to interoperability is among the secretary's four or five most important things to try to get accomplished for our country this year.

Mr. CARDIN. Well, I appreciate that.

According to the information I have, it was zeroed out in 2005.

I want to mention one other thing, which is port security grants for state and local governments. It was included in the 2004 budget in transportation security administration at $124 million. It looks like that it is now in the opposite, domestic preparedness, but at $45 million, which would be a substantial reduction in port security.

Next to the airports, I would say that the next highest priority has been in port security. And I can tell you, again, from the Port of Baltimore, but speaking to my colleagues that represent many other ports, there is tremendous need there, and I would hope that we would be increasing the Federal Government's commitment to local government for port security and not reducing it.

I appreciate perhaps you could look into that also and get back to me.

Admiral LOY. All right, sir.

Mr. CARDIN. Thank you, Mr. Chairman.

Chairman COX. I thank the gentleman. The gentleman's time has expired.

The chair recognizes the gentleman from Connecticut, Mr. Shays, for eight minutes.

Mr. SHAYS. Thank you, Mr. Chairman.

Mr. Chairman, I have to control myself in this hearing because I find myself feeling like we are ships passing in the night. I find myself thinking, "Maybe we don't have a terrorist threat. Maybe it is all in my imagination. Maybe the 20 hearings I had before September 11 were really just, you know, make believe. Maybe the three commissions that we had"—talking about the terrorist threats—"we are just inventing this. Maybe September 11th didn't even happen."

I vowed after September 11th that I would not be silent about the threat. And now I am hearing that we have a system that I think makes sense. I think it makes sense. I do not care what color you call it. We have low, we have guarded, we have elevated, we have high, we have severe. I think it makes sense. I congratulate you for having a system that warns the people who can protect us in the general public.

What I think is idiotic, foolish and stupid is to go to a high threat and then tell the public, "Just do what you normally do." I cannot think of anything stupider than that.

Because it would seem to me that when you are going to high threat—now high threat is—a high condition is declared when there is a high risk of terrorist attacks in addition to the protective measures taken under the one below it.

How about just elevated condition? An elevated condition is declared when there is a significant risk of a terrorist attack.

You have low risk, you have general risk, you have significant risk, you have high risk, you have severe risk.

Maybe the problem is, on this committee, that we do not think you were right in going to high risk. But I think, Admiral, you thought you were. Correct?

Admiral LOY. Absolutely.

Mr. SHAYS. And we are now under significant risk. Isn't that correct?

Admiral LOY. Correct, sir.

Mr. SHAYS. Significant. Not general, not low, not no risk.

Admiral LOY. that is correct.

Mr. SHAYS. And it was based on the reality of information that was coming to you. Is that correct?

Admiral LOY. that is correct.

Mr. SHAYS. Why would the department tell people to do everything they would normally do? We are not at low risk, we are not at general risk, we are not even at significant risk. We are at high risk, second only to severe risk. Why should I just do what I normally would do?

Admiral LOY. I think it goes to both the comments from the chairman and from Mr. Turner that the notion of the secretary's comments when he has solicited awareness, when he has solicited preparedness and when he has solicited from the citizenry an understanding and even an endorsement, that their responsibilities entail recognizing there may very well be some inconvenience associated with what has just occurred.

Mr. SHAYS. So it is just about inconvenience? In other words, from the general public, we just have to know it is just about inconvenience?

Admiral LOY. Of course not, sir.

Mr. SHAYS. OK.

Admiral LOY. The reality here is that having solicited those senses of understanding from the American public, the secretary's also suggesting that they should go about their normal business as best they can under the heightened threat condition that has been established.

Mr. SHAYS. But maybe normal business does not mean you do not have to do something. Why would you have them do something that puts them at risk if they do not have to do it? Why would you put the general public at risk?

Admiral LOY. We are not trying to put the general public at risk, Mr. Shays.

Mr. SHAYS. In Israel, if they were at high condition, they would not invite people to assemble in a large crowd. Now, if you have to take a bus to get to work, they would tell you to take a bus. But they recognize there are certain things they do not want the public to do.

I have not heard one thing that you have said, even when you are at high alert, that you do not want the public to do. Tell me one thing they should not do.

Admiral LOY. I certainly do not think they should be doing things that are foolish as it relates normal activity.

For example, the question was raised in terms of whether or not the church group should go to Washington, D.C., to see the sites at orange as opposed to yellow.

My counsel is that having gone to orange, we have also raised the security paradigm to the degree that the secretary is encouraging that trip to be taken, and that trip can be taken safely and securely because of what we have undertaken to actually put into place activity-wise associated with the threat condition rise.

Mr. SHAYS. So if you think a plane is going to be hijacked, potentially from Europe to the United States, you would still tell your child to fly on any plane coming from Europe.

Admiral LOY. Sir, through the course of this last period, as a direct answer to your question, we thoughtfully, I believe, gathered all the right minds to the table, including our international colleagues at the government-to-government level and at the airline level, and arrayed what we felt would be the prescription of activities and mitigating strategies if in fact that plane were to fly.

And the choice, as you saw in the press several times along the way, made either by the government or by the airline—.

Mr. SHAYS. So it is a foolproof system? You are going to catch all terrorists?

Admiral LOY. Of course not, sir.

Mr. SHAYS. So isn't there a possibility that you know that a terrorist might be taking a plane from Europe and they might actually succeed, you might not catch them? Isn't that a possibility?

Admiral LOY. There is not a single moment where the secretary or the president or anyone else has said that we have a foolproof system. This is a journey, sir; it is not a destination.

Mr. SHAYS. I will tell you what I would do. I would do the following: If I knew a plane likely is going to be hijacked from Europe—because they do not have the same procedures we have, they do not have fire marshals—I would advise the people I love not to take a trip to Europe right now, just defer it until you go to code yellow or until you go to code blue.

Admiral LOY. And the point, sir, is if we provide the public with information, they can make those decisions. They can make those decisions.

Mr. SHAYS. So you want the public—so you do not want them do what they normally would do. You would like them to use their brains and maybe make a decision.

Now, if they want to make a statement of patriotism of not letting terrorists interfere with them in any way, let them make that. But shouldn't they be the ones to make that judgment?

Admiral LOY. And that is precisely why the secretary offers them both the combination of a threat condition change and the reflection that it represents in terms of additional activities security-wise, as well as, we heard earlier, the challenge to tell them in a public sector that it is their decision to make.

Mr. SHAYS. OK, I get your point.

We were concerned about planes being hijacked from Europe, particularly because they do not have air marshals and they do not do the same type of security.

Admiral LOY. No, sir. We were afraid—I will use that time loosely, to parallel your thought.

Mr. SHAYS. Concern.

Admiral LOY. We were concerned because of what we saw in the threat stream.

Mr. SHAYS. Well, but you do know the following: You do know they do not do the same process that we do. They do not have marshals on planes. Correct?

Admiral LOY. Many of them do not, that is correct.

Mr. SHAYS. And we encourage them to, but they still do not. We are encouraging them to do, and they are resisting.

Admiral LOY. Sir, in the case of many of—.

Mr. SHAYS. Isn't that true?

Admiral LOY. In the case of many of those, they in fact did exactly that.

Mr. SHAYS. OK, but we are encouraging them to. We are encouraging them to have marshals on a plane because we think there is a danger.

Isn't it not true that we were concerned about dirty bombs during this last code? Isn't that a concern?

Admiral LOY. Sir, I would take that one behind closed doors, if you do not mind.

Mr. SHAYS. Why? Why? Why would we take it behind closed doors? Why doesn't the public have a right to know? Why should I know and why should other people know and then tell their families to act accordingly but we are not going to tell the public? Why? Why? Why?

I want to know why, if we think there is a concern—I am not asking sources and methods. I want to know why the public does not have a right to know what you have a right to know if in fact it endangers the public?

If we are concerned about dirty bombs, why shouldn't the public know?

If we are concerned that it might be where a large congregation of people gather, why shouldn't the public know?

If we are concerned that it might be at a place where it is dramatic, why shouldn't the public know? Why should I know and you know but the public not know?

Chairman COX. The gentleman's time has expired.

But I think there has certainly been a number of questions put to you, Admiral Loy, so feel free to answer at whatever length you choose.

Admiral LOY. Thank you very much, Mr. Chairman.

Mr. Shays, the notion is very complex. The challenge here for us as public servants is to develop that security paradigm that will allow us to have confidence that the threat as identified and the map to economic sector—in this case, airlines—have an opportunity to develop a set of mitigating strategies that takes that threat sense down from where it was that gave us pause.

So our challenge through the course of those hours and hours and hours of discussions around that table at the CVITS twice a day, in international discussions with the players that were a part of our identified threat stream this past holiday season, was to take as good a set of judgments as we could in the interests of the security and safety of the flying public and to so require of anyone that was heading this way and were going to penetrate U.S. air space and get landing rights here.

And in each of those instances, sir, we either had those mitigation strategies met and those aircraft flew. Or in those instances where that was not possible, or chosen not be on the part of the international lines, those governments or those airlines canceled their flights.

Mr. SHAYS. Sir, I have tremendous respect for you. You are an American hero.

Chairman COX. The gentleman's time has expired.

Mr. SHAYS. Could I just please make this point?

Chairman COX. I am sorry, the gentleman's time has expired.

Mr. SHAYS. I just would like to say—.

Chairman COX. I am sorry, but the gentleman's has—.

Mr. SHAYS. —that it was a bureaucratic answer—.

Chairman COX. The gentleman's time has expired.

Mr. SHAYS. The terrorists know—.

Chairman COX. The gentleman's time has expired.

Mr. SHAYS. The terrorists know there there is a threat—.

Chairman COX. The committee will be in order.

Mr. SHAYS. —shouldn't the public know?

Chairman COX. The gentleman's time has expired.

The gentlelady from the Virgin Islands, Dr. Christensen, is recognized for five minutes.

Ms. CHRISTENSEN. Eight, but I will probably only take five, Mr. Chairman. I did not make an opening statement. But anyway, I only have a few questions.

But I want to thank you for this hearing, because the alert system is something that not only we in Congress but our constituents have to deal with on a regular basis. And to the extent that it can be clarified and brought to a level that is meaningful and where one is able to develop a specific response—which is what I think we are trying to get at today—this is a very important hearing.

I have, I think, three questions. Two to Admiral Loy.

And I want to welcome both of you for being here this afternoon.

And it goes back to the standardization of the responses at each terror level. Because you cited that in the area of airports, for example, I think in the instance of airports, they have clear responses as to what is supposed to happen when we go to an orange alert. But I think you allow that this is a work in progress and that other agencies, businesses, the public still have to develop a capacity and a knowledge base to be able to fine tune what needs to be done.

I wanted to know: Is there a systematic process ongoing to, one, develop those standards and then to communicate and put those standards in place? Or is this just kind of just flowing?

Is there something specifically being done to develop those standards, or communicate them and put to put them in place?

Admiral LOY. Absolutely.

Ms. CHRISTENSEN. And what is the time line that you have on that?

Admiral LOY. Absolutely, Ms. Christensen.

With respect to geographic locales, we have just literally received on the deadline of yesterday representative security plans from state and territory that is associated with our work.

We are reviewing them very, very carefully so as to look for those things that have become common concerns among states and territories to be dealt with in that fashion.

In the notion of your parallel with aviation, ma'am, that is a piece of the transportation sector. The other 12 major economic sectors are each being reached so as to have not only a blueprint for what they should be doing but rather to have them also help us

develop that blueprint. Because they know much better than we do what are the essential ingredients, for example, of securing their chemical plant or their nuclear plant or whatever it is that they are responsible for.

This is a very active and very ongoing outreach program. And I would like to think that by the end of this year we will have the national game plan for critical infrastructure protection in place.

The president has just recently signed, as I mentioned earlier, the homeland security presidential directive on that. The ball is now in our court to engage all the players as appropriate to do so. And we are very actively doing that.

Ms. CHRISTENSEN. The agencies or the Federal Government—and I often come back to one that I have responsibility for, which is the National Parks Service.

When we go to orange alert, a lot of the agencies, all they can do is a shotgun approach to responding to that alert. Is there something being done to also prepare standards in terms of their response at different levels? What is absolutely required of them? Because they are not being funded to respond to these alerts. The money is coming from other operational dollars.

Admiral LOY. There is an interesting question there, ma'am, for an authorizing committee, for example.

The notion of whether or not the interior budget ought to be looked at through the lens of whether there is adequacy with respect to homeland security activities and responsibilities may be something of interest to the committee.

I only parallel my personal experience in the counternarcotics effort when, as a Coast Guard commandant, I was obligated to make sure my budget that had to do with counternarcotics was authored through the Office of National Drug Control Policy for their commentary on the way to OMB so that they could pass judgment on whether what I was asking for was going to be sufficient to the responsibilities that they saw me doing for them in the counterdrug effort.

There may be a parallel notion here that would be of value to the committee.

Ms. CHRISTENSEN. I think they need some help. Many of the parks are areas where either illegal people or goods can pass through.

Admiral LOY. Yes, ma'am.

Ms. CHRISTENSEN. They need some help in developing specifically what they need to be doing, what they need to be putting in place at different levels of alert so that they can plan.

Admiral LOY. You are absolutely right. This is an all-hands evolution. It is not only private sector, state and local, but it is of course all the Federal agencies and our responsibilities as well.

Ms. CHRISTENSEN. And you said that as in the last orange alert for the country was dropped to yellow, there was still some targeted areas that remained at high alert. And I wanted to know to what extent were our members of Congress who represent those areas informed? Is that standard practice?

Admiral LOY. I personally picked up the phone and called several folks associated with helping them understand as the threat was going by. The secretary's judgment in terms of being lowered to yel-

low offered the opportunity for us to continue to concentrate on a couple of economic sectors and on several geographic locales. Those players were communicated with routinely, ma'am, including at the local level. For example—.

Ms. CHRISTENSEN. But specifically members of Congress—.

Admiral LOY. Oh, yes, ma'am.

Ms. CHRISTENSEN. —can be expected to be informed if an area in my district, or any of our districts, remain at high alert.

Admiral LOY. That would seem to be a reasonable thing to do.

Ms. CHRISTENSEN. Any my last question—.

Chairman COX. I am sorry, the gentlelady's time has expired, but I think we are going to have time for another round.

The gentlelady from New York.

Ms. LOWEY. Thank you, Mr. Chairman.

And thank you, Admiral Loy and Mr. Brennan.

As you heard from many of my colleagues today, and you hear from members of the public, as well as state and local law enforcement officials, there are real concerns about the vagueness of the systems warning, its lack of preparedness and response recommendations to state and local governments and the public.

In fact, even Secretary Ridge, the top official in charge of HSAS, has even expressed concerns about its credibility and conceded that it needs to be further refined. And you both were talking about it evolving.

In my judgment we need a system that issues fewer national alerts and instead crafts targeted warnings to localities or industries with specific information indicating where or what the terrorist target might be. And this is exactly the reform called for in the first responder legislation, which was approved by the committee.

As you may know, I represent a large portion of Westchester County, one of the largest counties in New York State. Within our borders we have the Indian Point nuclear plant situated among 20 million people within a 50-mile radius. We have the Croton and Kensico reservoirs which supply drinking water for 9 million residents of New York City and the lower Hudson Valley, the county airport, which houses the largest corporate fleets of planes in Westchester.

In light of the obvious threats to our region, our law enforcement officials work hard to protect these landmarks. So when the Federal threat advisory warning goes up, our local governments and local enforcement officials go into action, whether or not they have special intelligence from the Federal Government or guidance how to guard against these threats.

For example, Westchester County police department spent of $220,000 from December 21st through January 9th during the most recent heightened alert. Individual communities, smaller ones like Larchmont, spent $15,000; Ossining spent $8,000 for police officer overtime pay.

Now, on the surface—and I am right near New York City—these figures may sound small in comparison to some of the numbers that we hear. However, for towns of populations of fewer than 30,000 residents, these figures represent sizable portions of their

local budget. And they simply cannot continue to bear these additional costs without substantial help from the Federal Government.

And as one first responder from my district who testified before the committee said, "Look, we can't go to orange without first seeing green."

Now that takes me a statement you made before, and I think it is important to clarify it.

You said the $60 billion in grants, February 23rd the deadline. Well, this is the first time I have heard that, unless you are talking about grants to the states. These are not grants, as I understand it, that are going to localities.

And as my police chief, Chief Kapica in Greenburgh, said, "Look, I can't wait for the feds, for the state. I have to do what I have to do."

They need reimbursement.

So if you can tell me how much Federal funding has been allocated to reimburse localities for these costs and September 11th, I would appreciate it.

And this program that you referred to, I am assuming is money that is going to the state. Because otherwise, none of my localities have heard about it.

Admiral LOY. that is correct.

Ms. LOWEY. So it is going to the state?

Admiral LOY. Through the states, ma'am.

Ms. LOWEY. Well, I think you should know that that is not good enough. Because the localities have to be able to apply to some source of funds to reimburse—and obviously there should be appropriate review. We do not expect you to be handing out these dollars willy-nilly.

We need to get legitimate expenses reimbursed.

And so I would appreciate if you would consider that.

One of my questions is: Will the Department of Homeland Security support legislation to reimburse local jurisdictions directly?

Second, to follow up on the interoperability issue, this is one of the top priorities of the secretary. Yet there are no specific funds set aside in this bill, in fiscal year 2005, to enhance state and local interoperability.

And last year, Congress put $85 million under the COPS program for this purpose, but this administration has proposed zero, no funds, in DHS or COPS for interoperability.

I mean, I do not understand. If this is a priority, how exactly are we enhancing interoperability?

And I would dare say—what, is it six months ago, since I am still on yellow and not red—there was a hearing where the gentleman was telling us—I forgot his name—that they are going out with an RFP with interoperability, and then they are going to be issuing guidelines with interoperability.

Frankly, all our local governments are just going ahead with it.

So I would strongly recommend that there would be some kind of reimbursement programs for essential expenditures, because our local governments just cannot deal with it anymore.

I do not know if you have time to respond.

Chairman COX. Of course the witnesses may take as much time as they see fit to respond.

Ms. LOWEY. Thank you.

Admiral LOY. Thank you, sir.

The president's budget asks for I think $3.5 billion. It is important for us to take the $200 billion worth of supplemental Liberty Shield dollars and separate them from the notion of annual grants—I do not want to confuse the two.

The claims process associated with those $200 billion is of course—those are dollars against which only $60 billion worth of claims have come toward us. So there was about—I am sorry, millions.

There was this pool of leftover dollars, if you will, that was very important for us to gain as quickly as we could a sense of what the period from the 20th of December to the 9th of January was costing the first responders in the local communities.

So the call has gone out to allow that claims process to be initiated.

As it relates to annual grants, the $3.5 billion worth of grant requests that are in the president's budget is back to the discussion we had earlier, ma'am, on the adjusting nature of how best to provide those dollars in a post–9/11 security environment that is just dramatically different than times before.

And where there are areas of greater population, greater population density, greater critical infrastructure elements, like you were just describing in Westchester County, the notion that that distribution algorithm should reflect that is I think something that is—we are sort of in violent agreement at this point between the committee and the administration to how we get down to—the devil is always in the details—but the notion of it being other than just an across-the-board base-plus per-capita distribution algorithm I think is clarified by what the president is requesting and a doubling of those UAC grants for 2005.

Chairman COX. The gentlelady's time has expired.

The gentlelady from Texas, Ms. Jackson-Lee, is recognized for five minutes.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman—and a very important hearing and one I hope that I can capture for both Mr. Brennan and Admiral Loy the frustration that you have heard on occasion among members.

For the last two State of the Union addresses, we have had the president dominate his message to the American public with the idea of either war or the war on terrorism.

We are living in a state of panic, a state of fear.

This committee, I believe one of the singular committees in this Congress and in this nation to able to be a partner when what is a 170,000-person department—that is a lot of people—are trying in essence to get its act together. And I do not say it negatively. I know there are hardworking individuals there.

If I recall correctly, the president's recent State of the Union address took 35 minutes on the issue of terror. And so, when we hear—keeping in mind the line of questioning of Congressman Markey—that there was an incident at the White House, obviously there is great concern that we now find a similar incident in the Congress. And who knows where else it might occur.

You can imagine the public's view of this incident, as to where it might occur next.

So I am going to ask the chairman of this committee—because we cannot be problem solvers if we cannot be part of the factual information—that we hold a secured briefing and meeting with the appropriate officials of the Homeland Security Committee to provide us with both the knowledge of the occurrence at the White House, how the information was disseminated, who it was shared with and its ultimate—I do not want to use the term tracking, but I will use it—to the point where we are now in the United States Congress facing a similar incident.

I am going to ask that to you, Mr. Chairman, that we have such a briefing.

We have had those. And I do not even like to call it a briefing. I want it to be a meeting where we are engaging on what I perceive to me a national problem that we have to address. And I would like to have that request made. And I am putting that on the record.

I do not know, Mr. Chairman, am I allowed to yield to you? I know I would be losing my time. I want to proceed. But I would like to make that offer, Mr. Chairman.

Chairman COX. Well, I would advise the gentlelady that at 7 p.m. this evening on the House floor there is precisely such a discussion, for members only, on the ricin incident in the Dirksen Senate Office Building.

Ms. JACKSON-LEE. And Mr. Chairman, what I would offer to say to you is that I would prefer to have a separate meeting for members of the Homeland Security Committee, inasmuch as this takes a lot longer time. And as well, we are entrusted with the responsibility to secure the homeland.

So I will make that request still, recognizing there is a meeting this evening.

Let me also then continue—and I thank you, Mr. Chairman, very much—to lay that groundwork for why we are concerned with what I am hearing today.

Let me ask the question, or let me put on the record so that you also know the frustration with the reimbursement question that my colleague from New York has raised.

Cities nationwide are now spending $70 million per week. Houston, the fourth largest city in the nation, is obviously spending even more.

In a 145-city survey on either the homeland security, Iraq war on terrorism and war in Iraq, with the homeland security issues and the question of alerts coming and going, they may spend over $2 billion in the next six months.

So you did not answer the question of Ms. Lowey on the point of whether or not you are reimbursing cities now, directly, for the costs they have already expended. Can I just get a yes or no or where we are in that position?

Admiral LOY. Yes, ma'am. As I indicated, we have set a February 23rd deadline for the claims that are put together as a result of the experiences from 20 December to 9 January. And we expect to pay the bills when we get those claims and have reviewed them.

Ms. JACKSON-LEE. And those will be directly to the locality?

Admiral LOY. I do not know that to be the case, ma'am. I am not personally familiar with the process of how the claim goes in and how the claim goes back out.

My sense is of course that the difference between working with 55 entities, the states and territories, as opposed to a countless number of entities, if you were dealing with each and every city in the country—.

Ms. JACKSON-LEE. Let me stop you for a moment so I can get my other question on the record here, so you can answer it. Let me complain or raise a question of concern on the idea that it goes to the states and not directly to the localities.

I am going to research that with you. I understand that you do not have the specific information.

But let me move forward.

During the Super Bowl weekend, there was a decision for a flight leaving from London not to come into Houston. My question is whether the TTIC is involved in this kind of intelligence assessment.

If that is the case, I want to hear from Mr. Brennan whether or not he is comfortable in light of the vulnerabilities and failures of the intelligence system, as related to the Iraq war, as we are now seeing unfold.

Are you confident in the intelligence that is now moving this alert system up and down, up and down? And what is it that you are doing to vet the intelligence that is coming to ensure that even as we use the system that we are now critiquing, that you in fact have the information to make determinations that would then cause you to go to orange alert or yellow alert, which then generates this high cost that we are now expending in our local communities?

What is the basis upon which you are utilizing or collecting intelligence? And what is the basis upon which you are vetting intelligence to make sure that we have viable intelligence to make the right decisions?

Chairman COX. The gentlelady's time has expired.

But both Admiral Loy and Mr. Brennan, please take whatever time you see fit to answer the questions.

Ms. JACKSON-LEE. I thank the chairman.

Mr. BRENNAN. As you I am sure understand, there are many different types of information that come into the U.S. government regarding threat—some of high credibility, some of low credibility.

Analysts and TTIC, as well as in other organizations, constantly look at that information, evaluate it, assess it, digest it, challenge it and compare it with what we know about what terrorists are doing.

We then, as an intelligence analytic element, we interact then with those agencies that collect the information, whether it is collected from human sources or technical systems or whatever it is that they do, to make sure, then, that we provide them the feedback as far as what our questions, what our requirements are so they can then go back to do the vetting of the sources that is necessary.

But this is a constant back-and-forth process.

We get the information in, we look at it, we compare it, then we provide feedback to those organizations that are providing the information to us.

And so what we try to do is to appropriately characterize the nature of the information to the Department of Homeland Security so that they fully understand the nature of the information, any questions that we might have about it, as well as our assessment of its credibility and reliability of the sources.

So it is a cycle in terms of—a cyclical process. The information comes in. We provide it to customers. They have issues or questions about it, we have our own and we pass it back to the collectors so that they can better vet those sources.

Ms. JACKSON-LEE. Admiral Loy, you are the recipient of the information, at least the department is.

Admiral LOY. Yes, ma'am. John describes it exactly the way we watched day after day through the course of those weeks, Ms. Jackson-Lee.

And the specificity and credibility of that intel stream is always going to be the judgment we need to take when that analytic product, as a result of that give and take John just described, is then offered to the Department of Homeland Security.

Our intelligence shop will give us a good assessment of that product that they just received and then map it across the vulnerabilities that we know to be in our country, in all those economic sectors.

And then our challenge is to make a good judgment, a risk assessment, if you will, knowing this threat piece that was just provided to us, knowing the vulnerabilities that are there—what are we going to do about it and what are the tools that we have to do it, including the communications tools to tell locales, economic sectors and indicate specifically, as you alerted with your question, the aviation industry as it related to the flight in question that was heading to Houston on the even of the Super Bowl.

That flight, as I can recall, would originally have arrived in Houston around half-time. And the combination of the threat piece that we received, and our engagement process with vulnerability, as we understood them at the time, caused us to engage with that particular airline, prescribe what would have been a set of mitigating strategies that we felt were appropriate if it was to fly and leave the judgment associated with flying to the airline.

That process worked through that particular event.

And frankly, the day-after-day engagement between TTIC as the threat collector—collector in the sense that it is provided as information for them to produce a tactically actionable product, if you will, and then offer that to the customers elsewhere in the business of securing our homeland.

Ms. JACKSON-LEE. Thank you, Mr. Chairman.

I think their answers evidence the need for a security briefing of this committee. Because as you well know, if our nation's citizens continue to hear about alerts and they do not respond, they are not being secure.

So I think it is very important that we have this closed-door meeting of the Homeland Security Committee.

Thank you.

Chairman COX. The chair recognizes himself for five minutes.

Admiral Loy, Mr. Brennan, you have heard from a number of our members questions coming at you from I think both directions on the clarity or ambiguity of the threat-level message, not to law enforcement, not to Federal agencies, to governors, but rather to the general public.

And that remains a concern of mine.

I want to be absolutely clear and unambiguous in my compliments to TTIC, to the Department of Homeland Security, to the administration across the board on the progress that you are making, the very rapid changes that you are making in the way that government does business when it comes to sharing information among people in the government who can do something with it.

But I have great concerns about the adequacy of our system for dealing with the general public, because I think that the confusion that is sown is about equal with the benefit that it gained, and that tradeoff is not working as well as it might.

But let me turn now to the second part, which is actionable information in the hands of people who can act, people who are responsible because of their job descriptions for doing something with this information.

There are two main sources of responsibility for the department. We have Homeland Security Presidential Directive 3 and we have the Homeland Security Act.

HSPD–3 tells departments and each Federal agency that they are responsible for developing their own protective measures in response to each threat level.

The directive also recommends, as you pointed out in your testimony, is binding on the Federal Government, advisory as to everyone else, it recommends that governors, mayors and others develop their own protective measures for each threat level.

Then we have the Homeland Security Act, which authorizes the department to provide guidance to state and local government—to the mayors, the governors, the police chiefs, the fire chiefs, the first responders and so on—about what they should do at each threat level.

And this includes also private sector entities and the public.

It is my understanding that we are not yet at the point where we can take a look at a classified document that says, "Here are the protocols for this sector," or "Here are the protocols for this law enforcement arm when we go," for example, "from yellow to orange."

What guidance, if any, has DHS issued to Federal, state and local and private sector agencies regarding the appropriate protective measures at each level? In what form has that guidance been given? And is it sufficiently digestible that it would be sensible for the committee to review it?

Admiral Loy?

Admiral LOY. Sir, it varies across the board, if you will, in terms of sectors of the economy. The focus is associated with sectors of economy at this point in terms of being able to identify, with clarity, such that the state and local elements as well as the private sector elements, know what is expected of them, if you will, and

what they should—the encouragement process here, of course, is to identify the kinds of things that they should expect of themselves.

And I go back to Mr. Turner's I think absolutely right-on commentary about all of us rising to the occasion in this very different security environment that we are all part of today.

So, for example, with respect to aviation security—one that I just happen to know a good about, based on what I have been doing for the last two years—there are very specific all the way down to encouraged additional patrols to be foot patrols, not in uniform, around the airport terminal building, looking for the briefcase that is left unattended.

It has to do with the parking lots and how we are actually going to be dealing.

It has to do with threat reduction plans associated with potential bombings, given that vehicle bombs remain one of the most dramatic potential sources of problem.

So in the case of the aviation piece of the transportation sector, enormously specific guidance has been provided—actually, I would call it worked through with the airport directors and with the airlines themselves.

It has to do with identify authentication of people in those airports.

It has to do with access control of how we deal with elements in those airports.

There are probably less robust but aggressive and growing interchanges with the rail industry, with the transit industry, with other elements in the transportation sector.

that is just one of this puzzle of sectors the secretary's responsible for across the board.

We have established ISACs, as they are called, information sharing and analysis centers, associated with each of the major economic sectors in the nation. The ability to exchange and hear from them so they are part of the design work of that set of things we would be expecting of them or ask of them at different threat condition levels, that process of engagement is robust as we speak at the moment and about to almost explode, sir, as we are moving with respect to this critical infrastructure national game plan that is going to be built.

Chairman COX. So I do not want to use up any more of my time in asking new questions, but just to re-ask the question that I already put, is the information in digestible form for this committee?

Admiral LOY. There is absolutely a lot of it, sir, that we would be delighted to share and help you understand where we are trying to go and where we are with respect to—.

Chairman COX. I say that because I think every member on the committee has had the same experience of a police chief in my hometown of Newport Beach, California. What is the Newport Beach police chief supposed to do? What should his department do differently when the threat level rises? Or is it up to him? After a fashion, HSPD–3 leaves it up to everybody to come up with their own.

Admiral LOY. To a degree there is a strong encouragement process and then there is absolutely an appropriate "let the mayor define what is going to happen in his town, let the governor define

what is going to happen in his state, let the police chief be part of the process of defining what is going to happen in his responsibility area."

Yes, sir?

Chairman COX. The gentleman from Texas is recognized for five minutes.

Mr. TURNER. Admiral Loy, that reality that every mayor and every governor and every CEO of a corporation is complying with your alert level voluntarily—there are no requirements of law to do so—is the very reason I think it is so critical that we move forward to a more sophisticated system.

Because I heard an emergency manager at the U.S. conference of mayor's meeting just a couple weeks ago that I was a part of. He was from Arizona. He reminded everybody around the table at this meeting of the mayors and emergency managers that they did not have to comply with what the Federal Government was saying, that was theirs.

And some of them were somewhat shocked. They kind of thought, well, maybe they were supposed to do this.

And he reminded them, "No, this is voluntary." And he said many times he has not complied when the alert level has gone up in recent times.

So I think there is beginning to be an erosion of confidence in the system.

You mentioned many times the importance of looking at threats and matching them against the vulnerabilities. And that is what the task is all about, as you go through analyzing these threats.

And yet, a few weeks ago, I read in some publication that Assistant Secretary Liscouski said that it would be five years before the department would complete the congressional-mandated national comprehensive threat and vulnerability assessment.

So it struck me that that time line is totally unacceptable. And so I would ask you: What do we need to do in the Congress and what do you need to do to be able to shorten that time frame to accomplish that very critical assessment?

Admiral LOY. I could not agree with you more, sir. That is unacceptable.

Someone was suggesting to me just the other day that the notion of standard-setting for interoperable communications was something that might be at 18 or 24 months out. And I had to help them understand that is totally unacceptable. It should have been maybe done by now.

But there are challenges associated with this, sir, that are enormously difficult. I do not think there is plenty of "authority" in the Homeland Security Act and HSPD–3 to enable the secretary and I and others to get on with the business of these enormously important things that you described.

On the other hand, Congress has acted in addition to the Homeland Security Act in many ways. If you think, for example, of the MTSA, the Marine Transportation Security Act, an augmenting piece of legislation where the Congress felt for whatever correct set of reasons, probably that either we were not moving fast enough or the nature of the maritime transportation system deserved guidance in the form of legislation.

And in the president's budget today you will see a $100 million worth of requests from the Coast Guard to get on with the implementation of the ingredients of the Maritime Transportation Security Act that the Congress passed last year.

I would offer in this greater sense, there is almost a repeatable series of things that must occur with respect to each of these sectors. There must be a standard-setting process.

There must be a vulnerability assessment process. There must be an identification of mitigating strategies. And there must be, then, an action plan that comes out as a result of that sequence of events with accountability at the bottom end of it as the most appropriate and final loop for us all to close.

Mr. TURNER. You know, that description you just made there, what needs to be done, it would be very helpful if you could lay that out in a letter to the committee as to what the process is so we can have a better understanding.

And if you could, also let us know what we can do to help move it along. Because I think we have got to come to grips with the fact that five years is not acceptable.

There is another issue that I wanted to lay on the table before my time expires for you to respond to. And that is it is not only the collection of intelligence and the analysis of it and matching against vulnerabilities, but it is then turning around and providing information back to those who have a need to know.

And a few weeks, maybe it has been a couple of months ago or longer now, the department made an announcement that we are going to change the policy regarding information sharing. And the governors were able to designate, I believe it was three people, within their office that could receive classified information.

Now, the Gilmore Commission made some recommendations on this. And I think it is incumbent upon the department to take a look at this. And I think that we are all of like mind here, that if this information is going to mean anything, we have to be able to share it with people that can use it. Otherwise, you are in the same position that I am in when I get a briefing, and that is I cannot tell anybody this classified information or I violate the law.

And so, since I am not a first responder, since I am not out there on the front line anywhere, then it is good for educational purposes in terms of congressional oversight, but it is not making the country a lot safer in the short term.

And the Gilmore Commission said this: "We should designate one or more security-clearance-granting authorities which can grant security clearances Federal Government-wide." In other words, we need some entity that can grant security clearances that will be recognized by all Federal agencies.

We also need to, I think, extend that to local and state governments. They said we need to develop a new regime of clearances and classification for dissemination of intelligence and other information to state and local governments and the private sector, and develop a training program for state, local and private sector officials for interpreting intelligence products. Obviously not only for interpreting but for understanding what the classification system means and what you can and cannot do with that information.

But to say that we are collecting all this information and we are understanding these threats and yet we are not passing this information down to those who need it, who could use it—and I am not just talking about passing it down to the folks that might be affected in a given area—because when you are relying on this color-coded system, you know the folks in Houston need to know just as much as the folks in Buffalo, because if the threat relates to Buffalo, they then know it does not relate to them.

But we have to get to the point where we broaden the number of people who we have enough trust and confidence in, and there is a lot of patriotic Americans out there working real hard on front lines that I would trust—.

Admiral LOY. Yes, sir.

Mr. TURNER. —that we can share this classified information with and get them in a position where what we are collecting would actually be meaningful in the event that the worst occurred.

Admiral LOY. Sir, let me take a crack at it, if I may sir. And John probably has some thoughtful cautions along the way with respect to sources and methods and things that he is far, far, better to answer than I.

First of all, we may be able to take a lesson from, again, the aviation book, sir.

Well before 9/11, there was a category of information known as SSIs, sensitive security information, that had been part and parcel of the means by which airlines and airports worked with the FAA and others in terms of concerns that had been, of course, part of that community's interest since Lockerbie and since many, many years before 9/11, the means by which we could translate—I will use that word—the classified information you are describing such that it is totally there with respect to its import at that local chief of police station or JTTF locally in the city is absolutely a goal that we should all have.

To find the way, A, to communicate it, that is the technical end of the communications channels, and also so that the receiver, that first responder set that we are expecting so much of, to be as armed as possible in terms of understanding, sort of, what they are getting into.

And I could not agree with you more that we should find and are in the midst of trying to design better ways that will approximate that SSI system that served the aviation industry reasonably well.

John?

Mr. BRENNAN. Mr. Turner, I would not disagree with the comments that you read of the Gilmore Commission, first of all.

second, I think it is critically important that there be a national enterprise business process architecture. But honestly, the technical challenge I do not find as daunting as the engineering of the business processes that need to go on in terms of bringing together the different elements of the Federal family, then bringing in state and local and local police or law enforcement officials.

That type of architecture, as far as how information should flow, who it should flow to, under what circumstances individual components should receive information, that is a tough, tough challenge as far as, again, putting together a national architecture of moving information very quickly—which can be done—but as far as who

has that responsibility in certain areas, I think this is still being worked out with the state and local officials and the Department of Homeland Security.

But what we are trying to do is to get the Federal system right as far as the terrorism intelligence feed to the departments so that they can then take it to the next level.

Admiral LOY. If I may, sir, just a closing comment on that if our answers of course have been adequate.

There is a system called JRIES, J–R–I–E–S, it is a Joint Regional Information Exchange System. I might not have all the acronym correct. But the notion there is that the technical end of being able to do the communication is a system that we need to build. that is the how to it.

Then the what to be shared and the means by which that classified matter through the JRIES can actually be exchanged between levels of government, for example, Federal, state, and local, is absolutely on point. And we are about to develop a couple prototypes to prove that it has its merit and move out on it, sir.

So we could not agree with you more. The rightness of being able to share the tactically sound and valuable information among those players that can best use it for our national interest is right on target.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Chairman COX. The gentlelady from New York is recognized for five minutes.

Ms. LOWEY. Thank you, Mr. Chairman.

And I want to thank you, Admiral Loy, and Mr. Brennan for being here today. And I want you to know that we appreciate the enormity of the task.

However, as a member of Congress—and I know I speak for my colleagues as this hearing winds down—we represent over 660,000 people. I am the mother of three, a grandmother of six. As I travel around my district, the fear is palpable. These youngsters are not growing up the way I grew up.

And they all want to know, what should we do? Should we go to the mall? Should we go to Times Square? Should we take an airplane? Should we take the train?

So I want to make it very clear that although I understand how hard everyone is working, and I know we appreciate your efforts, when you look at 170,000 people that are making policy two years after 9/11, as someone who lives 30 minutes from New York City who has family and children in New York City, I frankly think in order to earn the public's confidence we have to move more quickly.

It is just not good enough to say that we are thinking about it and we are planning it, and a year from now and five years from now—we were talking about all the nuclear plants that are not up to standards that you and I would deem adequate—we just have to move more quickly.

And it seems to me that DHS should be able to not only decide that it is orange or green or yellow, but they should be able to provide some kind of standard, some kind of information to the locals. They are not receiving it.

In fact, I guess it was at the last time—I was looking through the dates. It was awhile ago, when Secretary Ridge appeared before the committee, and he testified before the Senate Government Affairs Committee last May. He also acknowledged that the process for notifying state and local agencies of the change in the threat level needs improvement.

I wonder: Have there been improvements made? It is my understanding from that hearing that when the secretary decides to raise or lower the threat level, DHS makes a conference call to as many state and local law enforcement agencies as can be reached.

Number one, approximately how many state and local law enforcement agencies are you able to reach through this method? My people, who I meet with regularly, tell me they hear about the threat level through the media.

Is this the best method in a time when you are trying to be as efficient as you can?

I would be interested to know who is on the conference call. I mean, fire departments, for example, are so critical to increasing security protections during an increased threat level. Are they part of this effort? Or are the mayors part of this conference call—and they are supposed to alert.

I just wanted to, as we close down this hear, let you know that I know your concern. But from the perspective of most members of Congress, you hear our frustration and we just do not feel that the department is moving as efficiently and as expeditiously as it should.

And I understand the complexity. But I just hope that you get that message loud and clear.

And perhaps you could answer that one question about who is on this conference call. Do you think it is working efficiently? Should we be e-mailing or BlackBerrying everybody? What kind of information are the locals getting?

And I believe you answered—I believe it was Chairman Cox—that you are not providing specifics. With all the expertise you have, with all the various people in play, not to provide some kind of directive to the locals, and just say, we are in alert, that does not seem to be as good as we could possibly be.

Admiral LOY. Yes, ma'am. To answer your question directly, the conference calls that are cited are with the homeland security advisory players in the respective states. And it is, for lack of a better analogy, it is a phone tree, if you will. And we count on those state officials to advise their local constituents as appropriate to what it is that has been passed to them.

Now, in addition to that, depending on what we are actually seeing in the stream. For example, in the holiday period, we were on the phone several times a day to Ray Kelly and his team; we were on the phone to Mayor Hahn and his team several times a day; we were on the phone to Las Vegas and their team several times a day to update them on whatever it was that the twice-daily sessions associated with TTIC re-analysis of the threat stream was helping us understand.

We made executive visits. We comprised teams from the Department of Homeland Security that went and visited Los Angeles and Las Vegas and New York and Washington, D.C., because that is

where the threat stream was telling us in this particular period these folks deserved a more wholesome review of the information that we have so they can understand what it is that is being asked of them.

Now, can we make, you know, 30,000 executive visits in a 10-minute period, when we are trying to "pass the word"?

There are technical and substantive values to both the technology that you are describing to help us do that better—whether JRIES is the answer, we will know very quickly and we will be able to do that or whether the holding on to the blunt instrument nature of HSAS in its color-coded fashion that we have it today may continue to have value there, when each of them who sees it occur understands what that translates to them—and then of course the follow-up that we would have with anyone that we would be getting more specific information for.

Ms. LOWEY. Just let me thank you very much and thank the chairman.

And I just want you to know we feel as if we are all on the same team, Democrat and Republican, and whatever we can do legislatively or in any way cooperate, we recognize the urgency of this issue, and we applaud you for taking the responsibility.

Admiral LOY. Thank you, Ms. Lowey.

Ms. LOWEY. Thank you.

Chairman COX. The gentlelady's time has expired.

The gentlelady from Texas, Ms. Jackson-Lee, is recognized for five minutes.

Ms. JACKSON-LEE. Thank you, Mr. Chairman, very much.

And gentlemen, let me do as I did earlier and give you a few pearls of thought, if you will. And then, if you would comment.

But allow me a moment of personal privilege to add my appreciation and applause for the law enforcement that included Department of Homeland Security, United States Customs and TSA, and my own Houston police department, and various country and other local law entities for this past weekend. I believe they did an excellent job in Houston with the Super Bowl. Massive number of people, massive number of potential activities that could have occurred, good and bad.

I think most of the good did occur and none of the bad. And so I want to acknowledge that and express the appreciation for the service that was rendered.

Chairman COX. If the gentlelady would yield, I think the question was put earlier, you know, what should people do differently when we are at this heightened state of alert, and I think the example was given during half-time of the Super Bowl. People should not do that.

Admiral LOY. Thank you, Mr. Chairman. I could not agree more.

Ms. JACKSON-LEE. Being a supporter of the First Amendment, and I appreciate and yield to the chairman on his views, I will just associate myself with the views that Houston did a great job. And of course the law enforcement did a very good job.

Chairman COX. Of course I agree with the gentlelady, and I thought it was a great game as well. And Houston did a wonderful job of hosting the Super Bowl.

Ms. JACKSON-LEE. Thank you very much.

A lot of interesting things occurred. We could have been a little better on the streaker that was on the field that no one was able to capture.

But let me proceed and be on the same theme, if you will, of the frustration is not with the hard work that you are obviously engaged in, it is that we want our fellow Americans, our nation, to be safe.

So let me ask some pointed questions.

I have held a number of meetings on terrorism in the Houston area—one, I want to thank the ranking member, who was present, and we look forward to the chairman being present—a very good meeting in the summer that we visited a lot of sites and heard from at least 50 or 60 witnesses on this question.

Subsequently I held another meeting toward the end of this last year, December 31st. And one of the questions asked was that monies seemingly had not been distributed to local entities that were promised since 2001.

That may require you to go back to your drawing boards.

And, again, this city is Houston, Texas. But this is my law enforcement that truly, I would say, is victimized or impacted by the fact that it seems that monies go to the states and not to the local entities. So I would like to have that information.

And then, to follow up, as to whether or not this application process for the 23rd will—and you were going to look into it because you were not sure—go directly to cities, or whether or not it will go to state entities. That is a definitive and a real problem for us.

In addition, one of the issues were that local communities need more hospital beds and medical equipment in time of tragedy. And how does the Homeland Security Department interface with them on that basis?

Let me cite for you out of the U.S. Conference of Mayors another point—I made one earlier: Cities have received little direct Federal assistance for homeland security since the attack on September 11th. The president's proposed an additional $1.4 billion in aid for local governments, recommending that all but $50 million of that funding be channeled first through state bureaucracies.

I think it is key that the Homeland Security Department be engaged with the administration—you are part of it—but with the White House on this fallacy, where monies are not coming directly to local facilities or local entities, because they are, in fact, spending the money.

I appreciate the states' role, but it is the Federal Government that the local communities look to. Those monies then are stopped, if you will, estopped, midway, and it is a long, long time before they get there.

And I think that is unfortunate.

I do not know where I am going to come down as it relates to alerts, orange, yellow and other colors. But I will say to you that I think it is imperative that we engage and not be afraid of each other. It appears that we are afraid of each other—it is the administration, it is the Congress. Because what is happening is that individuals are becoming less engaged when they hear the alert system.

that is the only criticism. that is what we are saying to you. Less engaged. While cities are either spending money or forgetting about it.

The Red Cross at one of my meetings suggested maybe in the alternative that you offer a plan, review your personal disaster plan, ensure you have supplies, develop alternative routes to and from work, exercise caution when traveling, have shelter in place, localities for you.

One of my big issues with respect to the schools, we need to think about them. And if you could comment on that.

Let me finish, however, by making this point: Citizen Corps, which is a very, very good promise and proposal, that is supposed to be organizing our citizen groups in our respective communities. Not many citizens are aware of Citizen Corps. They come in; they take up the larger entity, which is the county in my instance. They may be doing a great job. I want to compliment them. But neighborhoods do not know anything about it.

Citizen Corps needs to be diversified. It needs to be smaller. It needs to go into neighborhoods. And it needs to be funded.

Mr. Chairman, I see the gavel. I will say one last sentence. And that is: You might answer me on whether or not you have been able—if good intelligence is important, have you been able to diversify your analysts? Are you pulling from diverse populations? Do you have Arabic speakers? Do you have African-Americans? Do you have Hispanics? Do you have Asians?

That has been a key concern of many of my colleagues. And I might just add, Congressman Donna Christian–Christensen, who had to leave, we are very concerned about that issue.

Chairman COX. The gentlelady's time has expired.

Ms. JACKSON-LEE. I thank the distinguished chairman.

If you would answer the series of questions. I hope you were gathering notes. I was, so I hope you will be able to answer some of them.

Admiral LOY. I will try several, ma'am. And then John perhaps has more insight on the last one.

First of all, Citizen Corps, I think the public affairs dimension of that is enormously important. And we do need to be as understanding as we can with what the potential is there for its purpose. And its purpose is to basically enhance individual citizen preparedness.

Ms. JACKSON-LEE. Right.

Admiral LOY. And the flow of the dollars through that particular process, in terms of community emergency response teams, and their ability to be adequately resources, so as to be able to do what they are supposed to do when they are supposed to do it, I think Citizen Corps is a great program. I think the president has asked for $50 million for the program for this upcoming year?

Ms. JACKSON-LEE. We may want to talk. That is not happening. I will just say on that point.

Admiral LOY. Yes, ma'am, OK.

As it relates to the flow of monies, first of all, I think it is enormously important as we look at the absolute dollar amounts asked for in grants this year to have some context to this over the course of a couple of years.

Over the window of 1999 to 2001, I think there was a $1.3 billion total to the grants to be administered in that fashion; 2002 to 2004, not counting the $3.5 billion the president is asking for this upcoming year, $13 billion, a 900 percent increase in those two windows of time.

So the context in which we think our way through numbers, in terms of their absolute value and potential value to preparedness in the nation, is very important.

And lastly, I could not agree with you more that we must have an efficient system for the distribution of those dollars. I am a new arrival to the department. I will guarantee you I will take on the challenge of looking very carefully at the efficiency of the system as you were describing your frustration in terms of the Federal through states on the way to the locals. I do not see any reason why that should not be as it is called for, as I understand, something like an 80 to 85 percent pass-through, on to the cities and counties of our respective states.

I will take a round turn on that, ma'am, and look forward to working with you on it.

Ms. JACKSON-LEE. I look forward to that.

Mr. Brennan?

Thank you, Admiral.

Mr. BRENNAN. Ms. Jackson-Lee, the Terrorist Threat Integration Center takes that word in its title, "integration," very seriously. From the standpoint of that, we recognize how much of a force multiplier the integration of those different perspectives and agencies within the U.S. government can bring to the fight against terrorism.

There is a rich diversity there. We are fortunate I think right now to have within the TTIC population African–Americans, Hispanics, Asians, Arabic speakers and others.

Since we are not an independent agency or department, we do not have direct hiring authority. So we receive the analysts who are sent to us from those departments and agencies. And one of the things that we are going to be looking at is ensuring that we have within the TTIC population that type of richness and diversity, not just in terms of departmental representation, but also in terms of the richness and diversity of America.

Ms. JACKSON-LEE. I look forward to working with you further on that, and also tracking how those individuals are shared with you and what opportunities you will have to have your own impact on that diversity as well. I think it is key for good intelligence.

Mr. BRENNAN. I look forward to it. Thank you.

Ms. JACKSON-LEE. Thank you, Mr. Chairman.

Chairman COX. I thank the gentlelady.

Before we proceed, I have an announcement I would like to make. Today is the last day for our senior counsel, Mike Jeffroy, whom many of you know, who has ably served this committee. He is here on his last day for a while at least, because he is going to be leaving for six months. He has been called up by the United States Marines to go to Iraq.

And I want to wish him Godspeed and to thank you both for the outstanding work you have done in making America safer, working here in Washington in the Congress, and for what you are em-

barked upon to make Iraq and the world a safer place as a United States Marine. Thank you very much.

[Applause.]

I want to thank our witnesses. You have been very patient through 2.5 hours, nearly three hours of hearing here. We have covered a lot of ground. I think we have made a lot of progress in informing the Congress. And hopefully you have learned something from our questions.

There is, as you know, in progress a GAO analysis of the color-code threat warning system. The GAO has briefed both the Democratic and Republican staff. I believe it is GAO's habit to work with the department while they are preparing these reports, and I take it that you have heard from them in the process of this.

But I would just note that much of what you have heard from the members here has also been echoed in the interim report from GAO on this subject, specifically that Federal, state and local agencies wish for much more detailed information and advance information, separate from the color-code warnings.

Some 85 percent of GAO customers said that they got this information first from television, the same way, in other words, that Al-Qa'ida or Osama bin Laden's getting it, when it is made public to the world.

Second, GAO pointed out that nobody is doing a good job—nobody meaning not the Federal Government, state government, or local government—of tracking the costs associated with this system.

Perforce, we do not have a way in the Federal Government of measuring this system's effectiveness. Simply put, are the costs worth it? We do not know, because we do not know what it costs. There is no accounting system that is agreed upon by anyone.

Some people are keeping careful track of their costs, but others are using different methods completely. And there is not any common denominator.

I think as we go forward, we have to have some system of measurement, and that, thus far, is lacking.

Lastly, GAO reports that Federal, state and local government agency officials indicated that they would like to receive more information and intelligence on a regional, state and infrastructure sectoral basis . That is something, of course, that you have heard from this committee before.

So we hope that you take these suggestions to heart. And we look forward to working with all of you.

I would yield to the gentleman from Texas, if you have any closing comments.

Mr. TURNER. Mr. Chairman, I think it has been a productive hearing. And I join you in thanking our two distinguished witnesses, great patriots who are working hard to be sure this country is safe.

And we appreciate what you do and those who work with you.

I have often had the opportunity to be impressed with the quality of people that we have serving this country. And you two here today are fine examples of that. So thank you very much.

Chairman COX. That is a fine comment. One I wish to join in. I want to thank you, Admiral Loy, Mr. Brennan, for your service

to our country. And in addition, for your very close cooperation and work with this committee and with the Congress. We look forward to continuing that relationship.

This hearing is adjourned.

[Whereupon, at 3:29 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

QUESTIONS AND RESPONSES FOR THE RECORD SUBMITTED BY DEPUTY SECRETARY JAMES LOY

QUESTIONS FROM CONGRESSWOMAN LORETTA SANCHEZ

Question: **1. Since the inception of the Homeland Security Advisory System, the threat level has been raised to Orange 5 times. Thankfully, no attacks occurred at these five times. Do you have evidence that the increased threat level prevented attacks, or did the attacks simply not happen—in other words, were these false alarms?**

Answer: The protective measures and alerted posture the Homeland Security Advisory System elicits and the incredible work done by all members of the Department of Homeland Security and other Federal, State, local, tribal, major city, and private sector partners serve as a deterrent to terrorists and terrorist actions. Based both upon the scope of measures implemented and on the intelligence we have received, we believe that the current system is effective and that attacks against the homeland have been prevented. With each new threat and with the lessons learned from unfortunate international incidences, DHS is learning about how it can continue to secure the homeland and to provide a significant deterrent.

a. Is this a sign of the limitation of our intelligence capabilities?

Answer: The Information Analysis and Infrastructure Protection (IAIP) Directorate and specifically the Office of Information Analysis (IA) believes it has the capabilities to adequately analyze all intelligence information, compare threat information, and issue timely warning products to state, local, tribal, major city, and private sector officials.

b. I know this is an unclassified setting, but can you tell us about any activity that DHS or other law enforcement agency thwarted that coincided with the Orange alert?

Answer: The answer to this question is classified. he Department is willing to provide the answer by way of a secure brief or some other means acceptable to the Committee.

c. Can you tell us generally what you perceived as the threat that made you decide to increase the threat level to Orange?

Answer: In each case of the five times the threat level has been raised to Orange, Department of Homeland Security (DHS) officials, and specifically the Secretary of DHS, felt that the particular combinations, in each case different, of the credibility of the threat information, the degree to which information was corroborated, the specificity and imminence of the threat, and the gravity of potential consequences of an event were high enough to warrant alerting the Nation.

d. The second time the threat was raised was just after the attacks in Bali and Kenya. The fourth time the threat was raised was just after attacks in Saudi Arabia and Morocco. What advanced intelligence did we have about these attacks? Did These attacks correspond to increased levels of chatter? If so, why wasn't the threat level elevated before these attacks?

Answer: Beginning in the Fall of 2002, a body of intelligence originating from overseas suggested that Al-Qa'ida operatives were planning multiple operations against U.S. or Western interests. Although the Homeland was never directly or overtly mentioned in those reports, the possibility of an attack on US soil could not be dismissed. That particular body of reporting developed over a six-to-nine-month time frame in the period between the Bali and Kenya attacks in the Fall of 2002, and the May 2003 attacks in Morocco and Saudi Arabia. By the May 2003 timeframe, this body of reporting, combined with the Morocco and Saudi Arabia attacks, raised

the potential that an operation in the Homeland was near or close to execution, which led to the decision to raise the Homeland Security Advisory System level.

e. Has anyone been apprehended as being part of a terrorist plot in relation to previous Orange alerts?

Answer: The answer to this question is classified. he Department is willing to provide the answer by way of a secure brief or some other means acceptable to the Committee.

2. A U.S. Conference of Mayors survey conducted last year reports that, because of the war with Iraq and repeated elevations to high alert, cities were spending up to $70 million per week on extra security measures. Los Angeles alone was spending about $2.5 million a week. Clearly our First Responder community is taking the threat alert system seriously, even though it is far from clear what they should be doing.

In the First Responder bill that recently passed our Emergency Preparedness Subcommittee, and will go through the full Committee soon, we have included a provision which would allow for Federal Funds to support States and localities in covering the added costs associated with these changes in threat level. **Would you support such a provision?**

Answer: We do not support such a provision. We have already significantly increased the funding to local communities to improve their capacity to respond to heightened threat levels. In FY 2004, programs such as the State Homeland Security Grant Program ($2.2 billion) and the Urban Area Security Initiative Program ($727 million) both help local governments meet the preparedness costs associated with increased threat levels. In addition to the funds provided in FY 2004 through SHSGP and UASI, the Department has provided additional significant support to our Nation's emergency prevention and response community, including more than $2 billion under SHSGP in FY 2003 and nearly $800 million under UASI in FY 2003. Similarly, in FY 2002, State and local agencies received more than $315 million to support a wide array of activities to enhance our Nation's preparedness through ODP's State Domestic Preparedness Program.

We have also created a Homeland Security Funding Task Force to help streamline the grant process and enable local governments to quickly receive the funding necessary to prepare for future threats. We think these measures—in addition to the over $8 billion that has been allocated and awarded for First Responders since March of 2003—go most of the way to helping defray the costs associated with increased threat levels. When we change the general threat level, state and local officials have a responsibility to decide how to address and resource the protective measures they implement. For the threat advisory system to be effective, it must be driven by actionable intelligence and public safety rather than the fiscal consequence of a particular advisory.

Question **3. What new systems are you putting in place to make sure state and local first responders hear about and can react to changes in the alert system before the general public hears about the changes from their local news? Do you find this to be an important aspect of the threat alert system?**

Answer: We recently announced the expansion of the Homeland Security Information Network (HSIN). This system has been gaining ever expanding acceptance within the communities of users which are stakeholders in the DHS mission. This system, tested and now in use in the Homeland Security Operations Center, provides real-time connectivity between DHS and local communities in all 50 states and 50 major urban areas. This system already facilitates critical information sharing between federal and local governments, thereby strengthening our homeland security. This system is the most cost effective way to bring information and critical tools to first responders and decision makers at all levels of government. In addition, DHS in conjunction with DOJ is exploring all available avenues to make HSIN, RISS, and LEO more compatible to enhance information sharing across the Federal enterprise and with State and Local, Tribal, and private sector security providers. Within the next 60 days, the DHS and DOJ systems at the SBU level will allow cross posting of information, by later this year, we will have agreed upon a plan which will make these systems more compatible, as well as a longer term plan for making the networks fully interoperable.

At the Secret level, DHS is developing and fielding HSIN-Secret (HSIN–S) which will allow for more robust delivery of critical information to the State, major city, and private sector security decision makers and providers. A significant part of making prudent decisions about the level of response at the local and state level will be significantly enhanced by the ability to share at this level. In addition, HSIN–S will become the secret information and intelligence sharing backbone for

the Federal government organizations which are not part of DoD. The network will interface with the DoD SIPRNET to assure robust sharing and exchange capabilities to deal with threats and incidents—whether natural or man made.

In the near future, this system will be accessible to select private sector critical infrastructure owners and operators as well as government officials. Users will have the ability to receive important threat information prior to the general release, providing the opportunity to prepare for, and possibly forestall, any potential terrorist activity. We recognize that information sharing is an important component to the success of the Homeland Security Advisory System (HSAS) especially as nearly 85 percent of the nation's critical infrastructure is owned and operated by the private sector. HSIN will provide operators the necessary lead time to take protective measures on a real time basis—independent of a change in the threat level—as necessary to ensure the safety of their facilities.

Questions**4. A vague, color-coded terror threat advisory system has the potential to needlessly scare Americans living in relatively safe towns and cities, OR desensitize Americans to the real terrorist threats. Have you considered replacing the current broad terror threat advisory system with one that is more specific?**

Answer: The Homeland Security Advisory System (HSAS) has evolved throughout the history of DHS and currently includes the flexibility to assign threat levels for the entire nation, or a particular geographic area or infrastructure sector, depending on the credibility and specificity of available threat information. The HSAS is a collaborative process which takes into account current threat information and incorporates the perspectives of other federal entities (both within and outside of DHS); state, local, and tribal partners; and private sector stakeholders.

The elevation of the HSAS level to ORANGE for the financial services sector in New York, northern New Jersey, and Washington, DC in August of 2004 demonstrates how the HSAS has matured and is an example of its flexibility to adapt to available threat information. This flexibility allows DHS, local communities, and others to target resources appropriately and reduce resultant costs where possible.

DHS learns new lessons and continues to improve the system each time HSAS level changes are considered.

QUESTIONS FROM THE MINORITY STAFF

Question: **1. The President included $10 million in the FY 2005 budget request for the Homeland Security Advisory System (HSAS). What specifically will these funds be used for? Are there personnel costs associated with this request? Are there technology costs? Will the funds be expended in a way that speeds notification and allows for more targeted warnings? If not, why not? If so, what specific steps will be implemented? What is the projected budget for the HSAS in the coming years?**

Answer: There is no specific $10 million line for the Homeland Security Advisory System (HSAS) in the FY 2005 budget request. It is important to understand that HSAS represents and encompasses the day-to-day work of the Information Analysis and Infrastructure Protection Directorate (IAIP) and the Department of Homeland Security: constantly monitoring the threat picture, mapping specific threat information against the nation's critical infrastructure, assessing preventive and protective measures already in place, issuing timely and actionable bulletins and advisories, and when necessary, recommending change in HSAS level to the Secretary. HSAS currently has the flexibility to allow us to, if the information is specific enough to support it, tailor an advisory or other activity to a specific area or critical infrastructure sector. Because level of activity and resources involved in administering the HSAS is dependent upon the daily situation in the homeland, it is very difficult to tie specific resources and requirements directly to its operation.

Question: **2. What steps are being taken to ensure that information in the HSAS, especially recommendations for responsive action, reaches State and local first responders?**

Answer: We are implementing the Homeland Security Information Network (HSIN) of which the Joint Regional Information Exchange Systems (JRIES) is a part, to establish real-time connectivity between DHS and federal, state, and local governments. Eventually HSIN will link DHS to select owners/operators of private critical infrastructure. When fully developed, HSIN will substantially increase the nation's capacity to prevent a potential terrorist attack or effectively respond to one.

Question: **3. Is the Department of Homeland Security (DHS) developing a plan to differentiate its warnings to targeted American communities as in-**

dicated by threat intelligence? How many times has a targeted, as opposed to a nationwide, alert system been used?

Answer: The elevation of the HSAS level to ORANGE for the financial services sector in New York, northern New Jersey, and Washington, DC in August of 2004 demonstrated how the HSAS has matured and is an example of its flexibility to adapt to available threat information. This August 2004 elevation of the HSAS level was the first targeted HSAS level change.

As the HSAS has evolved, it has come to reflect the need for certain localities and/or specific areas of industry to be given the various threat related issues. As such, DHS has become adept at providing information to states and infrastructure sectors through Homeland Security Information Bulletins and Advisories. Additionally, Department officials speak personally with State, Local, and private sector partners when the need arises. This personal communication, along with the flexibility in the system to allow DHS to communicate broad, generic threats to the Nation and specific threats to a locale, embody the enhancements that have been needed this far. Additionally, DHS communicates with the officials described above through regular conference calls and through calls made to specific locales and sectors as the threat requires. Lastly, during specific events and periods of high alert, DHS sends officials to areas and events of concern.

With each raising and lowering of the Homeland Security Advisory System (HSAS), the Department of Homeland Security learns new lessons and improves its notification process.

Question: **4. Admiral Loy, your testimony included reference to information bulletins, threat advisories, conference calls, and executive visits as means used to convey threat information without changing the threat level. Please provide additional information to the Committee on the use of these additional tools, including the number, types, and recipients of such past communications.**

Answer: Information sharing is one of the critical mission areas that the Department of Homeland Security (DHS) has set as a priority for better preparing the homeland. The DHS Office of Information Analysis (IA) prepares warning products, in conjunction with the other DHS entities, and distributes them to state, local, tribal, and major city officials through the Office of State and Local Government Coordination (SLGC). These products, which include both Homeland Security Advisories and Homeland Security Information Bulletins, allow DHS officials to communicate threats and suggested protective measures to regions and/or sectors of concern, without changing the threat level. Additionally, unclassified information is shared through a daily Homeland Security Operations Morning Bulletin and the weekly joint DHS–FBI Intelligence Bulletin. SLGC also coordinates bi-weekly conference calls with all of the Homeland Security Advisors in all the states and territories to help relay important departmental information as well as respond to queries from advisors. The Department has also paid for and established secure communication channels to all of our state and territorial governors and their state emergency operations centers. This investment in communication equipment included secure VTC equipment along with Stu/Ste telephones. Additionally, DHS has worked to ensure every governor has been cleared to receive classified information and are working with the Governors and their Homeland Security Advisors to provide security clearances for five additional people who support the Governors? Homeland Security mission. This provides DHS an avenue for disseminating classified information directly to the location that needs the information.

Question: **5. What steps has DHS taken, and what additional steps are planned, if any, to link the HSAS to other existing alert systems, for example the Emergency Alert System?**

Answer: DHS is working with the Department of Commerce's (DOC) Oceans and Atmosphere Undersecretary to provide in the near future the dissemination of emergency messages via the National Oceanic and Atmospheric Administration's (NOAA) Weather Radio System. (Messages sent out on NOAA's Weather Radio System can also be disseminated via DHS/FEMA's Emergency Alert System—EAS). The Memorandum of Agreement, signed on 6/17/04, provides for enhanced DHS capability to provide warnings, advisories, and other vital information to the general public in a manner that allows for reaching the maximum population with minimum delay. Of note, messages can be targeted to the whole Nation, specific regions, and even to the urban area level.

DHS is also in the process of studying all alert and warning systems to seek other opportunities for linking the HSAS.

Question: **6. The Gilmore Commission states that by providing real-time, useful guidance to federal, state and local government, an improved home-**

land security strategy can help create a "new normalcy" that acknowledges that the threat of terrorism will not disappear, but still preserves and strengthens civil liberties. The country has been under the "Yellow" alert level for most of the time that the Homeland Security Advisory System has been in effect. Should we regard "Yellow" as normal?

Answer: While the Department of Homeland Security (DHS) has kept the Homeland Security Advisory System (HSAS) at "elevated" for a number of months, the "Yellow" alert level should not be viewed as normal. No matter how long it is employed, a "Yellow" alert level is still indicative of a significant risk of terrorist attack. The fact that the risk has remained elevated for an extended period of time should not preclude the country from going about business as usual; however being always mindful that increased vigilance for activity deemed out of the norm should be made aware to appropriate Federal, State and Local entities. "Yellow" indicates to our state, local, tribal, major city, and private sector partners that, given threat information communicated through Homeland Security Advisories and Information Bulletins, they should increase surveillance and security of areas of concern, coordinate emergency plans as appropriate, take into account suggested protective measures, and implement suitable contingency and response plans.

Question: **7. Among the four criteria laid out in Homeland Security Presidential Directive-3 that underlies changing threat conditions (credibility of threat information, degree to which information is corroborated, specificity and imminence of threat, gravity of potential consequences), which factors weigh more heavily in the decision-making process? Or is each given equal weight?**

Answer: Department of Homeland Security (DHS) officials rely on judgment and experience to evaluate intelligence information received from the Intelligence Community, state, local, tribal, major city, and private sector officials, and DHS component entities. In any given situation, the credibility of threat information, the degree to which information is corroborated, the specificity and imminence of the threat, and the gravity of potential consequences can change. As such, DHS authorities, and ultimately the Secretary of DHS, weigh these factors against each other and determine the overall danger to the Nation.

Question: **8. When local governments and entities undertake additional security measures in response to raised threat levels, substantial costs are incurred. The Congress provided $200 million for critical infrastructure protection in the FY 2003n Supplemental Appropriation to help reimburse State and local governments and first responders for additional costs incurred under heightened alert, but a significant amount of these funds have gone unspent.**

A. Considering the statements of need from State and local officials, why do you believe more of the available funds have not been requested?

Answer: The Office for Domestic Preparedness (ODP) has received state reported obligations of approximately $108 million dollars against the $200 million provided through the FY 2003 Supplemental appropriation. This number represents the amount of funding, reported by the states, as firm obligations at either the state or local level. States were required to provide at least 50% of the Critical Infrastructure Protection funds to local communities. Our initial information from some states indicated that they were holding a small portion of funding "in reserve" for future alerts. However, ODP program guidance stipulated that states must obligate all funding within 45 days of grant award. As such, states and locals then began to re-direct those funds towards other authorized program costs. ODP's Information Bulletin #84, provided additional categories in which funds may be expended, such as equipment for target hardening, critical infrastructure site assessments, and protective security exercises and training. These numbers do not reflect the drawdown activity against these funds, and states reimburses themselves and their local jurisdictions on different schedules.

B. As additional security steps taken under periods of heightened threat fall clearly within the federal government's responsibility to "provide for the common defense," do you agree that it should be the federal government's responsibility to reimburse State and local governments for additional security costs incurred at times of heightened threat?

Answer: Homeland security is a shared responsibility between Federal, State, territorial, tribal and local units of government. The Federal government's primary role, including that of the Department of Homeland Security, is to assist States in preventing, preparing for, responding to and recovering from acts of terrorism outside

of their traditional incident management responsibilities. The Homeland Security Alert System was created as an information-sharing tool, not a rationale for additional Federal funds. DHS does not reimburse Federal agencies for additional security costs they might incur during heightened alerts.

The Department, through SLGCP, has provided States and localities more than $8.2 billion since March 2003. This support ranges from assistance to purchase specialized equipment needed to prevent and respond to a WMD event to training and exercise support. States and localities should be responsible to budget appropriate funds for their traditional homeland security missions, while receiving additional and supplemental support from DHS and ODP. Funds provided through DHS and ODP are meant to supplement, but not supplant State and local funds.