AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

INFORMATION SHARING AFTER SEPTEMBER 11: PERSPECTIVES ON THE FUTURE

HEARING

BEFORE THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 24, 2004

Serial No. 108–52

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

24–603 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
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
JOE BARTON, Texas
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
BEN CHANDLER, Kentucky

JOHN GANNON, *Chief of Staff*
STEPHEN DEVINE, *Deputy Staff Director and General Counsel*
THOMAS DILENGE, *Chief Counsel and Policy Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MARK T. MAGEE, *Democrat Deputy 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 4
The Honorable Sherwood Boehlert, a Representative in Congress From the State of New York 19
The Honorable Norman D. Dicks, a Representative in Congress From the State of Washington 28
The Honorable Jennifer Dunn, a Representative in Congress From the State of Washington 6
The Honorable Jim Gibbons, a Representative in Congress From the State of Nevada 39
The Honorable James R. Langevin, a Representative in Congress From the State Rhode Island 42
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas:
Oral Statement 47
Prepared Statement 49
The Honorable Nita M. Lowey, a Representative in Congress From the State of New York 35
The Honorable John B. Shadegg, a Representative in Congress From the State of Arizona 44
The Honorable Curt Weldon, a Representative in Congress From the State of Pennsylvania 6

WITNESSES

The Honorable James Gilmore, Chair, Advisory Panel to Assess Domestic Response Capabilities for Terrorism, Involving Weapons of Mass Destruction, "Gilmore Comission" and President, USA Secure 8
The Honorable R. James Woolsey, Former Director, Central Intelligence Agency:
Oral Statement 10
Prepared Statement 12
Ms. Zoë Baird, President, The Markle Foundation
Oral Statement 14
Prepared Statement 16

APPENDIX

Questions from the Honorable Sheila Jackson-Lee:
Responses from the Honorable Jim Gilmore 52
Responses from the Honorable R. James Woolsey 52
Responses from Ms. Zoë Baird 51

INFORMATION SHARING AFTER SEPTEMBER 11: PERSPECTIVES ON THE FUTURE

Thursday, June 24, 2004

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

The committee met, pursuant to call, at 10:39 a.m., in Room 2322, Rayburn House Office Building, Hon. Christopher Cox [chairman of the committee] presiding.

Present: Representatives Cox, Dunn, Boehlert, Smith, Weldon, King, Shadegg, Thornberry, Gibbons, Turner, Dicks, Cardin, DeFazio, Lowey, Norton, Jackson-Lee, Christensen, Etheridge, Lucas, Langevin, and Meek.

Chairman COX. [Presiding.] The quorum being present, the Select Committee on Homeland Security will come to order. The committee is meeting today to hear testimony about the critical need to continue improvements in the area of terrorism-related information sharing.

We have a truly exceptional panel of three distinguished witnesses, today.

Governor Jim Gilmore served from 1999 until last year as chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Governor Gilmore continues his focus on these issues as president of USA Secure, a consortium of technology and infrastructure companies engaged in homeland security-related businesses. He was, of course, governor of Virginia from 1998 until 2002.

The Honorable Jim Woolsey is a former director of Central Intelligence. He has many years of perspective on intelligence community reform efforts and the complications that entails. He also has many years of experience as a senior arms control negotiator at the Conventional Armed Forces in Europe Talks, the U.S.-Soviet Strategic Arms Reduction Talks, and the Nuclear and Space Arms Talks.

Zoë Baird is president of the Markle Foundation, and has for the past several years chaired its Task Force on National Security in the Information Age. The membership of this task force was marked, in particular, by its political diversity and technological sophistication. She is also a member of the Technology and Privacy Advisory Committee that advises the Defense Department on using technology in combating terrorism. Ms. Baird was previously senior

vice president and general counsel at Aetna and held senior positions at General Electric.

Full disclosure also compels me to note that all of our witnesses are lawyers. Far more significantly, each of our witnesses knows the world of intelligence and information sharing as it really is, understands its complexities and has carefully considered where we must go from here.

On behalf of the Congress and this committee, I want to thank each of you for sharing with us your insights today. You are, in a sense, preaching to the converted, of course. The members of this committee have from the start put preventing terrorism at the top of our listed priorities. That is making information sharing one of our preeminent concerns.

The question remains: what form reform should take, and how we should accomplish it. That is, of course, precisely the question that will animate the 9/11 commission as it completes its work. And if the answer is clear and simple, it has just as clearly alluded all of us to date.

The problem is as complex as it is vital and urgent. And let me stress the urgency.

On September 11th, Al-Qa'ida terrorists showed us, to our horror, that they were capable of exploiting a networked world against a U.S. government that was not networked. In less than 90 minutes, they brought down the Twin Towers of New York's World Trade Center and breached the walls of the Pentagon, itself, turning it into an inferno.

The toll, as we all know too well, was 3,000 innocent lives. And the terrorists succeeded, as we know, by exploiting the knowledge gaps that our stovepiped federal agencies had permitted to persist.

And almost three years later, all must acknowledge that despite serious and sustained efforts by the responsible government agencies, we still do not have the level of timely, routine and unfettered information-sharing we know that we need to prevent terrorism and to respond to it as effectively as we must.

The effort is not intellectual indulgence. It is not some administrative zero-sum game among executive branch agencies. Information-sharing in the post-9/11 world is job one. It is the irreducible minimum that we must do to ensure that our government can meet our most fundamental national expectation.

But using the authorities we, the people, conferred upon it, our government will safeguard us, our territory, and—this is critical—our constitutionally based way of life. We have come to call that mission homeland security, and we can conceive of nothing more pressing. There is no higher national priority.

The imperative of and challenges associated with information-sharing in the post-9/11 world draw people like our panelists today to deploy their expertise from much more lucrative pursuits in sustained and public consideration of how we can move critical information more efficiently to all of those, including state, local and competitive corporate entities who need it to met their own responsibilities within the overall homeland security mission.

If we, with their assistance, succeed, it will have been by fundamentally shaking entrenched bureaucratic cultures, by challenging residual resistance and complacency.

The task is well begun. Take a look at where we are. The 9/11 Commission's report will, like the joint inquiry's report before it, take hundreds of pages to describe a very straightforward problem that the terrorists exploited to devastating effect. We did not know what we needed to know, and what we did know did not get to those who needed it in time to be useful.

That is it. That is the problem that brings us here today.

DCI Tenet acknowledged the urgency of this problem and its solution nearly two years ago when testifying before the joint inquiry into the 9/11 attacks. Here is what he said.

"We must move information in ways and to places it has never before had to move. We need to improve our multiple communications links, both within the intelligence community and now in the homeland security community. Now, more than ever before, we need to make sure our customers get from us exactly what they need, which generally means exactly what they want, fast and free of unnecessary restrictions."

Let us take a look at what has been done about it since the attacks, the big innovations.

First, there is the Department of Homeland Security itself.

Second, there is TTIC, the Terrorist Threat Integration Center, a presidentially created interagency joint venture that is responsible for comprehensive analysis of all terrorist threat-related information.

Third, there is the Terrorist Screening Center, another interagency joint venture.

There is a fourth innovation, too. If DHS, TTIC and the Terrorist Screening Center are the new machinery in information-sharing, then the grease they will need to run smoothly is reflected in the March 4th, 2003, memorandum of understanding on information sharing. The attorney general, the director of central intelligence and the secretary of homeland security all signed this, binding their federal law enforcement agencies, the intelligence community and DHS itself.

This memorandum of understanding imposes sweeping new minimum standards for routine information-sharing to implement provisions of the Homeland Security Act and the Patriot Act.

The MOU requires that the secretary of homeland security be provided access to all information necessary for him to carry out the mission of the department. This reflects the language of the statute itself, which imposes upon the rest of the federal government requirements to provide information to DHS whether or not the department asks for it.

It provides that the federal government should speak with one voice by requiring that, except in exigent circumstances, the secretary of homeland security approve federal dissemination of non-law enforcement analysis to state-, local-and private-sector officials.

And it also requires that federal agencies generally disclose information they originate to other federal agencies, free of any originator controls or information use restrictions.

That may all sound unremarkable. It is, after all, just applied common sense. But these are fundamental challenges to the status quo ante of 9/11. And our job in Congress, as in the executive

branch, is to make sure that the requirements in that MOU are implemented fully and quickly.

Here on this committee, we have from the very outset stressed the priority of prevention and its dependence on unfettered and timely sharing of accurate information on terrorist threats. That will continue, and I am happy to report that our efforts are as bipartisan as is our panel today.

And what we do on this committee will never give those who look back on it in the future cause to suggest that we flagged in our oversight responsibilities or temporized in remedying the shortcomings we found. Because we all now agree that it is true, that what we do not know empowers our enemies, and what we do know will help defeat them.

It is true that, in this new war, the ongoing battle for our future, knowledge is the very essence of power. And we know by hard experience that if information does not move, people may die. It is that simple. That is the lesson of 9/11. We simply must get key information to those who need it most, and we cannot be satisfied with inefficiency or delay. We must make happen what must be made to happen.

We look forward to your perspectives and are grateful for your insights.

And moving on with this same sense of urgency, I recognize the distinguished ranking member from Texas, Mr. Turner, for his opening statement.

Mr. TURNER. Thank you, Mr. Chairman.

I have a chart I would like to ask the chair to allow me to put up.

Chairman COX. I would ask unanimous consent that the chart be admitted.

Without objection, so ordered.

Mr. TURNER. Thank you, Mr. Chairman. And thank you for scheduling what I believe, and I know we all agree, is one of the most critical issues that we could address on this committee.

And I want to thank the witnesses for being with us. I appreciate the work that The Markle Foundation has done to try to provide some guidance on how to solve some of these intelligence-sharing problems. And I appreciate Mr. Woolsey and Governor Gilmore for your continued involvement in the public sector to try to help and advise and to lead us in the right direction.

I think we all understand that coordination at the highest levels of our government on homeland security information-sharing is still, three years after 9/11, sorely lacking.

I think we saw a little window into that problem just a few weeks ago when Attorney General Ashcroft and Secretary Ridge issued what amounted to contradictory public statements on the same day about the current threat from Al-Qa'ida. They got together two days later and tried to remedy that with a joint press conference.

But I think, as Chairman Cox said on that occasion, the whole incident suggests that the broad and close interagency consultation that we expect and which the law requires did not take place in that instance.

So we were left with the public confused and still lacking in the basics, in terms of sharing information with the public regarding the nature of the Al-Qa'ida threat.

As the Markle report has indicated, as the Gilmore report has indicated, and as the soon-to-be-released 9/11 Commission report will point out, we are still falling short in three basic areas.

One, in the collection of information and the sharing of information with state and local officials.

Secondly, in synthesizing the counterterrorism analysis of the various and newly created intelligence fusion centers at DHS, DOJ and DOD.

And thirdly, we are falling short in that the federal government sharing of information with our first responders in timely manner, which I think is an essential part of being able to respond in this country to preventing and responding in the event of a terrorist attack.

So I thought the chart there would be useful, because what it shows you are the multiple lines of communication that now exist between the federal government and our first responders. This chart demonstrates how we are building separate, competing systems run by rival agencies to convey threat information to first responders.

For example, at DHS, we have the Homeland Security Information Network. At DOJ, we have the Regional Intelligence Sharing System. At DOD, it appears that the Joint Regional Information Exchange System, better known as JRIES, is another channel of communication that will be in use.

And it is also my understanding that the Terrorist Threat Integration Center, TTIC, is building out an on-line information system to reach first responders, as well.

So despite our good intentions, I would submit that we are building multiple, parallel information-sharing systems that cause more confusion for first responders and fail to ensure that all information gets to everybody that needs it.

In times of emergency, who will the first responders call on? Who will they rely on? Which information network will they turn to? These are all legitimate and important questions that the federal government needs to get a better handle on.

The Markle Foundation has very aptly pointed out, in its own comprehensive report, that there are major weaknesses in how the executive branch defines the respective roles, responsibilities and authorities of the federal agencies involved in assessing and disseminating homeland security information.

This lack of coherence is leading to turf battles between these agencies, gaps in the interagency information-sharing and analysis, and limited attempts to protect our civil liberties. We can and we need to do much better on managing interagency information-sharing.

I think the Markle Foundation concept is one that we have to come to grips with. That is, we have to collect information in real time into a common database available to all of the relevant agencies and personnel at the federal, state and local level. And that information must be accessible to the relevant state, local and fed-

eral officials and personnel who need it. And it should be available based upon the classification to which they should have access.

That concept has not been pursued by our government. And nobody, to my knowledge, other than what I have heard from The Markle Foundation, has seriously made an attempt to devise such an information-sharing system.

It was in the 2003 State of the Union address that the president announced the creation of the Terrorist Threat Integration Center, which was to, in his words, merge and analyze all threat information in a single location. The fact of the matter is that the CIA, the FBI, DOJ, DOD, DIA and DHS have all retained their own separate terrorist intelligence fusion centers.

Now, you can argue that competitive analysis of intelligence is a healthy practice. But creating and maintaining multiple intelligence centers is, in my judgment, a recipe for continued confusion and failure to coordinate the work of these various centers and have very real consequences to our security.

Mr. Chairman, it has been 30 months since 9/11, and it appears that we are still a very long way from solving what has been identified as the main reason that the federal government failed to detect and prevent that historic and unfortunate attack on our nation.

Again, I thank our witnesses for being with us today. I thank you for your continued work and effort to solve the problems that we are addressing today. And I look forward to hearing from each of you.

Thank you very much.

Ms. DUNN. [Presiding.] Thank you very much, Mr. Turner.

Do other members have opening statements?

Go ahead, Mr. Weldon.

Mr. WELDON. Thank you, Madam Chairwoman.

I welcome our witnesses. I have worked with two of them in a very close way. I have not had the pleasure of working with Ms. Baird. Jim Woolsey is one of the outstanding public servants in this city, and it is a pleasure to welcome him here, expert on intelligence and other issues.

And Jim Gilmore I am happy to see. I wrote the language that created the Gilmore commission, and I have worked closely with the Gilmore commission since its inception. If we had listened to the commission, who issued three reports before 9/11, and would have paid attention to the recommendations, we would have had a definite impact on the terribly tragic incident of 9/11.

But I want to talk about this issue today, briefly. This hearing is about post-9/11, but I want to go through with my colleagues something the 9/11 commission would not touch. And I assume they would not touch it because it would embarrass the Clinton administration and it would embarrass the Bush administration.

You see, my friends and colleagues, back in 1999, when I chaired the R&D subcommittee for the Armed Services Committee, we knew that data integration and data fusion was a challenge that had to be met.

In fact, working with it then, at that time, Deputy Secretary of Defense John Hamre, he challenged me to take the model developed by the LIWA facility of Fort Belvoir, which is the Army's in-

formation dominant center, which was stood up by each of the services, in this case the Army, to look at the capability of protecting the security of all of our defense classified information systems.

When the Army went beyond that, in developing with Fort Belvoir, they brought in external sources of data unofficially. I tested that system in the summer of 1999, and was so impressed with it that I convinced John Hamre to go down there, and he, like I was, was also very impressed, to the point where he said, "Congressman, I agree with you. We need to create a national operations and analysis hub."

And to my colleagues, here is the brief. This brief was developed in 1999, two years before 9/11. The goal was to integrate 33 classified systems that the federal government was operating, because that is how many there are—and here are all the agencies—33 classified systems, all the 3-letter agencies, all the agencies of the federal government, for one purpose: to have the ability to do data fusion, data analysis, for the issue of emerging transnational threats and dangers from terrorist acts.

John Hamre, he said to me, "Congressman, I will pay for it. DOD will fund it. I do not care where it is located. But you have to give in so CIA and the FBI that they should, in fact, become a part of this."

Let the record show that on November 4, 1999, in my office, the deputy director of the CIA, the deputy director of the FBI, and the deputy director of the Department of Defense, John Hamre, met with me for over one hour and received this brief, which I ask unanimous consent to place in the record. This brief calls for the creation of a national threat and data fusion center.

When we finished the brief, the CIA and the FBI said to me, "Congressman, we do not need that capability. We do not need that capability." We did not accept that. We put language in the Defense Authorization Bill, which I will also put in the record, calling for the creation of a national data fusion center in the 2000 defense bill.

Again, no one took it seriously. This was one year before 9/11.

Now, why the 9/11 Commission would not touch this, I am convinced, is because it would severely embarrass the previous administration but also this administration because we did not act on this recommendation until the president, in January of 2003, called for the creation of the TTIC.

And so I am pleased to be here today. And I am pleased to discuss what we have done since then. But I want our colleagues to know that the Congress is out front on this issue. If we have taken the steps in 1999 and 2000, perhaps we would have had a better understanding of the way that intelligence data could be fused to understand emerging threats.

Thank you.

Ms. DUNN. I thank the gentleman.

Does anybody else have an opening statement?

All right, let us move then to our panel's presentations. Why don't we start with Governor Gilmore. We are happy to have all of you here today. Looking forward to your testimony.

STATEMENT OF THE HONORABLE JAMES GILMORE, CHAIR, ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION "GILMORE COMMISSION" AND PRESIDENT, USA SECURE

Mr. GILMORE. Thank you, Madam Chairman. I am pleased to have an opportunity to be here today, particularly with these distinguished members of the panel.

I am personally acquainted with most all of you and work very closely, of course, with the congresswoman and Mr. Boehlert, Mr. Gibbons and others who are here and Mr. Weldon, most particularly, on the Democratic side. I am well-acquainted with most of the members. Appreciate your thorough leadership in these areas, Mr. Turner's wonderful opening statement.

We actually had Congresswoman Christensen participate with us on a bioterrorism program that we put together just recently.

So we appreciate the leadership of everyone.

I want to highlight Congressman Weldon. He actually wrote the language that created the advisory panel to this Congress on terrorism and domestic response capabilities involving terrorism, weapons of mass destruction, and wrote it in 1998 and established the commission in the beginning of 1999. He has followed the commission like no other in Congress, has been very careful with his leadership.

And, Congressman Weldon, we appreciate your leadership in all these matters. And hopefully, we have lived up to your hopes and aspirations for this legislation.

It has been my pleasure to chair the commission since its inception, when I was asked by the Clinton administration Department of Defense to actually do that while I was still governor of Virginia. I was delighted to be invited to do it.

I had been an intelligence agent in the Army intelligence back when I was in the service. In the 1970s, I had a high interest in the terrorism issues, so I was pleased to have the chance to work with the RAND Corporation as a staff organization and distinguished people from the responders community: police, fire, rescue, emergency services, retired general officers, intelligence people, epidemiologists, health-care people. It was truly a professional organization. It was my honor to chair that distinguished commission in their work.

The work that we did was over a five-year period. This Congress actually passed a statute to create this commission for three years. It was to have its final report December 15, 2001. We issued our very first report at the end of 1999, at which time we assessed the threat, and were concerned and warned, at that time, that the chance of an attack in this country on the homeland was a very high probability. And in fact some of our language used the word "inevitable."

In the second year, in 2000, we—and again, our commission never really looked back. It never attempted to blame anybody for anything. Our goal was to look ahead constantly and to try to provide this Congress with the best possible insight.

In the second year, we focused our attention on the national strategy, the need for it to be federal, state and local, for the White

House to have the proper facilities in place to create a national strategy and expressed great concern about the inability of the intelligence committee to share information either amongst itself or, frankly, up and down the chain between federal, state and local people—a cultural anathema which we believe exists to this day.

The third report was actually completed and at the printer, in which we discussed five major areas: How do you use state and local people? What do you do about the health-care community, particularly with the threat of bioterror? What do you do about border control? How do you deal with the military in a homeland situation? And then, finally, the issue of cyberterrorism.

And then the attack occurred while it was at the printer. The report was issued on time in December the 15th in 2001. And then this Congress, under the leadership of Congressman Weldon, extended the commission for two additional years.

In the fourth year, we focused our attention virtually exclusively on the intelligence—well, that is too broad. But we especially focused on the intelligence concerns, recommended that there be a fusion center, which later became the TTIC.

There was a debate in our commission for almost a year over the issue of whether or not we have a separate MI–5 organization to do intelligence work or rely on the FBI. As chairman, I have led the group that believed that the FBI should be required and forced to do it. Jerry Bremer, who had served four years on the commission, led the group that believed that the FBI could not do it and that MI–5 type of model was the better approach. And the commission adopted that, in fact, recommendation to the Congress.

Then finally, we just issued our last report this past year, in which we tried to look out once again, to express grave concern after five years; to, at the same time, express the desire that we should rethink where we are trying to go and to try to somehow eliminate the fear and anxieties, and focus our attention on the civil freedoms aspects.

The testimony that I believe I would give you today is a reminder that if we are going to address this issue in two pieces, which is prevent and respond—which I believe the Congress has expressed in numerous meetings and testimony that they are concerned about—is the recognition that vulnerability is really not threat.

It needs to be remembered that everything, particularly in a free society, is vulnerable. You have vulnerabilities in a less free society, quite frankly. But threat is the intentions and capability of the enemy. They may want to attack vulnerable things and systems and people. But the question is, what do they want to do, what are their intentions and what are they capable of doing?

And that brings intelligence to the fore. There is no way to address that kind of threat in any intelligent way, other than to focus our attention on the intelligence piece and to make sure that intelligence is available and coordinated and accessible.

And finally, we have to deal with the issue of how we share intelligence and information and to put the proper structures into place. This is a big challenge, particularly with this committee has to deal with issues of a disparate and disperse nature of the intelligence organizations. On the response side, we need to focus our attention

once again on harmonizing federal, state and local people into a unified program.

So with all this being said, it has been our pleasure to represent the Congress and to advise you for five years on these areas. This committee, we believe, is focused and central. We are proud of the work that you are doing. We recommended a central type of committee that would be in a position to address these issues; that is what this committee is. We appreciate your work and look forward to your leadership in the years ahead.

Ms. DUNN. Thank you very much, Governor.

We will next move to former director of the CIA, the honorable James Woolsey.

STATEMENT OF THE HONORABLE JAMES WOOLSEY

Mr. WOOLSEY. Thank you, Madam Chairman.

If it is all right, I will ask my statement to be inserted into the record, and I will use it as notes to speak from.

It is an honor to be asked to testify before you today. I am going to talk principally about the likely substance and sources of information that might be shared, since I believe that the organizational structure and the procedure should probably be derived therefrom.

First of all, in my judgment, this, what I call the long war of the 21st century, which we are engaged in now—and by the way, I believe it will last for decades, like the Cold War—will not be dominated, the information about it will not be dominated by foreign intelligence, as was the Cold War.

One learns very little about terrorists by looking at them with satellites. They have learned to avoid the links that we intercept, partially because of press leaks. And penetrating terrorist cells, particularly decentralized terrorist cells, is extraordinarily difficult—much, much harder than penetrating the KGB or the Warsaw Pact general staff.

We will get continuing information from intelligence liaison; that is, information provided by friendly intelligence services in the Middle East and elsewhere. But we are unlikely to be able to have the advantage that we had in Afghanistan of taking over Al-Qa'ida files, disk drives, senior Al-Qa'ida prisoners and the rest.

So if intelligence liaison is a source of much of our foreign intelligence, we are going to find that there are people who are in this business of decision-making who, for example, do not agree with the MOU of March, that there should be no restrictions on originator controls, or so-call ORCON restrictions on intelligence.

It is not the CIA principally you need to worry about here, it is the intelligence services of such countries as friends in the Middle East. Because any country, when they provide information to the United States and we to they, say, "By the way, this will not go beyond the following four people, and we are willing to provide it to you on that basis, but not otherwise," so very broadly disseminated information that violates those understandings with foreign intelligence services, will mean that those foreign intelligence services will not for long be providing information.

Second, it is important to realize that the 9/11 plotters worked principally in the United States and Germany, two countries where

the United States foreign intelligence services essentially do not spy. They knew what they were doing. They knew about civil liberties in Germany and the United States.

Although the CIA made a terrible mistake in not listing Al-Midhar and Alhamzi, the two pilots of one of the flights, whom they were tracking in Malaysia in January 2000 and not putting them on a watch list for the FBI and the State Department, generally speaking, the information that was available, potentially available, on the 9/11 plotters was not information from traditional sources of foreign intelligence.

So anyone who believes that in this long war of the 21st century against Islamist fanatics in the Middle East is going to be at all analogous to the Cold War, and that we are going to have a substantial flow of information from foreign intelligence and technical intelligence, I think is operating on a false premise.

I believe that, furthermore, we are going to have to do a lot of our own vulnerability assessments. Some of the most sensitive intelligence, in a sense, about our own vulnerabilities will come from us, from people working on red teams, understanding the vulnerabilities of the electricity grid, the oil and gas pipelines and the like.

And dissemination of that information will have to take place, but I think in very specific ways. Sometimes in a specific locality. If you have a vulnerability of the Golden Gate Bridge, a lot of people in San Francisco are going to be working on it, but people in the rest of the country do not need to know much about it. If you have a vulnerability of toxic chemical production and delivery, people in the chemical industry and the railroads will need to know about it, but probably not others.

Now, that is self-generated vulnerability information, not really intelligence, in a sense, but I think very important information.

I think that it is very important for us to realize that we are at war with Islamists from two sides of Islam.

And I say "Islamist" to connote a totalitarian movement masquerading as a religion. I believe that Hezbollah and their supporters in the Iranian government, that Al-Qa'ida and their supporters inside Saudi Arabia and elsewhere, are about as much Muslims as Torquemada was a Christian. And in order to denote that, I use the term "Islamist" rather than "fundamentalist Muslim" or otherwise.

But we are going to have for some time a nationwide problem with respect to Islamists, particularly from the Sunni side of Islam. And much of the useful information that we will obtain I think will be by first responders, by state and local law enforcement.

This is one of the main reasons why I believe it is important to leave the FBI in the lead. I agree with Governor Gilmore on this point, because they have a long history and background of dealing with state and local government.

It is true that their culture in the bureau is more, certainly, one of law enforcement, of grabbing one of the 10 Most Wanted, rather than long-term espionage penetration operations, but they have done the later twice successfully, once with the American Communist Party and once with the Mafia.

So I think the jury is still out, but at least for the time being I think we should stay with the FBI's responsibility.

Let me close by simply noting, the last page or so of my remarks express that I believe one of the most important sets of intelligence information we will deal with in this whole area is counterintelligence information, and that is information about Islamist penetration of American institutions and presence in the United States.

That sort of information is not wise to disseminate widely. I speak to you as the DCI who was on duty when we caught Rick Ames. And I rather imagine that those in the FBI who were on duty when Hanssen was apprehended would have a similar thought, that there were at least some aspects in both the bureau and the agency of internal information-sharing that were substantially too broad. And most counterintelligence officials on that sort of information think rather hard about the proposition that it sometimes is better to restrict information flow rather than broaden it.

I think we have to realize that, in this world we live in, sometimes important objectives—disseminating information properly and keeping it away from those who should not have it—conflict just as, unfortunately, sometimes liberty and security conflict.

And what we are going to need to do in the interests of doing the right kind—and in many cases, it should be extensive—of information-sharing, what we are going to have to do is make case-by-case determination of the types of information, what the source is and how we can disseminate it effectively without running into some of the problems of disseminating some types of information too widely.

Thank you, Mr. Chairman.

[The statement of Mr. Woolsey follows:]

PREPARED STATEMENT OF R. JAMES WOOLSEY

Mr. Chairman, Members of the Committee, it is an honor to be asked to testify before you today on "Information Sharing After 9/11: Perspectives on the Future".

Rather than deal with issues of organization and procedure related to information flow in these opening remarks, I thought it might be useful if I shared with the Committee some thoughts about the likely substance and sources of information that might be shared, since I believe that organization and procedure will be heavily influenced thereby. We need to understand what we are sharing and why before we design a system.

First, I think that the source of information about vulnerabilities of and potential attacks on the homeland will not be dominated by foreign intelligence as was the case in the Cold War. As contrasted with, say, the type of ICBM likely to be installed in a Soviet silo one learns very little about terrorists by trying to look at them with satellites. Further, although we once had some good sources via signals intelligence about terrorism, the terrorist groups have learned to stay away from many types of communications that might be intercepted and to communicate only very vaguely on others—in part the result of US media having broadcast such stories as, e.g., how we were listening to bin Laden's satellite telephone. And it is very difficult to penetrate terrorist cells with spies—much harder than, say, penetrating the KGB or the General Staff of the Warsaw Pact.

We have obtained important information on terrorism by our military success in Afghanistan and we do, and will, obtain much useful material via liason with foreign intelligence services. But the very disruption of Al-Qa'ida's overall command structure in Afghanistan has meant that we are dealing with a group of individual cells even more than in the past—even less likely to be penetrated.

It should also be remembered that the 9/11 plotters made their preparations principally, although not exclusively, in the US and Germany. US foreign intelligence agencies basically don't operate here (the circumstances in which they could assist the FBI under the Foreign Intelligence Surveillance Act are quite limited) and in

Germany they would rely on German authorities. The terrorists understood us well, and so they lived and planned where we did not spy.

Thus if anyone is constructing organizations and procedures for intelligence sharing based on the assumption that there will be a flow of foreign intelligence dealing with terrorist threats to the homeland that is at all analogous in volume and importance to what flowed about the USSR and its allies during the Cold War, I think he is building on a false premise.

Instead, in my view, we should focus heavily on how best to share two sorts of information about our vulnerabilities and potential terrorist exploitation of them.

One source will be our vulnerability assessments, based on our own judgments about weak links in our society's networks that can be exploited by terrorists—e.g. (to mention two that have been widely discussed in official publications) dirty bombs in shipping containers, or transformers in the electricity grid. We need to do this sort of analysis systematically and, where possible, without widespread dissemination of our judgments beyond those whose help is needed to make these links more resilient. Sometimes this will involve a number of people in a specific local area, or in a specific industry—the extent and method of sharing this sort of information will depend on the vulnerability and the steps we need to take. We cannot, of course, make ourselves wholly invulnerable to attack, but we can take away (or make far less lucrative) a number of the more attractive targets for terrorist attack.

A second source will be domestic intelligence.

How to deal with such information is an extraordinarily difficult issue in our free society. Not only are our borders extremely open, even with some added post-9/11 restrictions, to legally-traveling workers, students, tourists, and many others, but illegal access to the US is of course very widespread.

Further, if we focus for purposes of this discussion only on the Middle East, we must over the long run prepare to deal with terrorists from at least two totalitarian movements masquerading as religions: (a) Islamists from the Shi'ite side of Islam's great divide, such as Hezbollah, and those who support them, such as the government of Iran; and (b) Islamists from the Sunni side of Islam, such as Al-Qa'ida, and those who support them, such as wealthy individuals in Saudi Arabia and the Gulf and some portions of the Saudi Wahhabi religious establishment.

Concentrating on the second group as the most immediate problem, we know from the FBI raids on terrorist financing operations such as those in Herndon, Va., and on cells such as the one uncovered in Lackawanna, NY, that we have a nationwide problem from Sunni Islamists. The difficulty of penetrating and learning of the efforts of such groups is very great. Much of what needs to be done involves cooperation with local law enforcement. Only an effective local police establishment that has the confidence of citizens is going to be likely to hear from, say, a local merchant in a part of town containing a number of new immigrants that a group of young men from abroad have recently moved into a nearby apartment and are acting suspiciously. Local police are best equipped to understand how to protect citizens' liberties and obtain such leads legally. In my judgment, on these important issues the flow of information sharing is likely to be more from localities to Washington rather than the other way around.

It is first and foremost because of their history of working closely with local law enforcement that I believe we should leave the FBI in the lead with respect to domestic intelligence collection for the present. If the Bureau turns out not to be capable of refocusing a major share of its effort on domestic intelligence collection regarding counter-terrorism, a step that will to some extent require a change in the culture of a major part of the Bureau, then we will perhaps need to visit the notion of establishing an American version of Britain's MI–5. But I do not believe we are yet at that point.

Second, we will need to mesh the above sort of information flow from the grass roots with work being done at the national level. Among the most important national level efforts will be counter-intelligence—particularly understanding the activities in this country of individuals and institutions funded by radical Saudis and others in the Gulf, often allied with the most virulent clerics within the Wahhabi movement in Saudi Arabia. Not all Wahhabis or angry wealthy Saudis who give large sums to radical causes here or elsewhere have in mind supporting particular terrorist operations by Al-Qa'ida and its affiliates. But not all angry German nationalists of the 1920's and 1930's became Nazis—yet that was the soil in which Nazism grew. And it is in the angry soil fertilized by Wahhabism and a segment of the Saudi establishment that Sunni Islamist terror has grown—with substantial help from the some $70 billion that the Wahhabis and their allies have spent in the last quarter century or so to spread their hatred around the world, including here.

I would close by noting that the widest dissemination of information, particularly regarding our vulnerabilities or counter-intelligence, is not always the best policy.

In the aftermath of the Ames and Hanssen cases I am sure that both the Agency and the Bureau wished that at least some aspects of their internal information sharing had been more restrictive, not less so.

In this context I would call the Committee's attention to a recent report of what may well have been an unintentional omission on a form, but which raises the issue of how important it is to make careful judgments about how widely information is disseminated. In a piece in Salon.com day before yesterday, June 22, by Salon's Washington Correspondent, Mary Jacoby, it was reported that "[t]he policy director for the Department of Homeland Security's intelligence division was briefly removed from his job in March when the Federal Bureau of Investigation discovered that he had failed to disclose his association with Abdurahman Almoudi, a jailed American Muslim leader. Almoudi was indicted last year on terrorism-related money-laundering charges and now claims to have been part of a plot to assassinate Saudi Arabia's Crown Prince Abdullah." The article adds that the individual who was temporarily removed". . . has access to top secret information on the vulnerability of American seaports, aviation facilities, and nuclear power plants to terrorist attacks." It further adds that the Bureau had discovered that the individual". . . had failed to list on security clearance documents his work in 2001 with the American Muslim Council. . . an "advocacy group, which was controlled by Almoudi [and] has been under scrutiny in an investigation of terrorism financing. . . ."

The point is to get information to all those who need it, but only to those who need it and who can securely be trusted with it—unless by tear-lines and other techniques the information can be effectively declassified. It will always be the case, however, that you can make a better judgment about the weight you should give to intelligence of any variety the more you know about its source. And the more source information is disseminated, the more likely it becomes that the source will be compromised. Effective sharing of intelligence with those who can use it is a major and important objective, and so is avoiding the risk of compromising sources or vulnerabilities. Sometimes important objectives (liberty and security, e.g.) conflict more than we would wish. Each case of sharing, or not sharing, requires careful decision-making. There is no substitute for that.

Thank you, Mr. Chairman.

Chairman COX. [Presiding.] Thank you for you statement.

Ms. Baird is recognized for her statement.

STATEMENT OF MS. ZOË BAIRD, PRESIDENT, THE MARKLE FOUNDATION

Ms. BAIRD. Thank you very much. It is a real privilege for me to be here with these panelists and with this committee, which has done such an extraordinary job in trying to grapple with the new challenges facing the country.

Thank you very much for inviting me in to talk about the things that we have been considering at The Markle Foundation. I would ask also that my statement be included in the record.

As the chair has indicated, reports due out this summer from the 9/11 Commission, from the Senate Intelligence Committee, as with the joint inquiry, are expected to be highly critical of our nation's intelligence and law enforcement community in its ability to collect and share the needed information.

We can predict that they will report that the systemic barriers to information collection and sharing that existed prior to 2001, September 2001, which has already so effectively been articulated by the chair and Congressman Turner as a critical failure prior to 9/11, that those systemic failures exist today; they continue to exist today.

A number of reforms are already begun to be discussed: the notion of creating a U.S. version of the British MI–5, the notion of creating a stronger director of national intelligence or DCI with stronger powers, which members of this committee have been considering in the Intelligence Committee.

The introduction of these structural reforms, I believe, are going to awaken Congress, the administration, America to some new very large questions, some questions, which I had the privilege of thinking about in the mid-1990s with Congressman Dicks and Congressman Goss on a commission that was set up to look at the future roles of the intelligence community.

Those are issues of whether we can still continue to organize ourselves with the line at the border, with the separation between domestic intelligence and foreign intelligence. And I raise this now only to say that this committee, Congress moved with great speed to create the Department of Homeland Security, in fact, relative to other major governmental restructurings and reorganizations.

But I believe that, as these new recommendations come out this summer for other major structural reform, we are going to find that some very, very large and fundamental questions need to be grappled with first. And the consideration of whether to reorganize ourselves along a line at the border with separate foreign and domestic intelligence or whether to reorganize ourselves in some other ways functionally are going to cause us to take some time to consider those recommendations.

And I do not believe that we have the time to wait in improving our information-sharing. I believe it has been pointed out by all three of the members of this committee who have spoken that the urgency was there years ago, but certainly the urgency is there now.

And we need to move quickly to correct the situation, because information is the key to our future security. Information collection, sharing, while protecting civil liberties, is the essence for providing for our nation's security in this period of time where the biggest threats to our national security are from terrorists.

So whatever reforms are pursued, we believe that we should create a system of information-sharing between the existing actors, and that that system can serve any future organizational structures.

Using currently available technology, we believe that the government can set up a network that will substantially improve our ability to share information in order to prevent terrorist attacks, and that when this technology is paired with key guidelines that govern who gets access to the information, how it is used, that audit—so that someone like a Hanssen would not be able to go into databases where he had nothing to do, because, one, he would not have had the authorization, and two, we could have found that he was there, so he would not have felt it was an easy target—that this technology, coupled with strong policy guidelines, can quickly provide our country with both the ability to share information and the ability to enhance our civil liberties protections and our protections of sensitive requirements like sources and methods.

We have proposed, through this bipartisan task force that includes people from the Carter, Reagan, Bush and Clinton administrations with substantial expertise in national security, which includes people from the technology community with substantial expertise, both in traditional mainframe-type systems and new technologies, and includes civil liberties advocates, we believe that the most important issue the government has to face is getting an in-

formation-sharing network created, and that this, as Congressman Harman has called it, "virtual reorganization of government" can be done quickly and effectively and is a fundamentally new way of getting the government able to improve its decision-making.

I would be happy, in the question-and-answer period, to talk about the elements of a SHARE network, as we call it, that would meet these goals, but we do believe that it is achievable and can be done very quickly.

So I would just close with saying that there are a few key features of a network to work. It has to be decentralized, which means that information has to go out to the local people, whether it is a local FBI field agent or a local police department, as well as come in from them. Because they will see things that, if put together with information collected by more central authorities tasked by the FBI or the CIA, will make sense, will create a picture that we would not otherwise see.

We can do that using technology to provide authorization and permissioning and not create the kind of risks that Jim Woolsey and other have alluded to. And we can do it through things like minimizing, eliminating, the names of individuals until there is a demonstration of a need to know someone's name. We can do it in a manner that protects civil liberties.

So I thank you very much for having me here, and I am very happy to answer your questions. Thank you.

[The statement of Ms. Baird follows:]

PREPARED STATEMENT OF ZOË BAIRD

Good Morning, Chairman Cox, Congressman Turner and members of the Committee. I appreciate the opportunity to testify today.

Reports due out this summer from the Senate Intelligence Committee and the 9/11 Commission are expected to be highly critical of our nation's information collection and sharing capability. As we await the release of these reports, we can predict one of their findings with near certainty: That systemic barriers to information sharing, which seriously hampered the efforts of our nation's intelligence agencies prior to the September 2001 terrorist attacks, still exist today.

A number of recommendations have already been made about what further reforms are needed to better equip our government in the fight against terrorism. Some have recommended an American domestic intelligence agency, similar to Britain's MI–5, to improve collection and analysis of intelligence at home. Others have advocated the creation of a Director of National Intelligence (DNI) with greater authority than the current Director of Central Intelligence, to direct and coordinate the entire intelligence community.

Once the debate begins in earnest, we will find ourselves grappling with a number of very complex questions. For example, does the "line at the border"—the different rules for collecting and handling of intelligence depending on whether it is foreign or domestic—a line which has been eroded need to be substantially reconsidered? Must we find new ways to protect critical interests like sources of information or the privacy of our people because the line at the border or classification systems prevent us from fully understanding terrorists' intentions and capabilities?

It will take time to determine the right course of action on proposals for an MI–5 or an DNI, and once that course has been plotted, implementing any structural reforms could take years. But we do not have the time to wait to improve information collection and sharing. We need to impress upon responsible officials the urgency of this task and we need to act now. The actions we take can accelerate the ability of any agency organization, present or future, to improve our security.

Fortunately, by capitalizing on America's technological capabilities, we can begin to make our nation safer. Using currently available technology, the government can set up a network that streamlines operational and decision-making processes and substantially improves our ability to share information in order to prevent terrorist attacks. And when paired with clear guidelines to govern the system and effective

oversight, the use of information technology can also be the best way to protect privacy and civil liberties.

For the past few years, I have had the privilege to convene the Markle Foundation's Task Force on National Security in the Information Age. The Task Force, comprised of leading national security experts from the administrations of Presidents Carter, Reagan, Bush and Clinton, as well as widely recognized experts on technology and civil liberties, was created to focus on the question of how best to mobilize information and intelligence to improve security while protecting established liberties. In fact, one of our unifying principles is that information—managed through information technology—is the key to enhancing security.

In our most recent report, **Creating a Trusted Information Network for Homeland Security** (*http://www.markletaskforce.org/*), the Task Force recommended the immediate creation of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network, which would foster better analysis and sharing of information among all relevant participants at every level of government, with built-in practical and technological safeguards for civil liberties. Or, as one of your own Committee Members, Congresswoman Jane Harman, has called it, a "virtual reorganization of government."

The SHARE Network would represent a fundamentally new way of using information to facilitate better, faster decision-making at all levels of government. It has several key features:

- SHARE is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants in the system. Such an approach empowers all participants, from local law enforcement officers to senior policy makers.
- SHARE is based on the concept of "write to share." Instead of the Cold War based culture that placed the highest value on securing information through classification and distribution restrictions, SHARE recognizes that sharing information makes that information more powerful because it links it to other information that can complete the picture. SHARE moves from a classification system to an authorization system. By taking steps like incorporating "tear lines" in document formats, SHARE would encourage reports that contain the maximum possible amount of sharable information.
- SHARE is a hybrid of technology and policy. The system would use currently available technology to share and protect the information that flows through it. And when paired with clear guidelines that would determine the collection, use and retention of information and who should have access to information, it can both empower and constrain intelligence officers, and provide effective oversight. Such an approach is also the best way to protect privacy and civil liberties.
- SHARE allows for vertical and horizontal co-ordination and integration. Information would be able to flow not just up the chain of command, but also to the edges of the system.
- SHARE enables analysts, law enforcement agents and other experts to find others with common concerns and objectives, to come together in shared workspaces, to form "virtual" communities to exchange information and ideas.

While those are just a few of the technical and policy features of the SHARE Network, I think it would be useful to give you a real world illustration of how the system could actually operate.

Say a field agent at the Chicago FBI office and a CIA operative in Kabul become aware of separate leads that if put together might point to a bio-warfare attack in Chicago. Under the current system, reports from these two agents are unlikely to have enough actionable information to be moved through the system. However, using the SHARE Network, these reports would be linked through similar key words such as "virus" and "Chicago" or other linking tools. Instead of being housed in classified files and filing cabinets at the CIA and FBI, these reports would be distributed electronically to people who should see them. They also would be posted and available to be pulled by network participants with a particular interest. An analyst at TTIC, for example, might see both reports, contact the CIA and FBI agents and others to discuss their reports, begin to connect the dots and define actionable objectives. The FBI, CIA, and TTIC players could form "a virtual task force" by reaching out to other relevant agencies and individuals, perhaps at Department of Homeland Security, the Centers for Disease Control or a local police department, for more information. And they could organize the work themselves, without losing time or going to their superiors in Washington for approval.

Based upon their discussions, this group could now create actionable intelligence for their agencies: the CIA might elevate the information to a higher level, to the director, or perhaps up to the president. Through local contacts, the FBI would have

the option of notifying local police, so they could watch for activities related to a potential plot.

Meanwhile, because access to certain kinds of personally identifiable information would be restricted, and systems built in to verify the identities of those permitted access, we will have improved information sharing while better protecting our privacy and civil liberties.

Members of our Task Force have met with a number of officials at federal government agencies regarding our recommendations—some repeatedly—and have seen a high level of interest. In fact, a number of government agencies have been moving to direct the creation of processes that use key elements of the SHARE Network. The FBI, for example, has taken a number of positive steps in developing its new information sharing policies, including adopting a potentially extremely important policy of "writing for release," which encourages tear lines and "shar[ing] by rule and withhold[ing] by exception".

TTIC's posting of intelligence reports and other items on "TTIC Online," although not broadly available, is a step toward the kind of sharing we contemplate. And the Homeland Security Information Network, currently being developed by DHS, could strengthen the flow of real-time threat information to state, local, and private sector partners if they plan to share adequate information.

While this progress is positive, an agency-by-agency approach is not adequate. Individual agencies can only go so far before they confront obstacles to sharing with other agencies of the federal government or with state and local actors, not to mention the difficulties involved in working with private sector entities. In order for this networked approach to succeed, a national framework, such as our proposed SHARE Network, is critically needed.

Members of Congress can contribute to our nation's ability to prevent and respond to terrorism by calling for the creation of an information sharing network with the characteristics of the SHARE Network. In our Report, we called for DHS to be designated the lead agency of an interagency, public-private process to establish the concept of operations for the network. Policy guidelines need to be written that both empower government officials to share information and also strengthen protection of privacy and other civil liberties. Agency CIOs need to be given the direction, authority and budgetary commitments to build the network. CIOs also need to have the funds protected so that the funding is not reallocated. Agencies need to be encouraged to acquire information technology that is interoperable (across agencies, across systems, and with legacy systems), and has common data standards as well as security, access controls, identity controls, and audit capabilities. Availability of technology is not a hurdle to adoption of the SHARE Network; the hurdle is the manner in which agencies acquire technology.

In addition, proposed and current information sharing initiatives such as the Homeland Security Information Network, TTIC, US VISIT and CAPPS II need to be jointly reviewed as to whether they support these network objectives. Otherwise, waste, stovepiping and redundancy will occur if they are not built according to a common concept of operations.

The collection, use and sharing of information by government agencies needs to be guided by both Presidential directive and by Congressional oversight. We laud Congress's commitment to establishing internal oversight mechanisms within the DHS, including a privacy officer and a civil rights and civil liberties officer. We encourage the further development of informal and formal means of congressional oversight of the government's access to, use, retention, and dissemination of private sector data.

Other government bodies have a role to play as well. The Technology and Privacy Advisory Committee to the Secretary of Defense, on which I served, recently built on the Markle Task Force Report and made further recommendations for processes to protect privacy and civil liberties, including requiring in certain circumstances that an agency articulate the relationship to terrorism of information they seek on U.S. persons, and use of the FISA court for domestic information collection in sensitive circumstances.

Finally, as we have outlined in our Report, it will require continued engagement from the President himself, the heads of government agencies, as well as continual oversight from Congress to ensure follow-through. Indeed, agencies' performance towards a virtual reorganization should be evaluated by Congress after a reasonable implementation time, using specific and clear objectives for improved information sharing, based upon the set of metrics in our Report. If an agency has not performed adequately, the President and Congress should consider making any necessary changes.

While government migrates to the kinds of IT systems business has used for years to achieve the capabilities described above, there are immediate steps that can be

taken to begin reaping the benefits of new business processes. We should immediately create electronic directories to link people in different agencies working on the same problem, to identify experts in the private sector and universities, and to indicate which agencies have information on subjects of interests. We should adopt clear rules empowering government officials to get the information they need from other agencies. We could begin by ensuring that detailees at intelligence fusion centers have online access to all information. To facilitate sharing, we need to revisit the application of the "need to know" principle. To protect privacy, these rules should allow access to information without identifying U.S. persons by name, and establish processes for learning identities when necessary. And, to ensure greater public and congressional confidence, we need clear guidelines on how people get their names off watch lists, and how they seek redress for adverse government actions. The US VISIT contract, the development of the Virtual Case File at the FBI, the ongoing work of the TTIC and the TSC all offer opportunities to achieve critical, immediate incremental reforms if they are required to serve a common vision instead of being developed in stovepipes.

Implementing a system like the SHARE Network would allow agencies tasked with protecting our nation from terrorism to build information sharing into their overall mission before, and as part of, any major restructuring of our domestic or foreign intelligence agencies that Congress might undertake in the future. It would prevent information from being kept in agency silos, as too much still is, and would encourage analysts to push information to the edges of the system—to FBI and customs field agents, to police—instead of only moving information up the chain to the next level in an agency hierarchy or to a narrow set of analysts or operational personnel who are not allowed to share it with others.

Information, managed through technology, is critical to enhancing our security while protecting important civil liberties. Information-sharing itself is not the goal; rather, it is the means by which we can most effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information. The nation can never sufficiently harden all potential targets against attack, so the government must develop the best possible means to obtain advance warning of terrorist intentions through better intelligence.

The network the Markle Task Force has proposed would substantially improve our ability to uncover threats and prevent terrorist attacks. The technology to create such a network exists and is used in the private sector every day. Given the proper priority in budgets and leadership, we believe that it is possible to develop and implement major steps immediately, and many key elements of the SHARE network in about eighteen months.

Since September 11, many people in the government and the private sector have given a great deal of thought and effort to the problem of how our nation can use information and information technology more effectively to protect people from terrorism while preserving our civil liberties. Our Task Force has sought to contribute to the solution by providing the framework for a national strategy and an architecture for a decentralized system of robust information-sharing and analysis that makes the most effective possible use of information while instituting guidelines and technologies to minimize abuses and protect privacy.

Thank you.

Chairman COX. Thank you very much for your statement.

Thank each of you for your statements.

The chair will now recognize members for questions that they may have. As is our custom, I will recognize those members who were present within five minutes of the gavel in order of their seniority on the committee. Those arriving after that time will be recognized in order of appearance.

I recognize myself for five minutes.

Let me begin by asking how each of you recommends Congress conduct proper oversight of whether the Department of Homeland Security, which, as we all recognize, is central to information-sharing, analysis and distribution, is getting the information that, by statute, it is supposed to receive.

We all know that, even at the collection level, we do not know what we do not know. The entire Department of Homeland Security is, roughly speaking, in that position. The statue requires that

even without a request, precisely because they do not know what they do not know, information should be provided to them without asking.

How can Congress properly oversee whether that statutory mandate is being fulfilled? I would address it to each of the panel members.

Mr. GILMORE. Congressman, I think that the leadership of the Department of Homeland Security wants to have good interaction and communication with the Congress. I have never heard anything except their desire to have a good working relationship and to share that information.

Naturally, the committee has its budgetary power and authority. But I believe that a focus, putting the Congress into one focal point, which really is this committee, and any counterpart that it has in the Senate, gives at least the department a single place to go in order to communicate appropriate information. And that, I believe, is why this committee is so important, as creating that focal point.

Naturally, within the structures of the Congress, you have to have good communication on the appropriations side, so that there is some overarching strategic view of what the Congress wants to do with the department. But once again, this committee, I believe, serves that focal point. But the Congress, itself, you can use its budgetary authority. But I believe that there is a good desire for interaction.

Chairman COX. And let me ratchet this question up to make it clear where I think the toughest problem lies, because, Governor Gilmore, as you point out, to the extent that at least the House has organized itself so that there is focal point for oversight and authorization of this new department, we have accomplished that task.

But the greater problem is that if we are trying to assist the department in fulfilling its statutory mandate, we have to make sure that all these other agencies of government, including the entire intelligence community, including law enforcement, are sharing the information that, by statute, they must share with the department.

And that would require oversight that is even broader than the collaboration that we have put together here in the Congress to make this Homeland Security Committee.

So what tools ought we to use? And I know you are each familiar with the tools of Congress. How might we deploy them, in order to make sure this job gets done?

Mr. WOOLSEY. Mr. Chairman, I do not think this can be done effectively without having some sort of a joint hearing in which representatives from the Department of Homeland Security and from the DCI and from the FBI are present, because the latter two are going to be the major sources of information from outside.

Now, these could be difficult hearings. For example, if I am correct in my assessment and most of the information from foreign intelligence on a continuing basis is going to be from liaison services, from friendly services in the region, and each of them says, "No way, no how you are going to share this, CIA, with anybody," we have a problem.

I would think that executive session hearings, cooperative hearings with intelligence community and those responsible in the Judiciary Committee for the FBI, would be things that one might want to explore.

But I do not see any way of really getting at this other than having the other agencies at the table and doing it in a classified environment.

Mr. BOEHLERT. Will the gentleman yield to the Chair?

Chairman COX. Certainly.

Mr. BOEHLERT. I also serve on the Intelligence Committee, and this is something that concerns me.

As the chairman said, you do not know what you do not know. If we had these hearings, joint hearings between Intelligence, Homeland Security behind closed doors, highly classified, but we do not know what we do not know.

So if DCI says, "We are sharing all pertinent information with the secretary of homeland security," how do we know if he is not telling the truth? How does the secretary of homeland security know he is not telling the truth?

Mr. WOOLSEY. Well, in a classified environment, and with Intelligence Committee members or chairman present, one could presumably ask more specific questions, such as, "Have you gotten anything in the last 12 months from the government of Jordan? If so, what?"

I do not think a vague sort of a general question, "Have you given us everything that we ought to have?" will produce much more than, "Sure."

But I think if one wants to get into this, that is the sort of question I think you have to ask, because much of this information, if it is foreign intelligence—now, the FBI is a different question, but much of this information, if it is foreign intelligence, I think will come from liaison services. And each one of those is a unique and delicate relationship.

Ms. BAIRD. I am going to take a little contrarian position on that question. I think it is very difficult for Congress to know whether particular information is moving. I think you need to be much more focused on the rules for moving information and the process.

For example, if this committee or Congress called on the Department of Homeland Security to take responsibility for creating a public-private process to develop a concept of operations for how information moves across all these agencies, what are the requirements of what the FBI needs to share with DHS, and how does it get shared, and uses the technology to automatically—the rules require that the technology automatically moves information if people have certain levels of authorization to receive it, and then there is an audit that you can build in both with technology and with people to see whether or not that has happened.

And so this committee could, through requiring DHS to create a process for developing the concept of operations for information-sharing between agencies, impact whether or not there are rules in place and automatic tools for auditing and overseeing the implementation of those rules that is much more comprehensive than the committee could touch on by looking into specific instances of information-sharing.

The second thing that I think you could do is create—whether it is through joint hearings or some kind of inquiry into the information-sharing programs of different agencies that are being set up to see to what extent they are being set up under common frameworks that allow sharing between them.

So, for example, you have even just within the Department of Homeland Security the US–VISIT program, which is going to have billions of dollars put behind it, the Homeland Security Information Network, the CAPPS II program, which is struggling to find its way but will and probably has been very costly, even within that agency. But then you also look to the FBI and the development of the FBI's virtual case file and the watchlist information.

And you could have these various programs in front of the committee or the committee could consult and look at the various programs and review them jointly and see whether or not they are being set up to make it possible to even share information between these programs or whether or not the money is being put into stovepipe programs where the information will not get shared as part of a system.

So I would encourage you to think that your most powerful role would be systemic and one which influences the process of information-sharing, rather than an inquiry into specific information and whether it is moved.

Mr. GILMORE. Mr. Chairman, may I just add just sentence or two—

Chairman COX. Yes, Governor Gilmore, please.

Mr. GILMORE. —if I could?

First of all, I concur with Ms. Baird's view that the structural oversight is an appropriate place for the committee to look. But, in a direct answer to Congressman Boehlert's, you do not know what you do not know, but you can know what you want to know.

And that means that you have to have a committee that is steeped in expertise and works with this on a constant basis and understands what you consider to be the appropriate lines of inquiry.

You can know what you want to know because of your expertise. That is the importance of centralization of this thinking into a committee such as the one that we are before here today.

And then through the use of the vehicles that the director and Ms. Baird has talked about, then you can probe as to whether or not what you think is important is, in fact, being submitted to the department.

Chairman COX. Thank you very much. My time has expired.

Mr. Turner?

Mr. TURNER. Thank you, Mr. Chairman.

Ms. Baird, in your report and your statement, you mention what I think is probably the key to accomplishing the things we are not talking about, when you suggest that we need a series of presidential executive orders to carry out the objectives and to establish the guidelines for the agency's collection and use and sharing of information. And Mr. Woolsey raised those issues.

And I think one of our dilemmas is that the whole concept of the collection and use of intelligence has changed, because, as you said, much of the information we need to collect, it is available inter-

nally—our own vulnerabilities in sharing from the private sector, with the government, the ability to take foreign intelligence and limit its accessibility, and yet to be able to share what you can down through the FBI and even into local law enforcement. And we have never had to do that before, in terms of the intelligence community.

So we have a multitude of players. And now, as you see from the chart, we have developed a multitude of federal agencies charged with similar responsibilities.

And as you said, I believe, Mr. Woolsey, your recommendation was to leave the FBI in charge of contacting, working with these local officials, because, as you said, we all know they have done it for years. And yet, the Congress laid the Department of Homeland Security right in there beside them and said that it is your responsibility to communicate with local folks and local agencies.

And in our work on this committee, we see that interplaying already, because DHS is trying to communicate with local officials, and we have briefings from TTIC periodically. And on the same day that we get a briefing from TTIC, I will get a memo in my office in my district in Texas from the FBI telling me something else, something different about the threat that we currently face.

So the key, I think, as you suggested, Ms. Baird, we have to get to the point where the one person who can bring all this together will do it, and that is the president. Because our agencies are going to continue to build stovepipes. In many ways, we mandate some of them to be built. And until we put this on the table, and all the players are told through executive order that this is the system you must build, this system will never be built.

And I really do think that if any members of our committee have not had a chance to hear The Markle Foundation recommendations, that I would urge each of you to ask Ms. Baird to come by and give you a briefing.

Because you have to make the decisions about having a comprehensive, government-wide information collection and dissemination database, with all of the controls that you suggest, and accommodating the concerns that Mr. Woolsey has, and all of our agencies must rely on this single database for the collection and sharing of intelligence. And those in the high-tech community tell me this can be done.

And until we do it, we are going to still stovepipe and, I suspect, spend a whole lot more money, taxpayer money, and not get the job done that we could get done if we had approach it correctly.

And along the way, all these policy decisions about who gets to share what and all those decisions have to be made. And as I understand, your statement of the day, Ms. Baird, those kind of things have to be contained in presidential executive orders as well.

Am I fairly describing the concept that we are both mutually interested in pursuing, Ms. Baird?

Ms. BAIRD. You are, and I thank you for describing it.

And I thank you for the time you took to let us come in and show you a little computer-based visualization of how the system might work. And it would be a real privilege if anyone else would like us

to come by and do that as well. We have done that with the committee staff.

The one thing I might expand on is the issue of, you know, people are a little afraid of databases because of the civil liberties concerns. And we are not talking here, of course, about a single, you know, big super-computer sitting somewhere in the government with all the data in it on everybody in the country.

We are talking about leaving information where it resides but having people pointed to it to find it because of common interests. We are talking about a decentralized system that allows people to communicate directly with each other and to use this, as the congressman has called it, a database—you have not sat where I did, talking about the Poindexter program, so you may not have quite as sharply in mind that sensitivity. But it is a notion of information moving where it needs to get quickly and of people being able to find information.

So instead of having to play a game of Go Fish and sitting at your computer and saying, "Do you have any information on water reservoirs?" and sending that out to a lot of people or doing a Google or Yahoo search, our recommendations envision people having directories that tell them who is working on a problem in government at all levels of government, including state government, where some of our best work is done, at the state and local level.

It is a system where you can find the people who are working on the same problem you are working on and a system where you can get information that has been written on an unclassified basis with the name extracted or the source of the information extracted.

Because the database gives you access to all this information on an unclassified, or sensitive but unclassified, basis that enables you to know where to go to request more information or to dig more deeply.

So I thank you very much for what you have said. I would also emphasize that something like this cannot happen. And we will continue to have unconnected dots in this country and continue to be unable to prevent terrorism if we do not have a common concept of how information gets shared across the government.

The leadership has to come at the federal level. We have in our reports that the leadership has to come from the president.

Forgive me for going on here, but I would make one other comment. Much of the concern about government programs that are really critical—we need to be able to screen airline passengers in some manner; we need to be able to correlate disparate bits of data that, when put together, does indeed tell us something and enables us to be smarter than terrorists.

But much of the problem that has developed with the concerns about what happens to our civil liberties if we create these programs is that there has not been at a politically accountable, at a congressionally accountable level, a statement made of where do we fall in this accommodation of both security and civil liberties. And so you have very well-intended people in government developing programs, but they do not have the policy guidance from the political level.

So that is another reason why it is really critical, in our judgment. And as I say, this is a very broad group of people from every

administration in the last four. We concluded that is critical that the president take the leadership and call for the creation of a network like this and set the guidelines on what are the American values of this kind of system.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Chairman COX. Thank you. The gentleman's time has expired.

The gentlelady from Washington, the vice chairwoman of the full committee, Ms. Dunn, is recognized for eight minutes.

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

I want to ask you to address a broader question, if you would, please. There are several proposals floating around before the Congress right now, all of which are aimed at overhauling the intelligence community.

For example, the chairman of the Intel Committee, Porter Goss, has suggested elevating the DCI and giving him or her a budget authority over the intelligence community. The ranking member, Jane Harman, has proposed developing a new position, a director of national intelligence, to oversee the intelligence community.

If you were to come up with a plan to overhaul the intelligence community and its structure, what would that plan look like?

Mr. GILMORE. Congresswoman, I had a chance to review the two pending statutes that are before you, briefly, last night. And, to race right to it, I think that the real challenge that I would want to focus on is that if you are going to place somebody who is the director of national intelligence that you make sure he has the authority to run the show. If you are going to put the responsibility with him, then the accountability has to rest with him, and that means that he has to have the authority to do the job.

I may not understand the statutes completely, but I had some sense of nervousness that, perhaps, some of the people at the second tier might end up actually with more knowledge and authority than the guy at the top, in which case he is a sitting duck. And I would be concerned about that and ask the Congress to make sure that that does not happen.

I absolutely believe that budgetary authority is called for. In fact, when our commission first recommended a White House organization to develop a national strategy, we thought a central component of that would have been budgetary authority over all the different departments and all the different divisions in order to centralize some authority and power into one place to create that strategic vision. Likewise, I think that that model would work here, as well.

The third piece that concerns me is—and I do not know how, exactly, how you deal with this; I think this is going to require a lot of work, frankly—is what do you do about the Department of Defense, where all the money is and all the power is and all the knowledge is and all the assets are.

And they do not work for the CIA, and they do not work, presumably, for the DNI that would be under proposal here. And they do not work for the DHS either, which is the real challenge of having a separate department that focused on this area that does not have its complete hands around all of the elements and aspects of it.

There are some suggestions in these statutes for some liaisons and some conferral-type of requirements and so on. And I think

that the Congress just has to focus on that exceedingly carefully, in order to figure out how you are going to create that power structure in a way to centralize it at the director of national intelligence, which I think is a good idea.

Mr. WOOLSEY. Congresswoman, the director of central intelligence, in the 1947 statute, as the title suggests, is always supposed to have been head of the intelligence community.

It is just that the community did not really exist in 1947. Not only were there no satellites, there were not any U2s, there was not any Defense Intelligence Agency, there was not any National Reconnaissance Office, there was not any National Geospacial Agency.

And most of the National Security Agency was a collection of military service battlefield signals intercept operations. They had penetrated a very important Soviet code, so occasionally NSA would come up with something and give to the president, or after 1947, I guess, the DCI.

But the community really kind of was the CIA. And people did not think of there being two different jobs here.

As time has gone on, the change in technology, the growth of all these other agencies, the fact that most of them spend most of their focus on matters related directly and immediately to military needs, has produced the situation in which the director of central intelligence is in an odd situation. He is sort of the chief executive officer of the CIA, which is down maybe a sixth or less of the community.

And then with respect to the rest of the community, he is sort of the honorary chairman of the board. He does not have any executive authority in those other companies or agencies. He can kind of set the agenda and he can go out and visit them and he can help them get money sometimes, but he cannot move money around, he cannot move people around.

So, furthermore, his need to respond to the Congress has grown rather. Even in 1993, Congress was in session 195 days, and I had, as DCI, 205 appointments on the Hill that year. I was up here an average of more than once a day. And I think the time requirements of oversight have gone up probably since then.

So I think there are clearly two jobs there now. There is a job for someone who manages the CIA in the same sense that the director of the National Reconnaissance Office manages the NRO. And there is a job for someone who is the overall head of the community and has a lot to do with dealing with the Congress and the like.

I believe that would probably help. That is more along the lines of Congresswoman Harman's approach.

I believe that that would help rationalize some things in the community, because it is very difficult in the current job for there to be a dispute between, say, NSA and the CIA and have the DCI settle it, because NSA, understandably, regards him as in the CIA's camp, not as some neutral overall official.

I rather like the idea that is in Congresswoman Harman's bill of having some substantial aspects of joint authority between the secretary of defense and the DCI. Having a partner whose concerns and yours substantially overlap is not that bad in the Washington

that we are all used to, with all of its rather more solid body-checking checks and balances.

I had two excellent secretaries of defense to work with, Les Aspin and Bill Perry. For meetings that we co-chaired, I had a baseball cap made up with "Chairman" on it. And when I was chairing, I would wear it, and then I would put it on Bill Perry's head, and he would wear it. We would just work together.

It is not a good idea to ignore the fact that DIA—many aspects of the NRO, many aspects of NGA and many aspects of NSA actually are designed now to work closely with combatant commanders. And to put the DCI in as a sort of czar—the word "czar" gets used from time to time about having a director of national intelligence. And my reaction to that is that 500 years of rigidity and stupidity followed by the triumph of Bolshevism is not a good model for the management of the American intelligence community.

Now, I do not like czars. But I think that one could craft the statute—and I think Congresswoman Harman's is close—that has some important dual responsibilities, so that the DCI or DNI has more than he or she has now, a partnership is forced between Defense and that office, and the management of the CIA and its espionage and its analysis as an agency is separated out.

One final point: I would keep the title of the overall person who is responsible for the community DCI, director of central intelligence. That is what it always was supposed to be. You can come up with a new title for the director of the Central Intelligence Agency out at Langley. Put the DCI, the overall head, somewhere downtown, hopefully in the Executive Office Building, and give him or her responsibility as a partner with the secretary of defense for overall resources and personnel and management of the community.

Chairman COX. Yes, of course.

Ms. BAIRD. I would comment briefly that I think the members of our task force, many of whom have testified on these issues of the DCI or an MI–5 would nevertheless take the position that the most important thing Congress needs to do is what Congressman Turner was describing, the development of an information-sharing across both the domestic and foreign intelligence capabilities and the military and state and local.

And regardless of how you come out on the structural reforms that are needed, on the structural reforms, we are actually looking now in the next phase of our work at this issue of the line at the border and how information can be collected, both internationally and domestically, and shared in a way that is most effective.

And I think the Congress will find that if it looks separately at a DNI or DCI and separately at an MI–5, as opposed to looking at the whole system, that you will be living in the last generation as opposed to the next generation, and that Congress will need to look at whether or not you maintain a separate foreign and domestic intelligence for good reasons, where are the areas where we cannot keep them separate. I mean, for example, just looking at airline passenger screening, which this committee has certainly been very close to, there is a question of whether we can treat our citizens and U.S. nationals differently than the way we treat people coming in from Europe and others.

And these are new questions that we have to deal with. And will we forever be able to collect foreign intelligence without any of the rules that we have applied in collecting domestic intelligence, or will other countries expect that there will be some extraterritoriality of our civil liberties? So these are things that we are going to have to grapple with.

Thank you. Thank you, Chairman.

Chairman COX. The gentleman from Washington, Mr. Dicks, is recognized for eight minutes.

Mr. DICKS. Thank you all, and I appreciate all of your good work and statements.

And, Jim, good to see you again.

Ms. Baird, I have not had your briefing yet, but I am looking forward to it.

You know, I was on the Intelligence Committee for eight years and ranking for four years. And there is this whole concept of stovepipes and how do you share information. The examples I have seen where I really think you saw great sharing of information are the joint intelligence centers, which are set up when we are in a military conflict. We had one in Kosovo. We have one in Iraq. In fact, I think we visited it when we were there.

It is in that concept where I think the best work is done. And when we are in a military operation, your national technical means come right into this center. HUMINT is brought in. You have a relationship with your allies. And it all comes together in one place. The military then can get a good picture of what is happening and make their decisions.

It has always seemed to me if we could replicate that, where you have at the federal level people from the NSA, people from the CIA, kind of an overall center where information is shared.

I like the idea of trying to share the information. I realize that what Jim Woolsey says about the restrictions on layers on information is going to be a problem. That will not be in the database, and should not be, I do not think.

But I like the idea of trying to bring people together and share information at some level in order to make decisions.

I completely agree with what Jim said about the information is going to come, I think, from the bottom up. I mean, the information that is important, as it did before 9/11—again, the information was there. We just did not act on it.

This is one of the lessons I learned from my eight years on the Intelligence Committee. In situation after situation, we had the information. We just did not have the ability to act on it.

You can share all the information you want, but if somebody does not take the initiative and say, "Wait a minute, this is a serious matter that deserves to be given higher attention." I worry that you are still going to have a problem with a lot of data coming in, but who is going to make the decision and take the initiative to do something about it?

Those reports that came in from the FBI field offices about these people training and that not being acted on is one of the greatest, I mean, to me, one of the most shocking failures that we had. And it was right there in the FBI, the New York office. It did not happen.

The same thing happened in Desert Storm, Desert Shield. You know, all the information was there from the intelligence community, and yet we relied on government leaders in the area. And they convinced the president that somehow this was not going to happen. And we could not even get the deputies group back to make decisions.

Again, I want to just focus on this one point. How do we improve that? Another thing that worries me, too. In talking to my people in the state of Washington, National Guard General Lowenberg for one, I do not get the feeling that there is the sharing of information between the federal and state level, mostly from the feds to the state. If you are going to try to encourage this sharing of information, you have to get the locals.

And I agree, I think the FBI has the relationships locally to be able to work best with the local officials to get information and bring it back to the federal level.

But how do we encourage that? How do we improve that relationship, which is just getting started now between the locals and the feds? Because that has not been there in the past. There has not been a lot—except at the FBI level, but with maybe FEMA or other agencies like that.

But in terms of gathering information that is going to be important, how do we nurture that?

Jim, do you want to take a crack at that?

Mr. WOOLSEY. Well, quickly, everybody cannot do everything. And Homeland Security strikes me as being in a situation, with a lot of exceptions to this analogy, somewhat similar to the State Department. It is a customer for intelligence, but it is also a customer that is involved in implementing the policies that come out of the intelligence, and it is a customer that does some analysis itself.

The State Department does a lot of intelligence analysis itself in the Bureau of Intelligence and Research, a small, very effective organization, 100 or so analysts, and they do a very good job on a lot of things.

It is intimately involved in implementing the results of deliberations about intelligence, but it is not principally in the business of stealing secretes. It collects intelligence, it collects information, through diplomats talking to people overtly. But the CIA is who steals secrets and operates covertly.

On the domestic side of things, it seems to me that the institutions that are collecting intelligence, in the sense of secrets that people want to hide, probably are going to be the FBI working with, as I said in a statement, state and local police.

Because it is the local policemen on the beat whom the merchant has enough confidence to say, "You know, there are these four young guys just in from Afghanistan or someplace, and they are acting kind of strange. You might want to keep an eye on them down at the corner." The local police have a better feel for how to get information like that without intruding on people's civil liberties, and building up confidence of their community and so forth, than anybody else.

So I would see, in a very different kind of way, the FBI and the local police being the people who obtain information that some people may want to hide.

Homeland Security is a consumer. It also does analysis. It also is involved in implementing decisions that are going to be made about pulling people together to do X or do Y, in somewhat the same way the State Department is.

That is the genius of this chart, Congressman, is it sort of suggests that everybody is trying to do everything. And I do not think the system is going to work if everybody tries to do everything.

Ms. BAIRD. Congressman, if I could comment and pick up on your use of the example of the Phoenix memo from the FBI agent who was concerned and thought someone ought to look at the issue of a foreign national taking flight lessons.

And the kind of network that our group envisions is one where that Phoenix agent would not have to send that up the chain and take someone's time to give them authority to say, "Yes, it is important enough to follow up on your hunch." But instead, that agent would be able to find other people who were looking at people who were taking flight lessons or who have expressed concern about foreign nationals going to flight schools in the U.S.

So that Phoenix agent would have found the Minneapolis agent and would have found perhaps a local police report from a local flight school in Seattle or Florida, talking about people taking lessons without caring about taking off or landing.

And those people could create an informal group who work on the issue, who themselves, because of their own instincts and their own judgment, believe there is something to be worked on.

Now, should they have access to data on individuals where there is no suggestion that they are involved in terrorism? Of course not. But those are the running rules of the system. You can protect civil liberties and make sure that a lot of local people do not get out of hand simply because they have access to information in the network.

But I do not believe that you will ever get the kind of problem that you are talking about solved, if it always has to be hierarchical, as this chart suggests we structure government, where we have lots of boxes and you have to go get authority to do this and that. Instead, what—

Mr. DICKS. Ultimately, somebody has to take action.

Ms. BAIRD. Yes, indeed. But when the information—

Mr. DICKS. Share a lot of information, but until we find somebody who is going to be smart enough to say, "There is a problem here, we had better do something,"—

Ms. BAIRD. Right.

Mr. DICKS. —which did not happen at the FBI.

Ms. BAIRD. But they are more likely to see it in a way where the risk is clear, if it is not just one guy writing a memo about one person going to flight school—

Mr. DICKS. Yes.

Ms. BAIRD. —but if, instead, that whole team comes together, and they have identified the pattern because they care about it.

In terms of communicating with state and local actors, they ought to be part of that system, because they may see something. They may, you know, have brought in some people for some unrelated charge and learned something in that context.

Or if you are talking about bioweapons, the local agricultural inspectors may see things that are funny. We show in our demonstration—Congressman Turner probably cannot forget it—the image of a particular virus on the snout of a hog, which a local agricultural inspector would be the first to see, not someone in Washington who is looking for what the next bioweapon might be.

So that kind of respect for the potential perspectives of local people is something that is really important to focus on.

Mr. GILMORE. Mr. Dicks, if I could add something. We certainly concur that you have to find the proper structures for information-sharing. That is why we recommended the fusion center, the TTIC.

But one thing about our commission, it has been a strong advocate for state and local people, people who are out there walking the beat, people who are working at all levels of government.

The real danger that we have always had is that things are just so federal-centric. And while I certainly concur with the Markle commission, that we need to get away from a federal-centric type of approach—that was the heart of our commission—I would be a little more cautious about the decentralization idea. I think that has to be very carefully constructed.

But the point is this: We have to find a way to get information going up and down the line. We see it centrally as a culture problem—a culture problem. An unwillingness, particularly for federal authorities, to share information or even to seek information. And yet, state and local people are often going to have that information. We have to put a structure into place that encourages that cooperation.

Frankly, the FBI has not always done all that well. I was an elected prosecutor for six years, and the interaction with the federal was not particularly strong. But on the other hand, FEMA is a model for working together between federal, state and local people.

So I think it is a cultural issue. We have to get away from our federal arrogance that says that all knowledge and all assets and all residue of wisdom is located in the federal government, when the truth is that that wisdom will be enhanced by a partnership between federal, state and local people in an appropriate system.

Chairman COX. Thank you for your responses. The gentleman's time has expired.

The gentleman from Pennsylvania, Mr. Weldon, is recognized for eight minutes.

Mr. WELDON. Mr. Chairman, thank you.

And I just want to say that the last comment by Governor Gilmore I agree with totally. It has to be a partnership with the first-responder community locally. And he said that repeatedly in the Gilmore commission reports.

And, Mr. Chairman, as you know, my perspective is coming at the local level. And let me say, first of all, we have some very successful programs that are operating.

If our colleagues have not received the JRIES brief, they need to get it, because that program, which was stood up on March the 7th of 2003, has become an outstanding model, very aggressively supported by the law enforcement community. It was prototyped in New York and southern California, and now it has been made

available around the country. They have just linked up our law enforcement communities in Pennsylvania.

There is a two-way capability of information-sharing. There is a protected classification of data, where it does not have to go to the full level of being classified, but yet it is sensitive.

And it is working. Our law enforcement community is, in fact, receiving information, they are providing information. When I met with them and went to their national conferences, and I have been to two of them, they gave instances where one municipality in Louisiana is sharing information about impending threats that may have use for law enforcement departments in California or other states on the other side of the country.

So there is a successful process under way, actually established originally by the Defense Department, but then supported by the Justice Department, that I think is working. And I think it is working well, and we should build on that, and that, for law enforcement, I think, is doing a good job.

In the case of the first responder from the fire and EMS standpoint, they do not need that kind of capability. And I say that as a former fire chief, representing the firefighters in the counry.

They need information to know where to go to get resources. When Chief Morris arrived on the scene of the Murrah Building bombing in Oklahoma City, he did not need to know where the next threat was coming from, but he needed to know where he could go to get structural engineers, because he had an eight-story high-rise federal building with a day care in the bottom, that proposed a life-safety risk.

He needed to know where to get engineers to deal with the structural integrity of the complex while he was rescuing people.

That is why the Homeland Security agency needs to have a resource capability where the first-responder command officer can know where to go to get help form the federal government.

I remember, as I have said in this committee in the past, walking the freeway when it was collapsed at the Northridge earthquake, with the fire chiefs of San Francisco and Oakland, they were looking for people that were trapped inside their vehicles in between the two layers of the concrete structure that had collapsed on top of itself. And they were using dogs. And the dogs could not get down into the crevices of the sandwiched freeways to see whether or not there were people alive.

And I said to them, "Why aren't you using thermal imagers," which were a technology we developed for the military 15 years earlier that detect body heat used on our naval ships. And the two fire chiefs of Oakland and San Francisco said, "What are thermal imagers?" They had no idea that their tax money had been used to develop this technology.

So there needs to be a resource capability for a local emergency responder leader to know where to go quickly to get information and technology to assist him or her in dealing with that. That is a separate capability of information. It does not involve intelligence, but it involves resources.

And there is a third need, and members on both sides now have addressed this repeatedly, and that is the need for an interoperable communication system. The Gilmore commission has referred to

this. It has been a major priority of the fire service. APCO has called for this consistently at its national level for the past three years.

We still do not have a nationwide integrated emergency communication system, as we do in the military. Governor Ridge understands that. He is addressing that with more money. And members on both sides of the aisle have called for additional funding. And I think that should be a top priority of ours.

So I think we are making good progress. And I do not think we have to throw everything out the window. I think we should, first of all, understand fully what is available.

What I do want to focus on, again, gets back to my original concern at the beginning of this hearing. And that is what I think is the ultimate purpose of information-sharing for intelligence purposes, and also the sensitivity of the military having to be able to defend our information systems against the threat of cyberattack.

It is no secret the Chinese have stood up a fourth wing of their military specifically to focus on cyberwarfare and ways to bring down our capability to respond to our threats and perhaps to disrupt our information capability here in America.

And so, in anything that we do, whether its classified or unclassified, we have to take into consideration the security of those information networks.

But in the case of data fusion—and I want to ask you this question, Mr. Woolsey, because you were the CIA director in a previous life.

As far back as 1999, when the military was first developing the concept of data fusion for intelligence purposes, and when both the Navy's system, the Air Force's program and, more importantly, the Army system down at Fort Belvoir, the LIWA facility, the Land Information Warfare Assessment Center, was creating models that were supported by the private sector, companies like Northrup Grumman right on the cutting edge of this back in the late 1990s.

And when the Congress specifically called and offered to provide the funding, as John Hamre said—he was deputy secretary of defense—to pay for this capability, the CIA and the FBI said, "We do not need it. We do not need that capability." And I documented that in a meeting that was held with all three agencies on November the 4th of 1999.

We put language in the defense bill. They still did not come around.

A new administration came in. In fact, if you read the statement of General Downing when he resigned from the White House on June the 27th of 2002, one of the reasons he said he had resigned was because he spent much of his time at the White House struggling with a variety of federal offices to create a data fusion center that would keep a 24-hour watch on all interagency intelligence on terrorism activities.

It was not until four years after we first proposed the idea, long before 9/11, of creating a data fusion capability. And I gave you a copy and put it in the record, the brief for the NOA.

The NOA is exactly what the TTIC is. There is no difference. I mean, there is no difference.

So why would the CIA and the FBI in 1999, in 2000, in 2002, in 2002 object to a capability? It is finally in the State of the Union speech; in January of 2003, President Bush announced the creation of the TTIC. Why? Because I think that relates to our ability to continue to provide that integrated data to allow us to understand emerging threats.

So, Mr. Former CIA Director, give us your insights into what the real reasons are.

Mr. WOOLSEY. My first insight is, I am glad I resigned in January of 1995.

[Laughter.]

But I think that the cultures of both the CIA and the FBI are ones that have produced, in a number of circumstances, great successes for the country, but they are very specific cultures. And neither one is particularly oriented toward sharing data or information.

The CIA culture is really, I think, driven in many ways by the clandestine service. It is one in which the more important what you are doing is, the fewer people are going to know about it.

And you spend a lot of time cultivating an asset, obtaining something from him or her. And ideally you treasure it, and the director of operations knows about it, and the DCI knows about it, but it is so important almost nobody else, except the president, does. And that is success.

For the FBI agent, generally speaking, I think success is bravely kicking down a door and grabbing one of the 10 most wanted and helping a prosecutor get him put away for life. And it is participating in investigation to that end.

And the people who do those things do, I say again, in many circumstances great things for the country.

Neither one of those cultures is particularly oriented to saying, "Hey, let's have a data fusion center in which everybody gets to know what I have come up with and what I am doing." I mean, it is just sort of oil and water.

And so, what one needs to do is find ways—and that is sort of what my remarks were focused on—that we can encourage the system to share what needs to be shared in a way that does not compromise things like sources and methods and counterintelligence information and the rest, and leads both of those fine institutions into an amended version of their cultures, not one that rejects it, but an amended version.

And it takes time, it takes effort, it takes leadership, it takes cooperation between the Congress and the heads of the CIA and the FBI. And it is not going to happen fast, because one is really kind of swimming against the stream.

But we do not want to throw out those two cultures as we are doing it, because in other times and circumstances what they do is extremely valuable and useful.

Ms. BAIRD. The proposal that you have raised, I will be very interested in reading and interested in seeing whether it has some solutions for some of the problems that TTIC is facing.

TTIC, I think, has actually started up very effectively and has moved quite quickly to improve the fusion of information from different agencies. Unfortunately, most people at TTIC still do not

have access to the data from other agencies, other than their own, and it is very few people who are those fusion agents, if you will, who bring the information together.

And I think it is important, and as you look at this further, perhaps you have some recommendations on how the agencies can be putting information into their own systems that are written to share.

The FBI is, for example, making some very good progress in their new intelligence guidelines. They have taken the position that the FBI should write to share, not write to classify; that the information should be considered a share by rule and withhold by exception, which is a complete flipping of anything the FBI has done before, let alone any of the other agencies.

And the CIA and intelligence community is, similarly, looking hard at those issues, but a culture of classification is pretty deep there.

We are recommending a culture of authorization, if you will, which moves from the ownership and control and classification and the withholding of information, as Jim described it, for different institutional reasons, to one of writing to share and withholding of critical elements of information.

But those centers, TTIC or presumably the one that you recommended, have a very important role to play. It does not bother me that there might be some redundancy, that there might be more than one of those fusion centers, because not everybody is going to see everything.

But I also think we cannot fall into thinking that those are the only places where the dots can be connected. And connecting them with local people who are worrying about Chicago or their bridge, as Jim was talking about, is also very important.

Mr. GILMORE. Congressman Weldon, I would say this. I liked the description that Mr. Woolsey gave of the role of the CIA and the FBI. Earlier, I was actually, frankly, shocked to hear that the CIA stole secrets. I did not think we read each other's mail.

But with respect to the description, I think that is right, but I think that today's challenges require multidimensional approaches. It requires a recognition that more functions than that have to be done. And the challenge, I think, of leadership and indeed statesmanship is to provide clear direction from the Congress, that there is a recognition that there are more functions than that, in order to meet the challenge that we are facing today and we will face for other challenges and threats in the future.

So he or she will have to meet that challenge, and I think that the direction of the Congress from a committee like this one will help a great deal.

Chairman COX. The gentleman's time has expired.

The gentlelady from New York, Ms. Lowey, is recognized for eight minutes.

Mrs. LOWEY. Thank you, Mr. Chairman. And I want to thank you and the ranking member for holding these series of meetings.

And I want to thank all of our expert witnesses today.

I must say, as a congresswoman, or if I were one of the laymen sitting in the audience—though there may be many people in the audience who have great expertise—I would take a deep breath

and say, "Well, it is a good thing we have a lot of luck," that it is almost three years after 9/11, and with all the wisdom and the commissions and the foundations and the committees who are focusing on this, I just wonder if we will be sitting here three years from now debating the same concerns.

And I say that seriously, because you all present very serious issues. And I did not even mention our Intelligence Committee and those such as Ms. Harman and Mr. Goss, who are putting together and have put together very serious proposals.

And I also found it interesting, Ms. Baird, your presentation, as the others, was so very informative. And yet, when you began your remarks about a half hour ago, you said you are taking a contrarian position. Frankly, it sounds to me like common sense, what you are proposing.

And so, as a member of Congress, I just wonder, and my colleagues have been asking the same question—I am not quite sure who to address it—how do we move this along?

You are talking about a presidential directive. We see GAO reports that say 35 percent of local first responders do not feel that there is adequate connections to the federal government information. And we wonder, well, how do we improve on that quickly and not take another year, another two?

And I say that not to be impatient, but we have had such wisdom, we have had such good testimony, we have had so many good reports, you just wonder how you move the process.

And then I worry, and I think it was on March 25, 2004, the director of the FBI's terrorist screening center, Donna Bucella, told us that the complete screening and watch list database is not available. We know that. She said it would be fully operational at the end of the year. I will not hold my breath until that happens because of all the limits you mention on that.

So I really am asking a general question again. My colleague, Mr. Dicks, asked so many good questions. My colleague, Mr. Weldon, mentioned that he was focused on this issue in, what, was in 1997 or 1998?

I happen to come from New York. We lost hundreds of constituents in the World Trade Center. We are very aware of the issue of interoperability. In fact, I think it was about six months ago, maybe a year ago, Mr. Chairman, the person who is responsible for sending federal standards out in an RFP said perhaps it would go out in six months. I should ask you if it has gone out. I do not think anyone I know has received it.

So many of our local communities, being so close to New York, are buying their own equipment. And I am trying to put in place a bill which I have introduced that would reimburse those local communities, among other things, have a special area just focused on interoperability in the Department of Homeland Security, so we can work with these communities, who, frankly, are doing their own things because they have not got any directive from the federal government.

So I am not sure who I want to address this sense of frustration to all of you, but to speak for the average citizen, who, frankly, in my community, is in a state of, shall we say modestly, real concern, real anxiety, worried about the future, should we just say that this

is the greatest country in the world and we have had some good things happen and we will just muddle through, and with a lot of luck, maybe we will not have a 9/11 for another three years?

Maybe Mr. Woolsey. If you see that there is something integral to the departments of FBI and CIA that you think is an anathema to really having one list, how do we get past that?

One other point, and then I really want to hear from you.

When I am on an airplane, I know that someone is having to check with all these lists, and someone falling through the cracks is a real probability. And this is another area. I know that people who work at these airports, whether it is McDonald's, whether they are food handlers, still are not going through security, as I am.

The government move so slowly, and that is the nature of the beast. How do we get just that one thing done? Perhaps it is The Markle Foundation's recommendations or the Gilmore commission. How do we ensure that if I am getting on an airplane or a constituent is getting on an airplane that, even though there may be eight lists or 10 lists or 12 lists, we are going to catch that guy and stop that guy if you do not feel realistically they are going to be able to merge the lists?

Mr. WOOLSEY. Congresswoman, I do not think that cooperation is—I would not go so far as to say it is an anathema to the bureau or the agency. It is that, for important parts of what they have done in the past, keeping things very close to the vest has worked for them.

And as long as what one is doing is prosecuting individual crimes of fraud or kidnapping or whatever for the FBI, and one is recruiting specific KGB officers, the sort of behavior I described is perfectly reasonable behavior.

The problem is that we are in a new world.

Mrs. LOWEY. Right.

Mr. WOOLSEY. And it is a world in which one is going to have to be creative about the way one extracts information that has been stolen either by the CIA overseas or given from an intelligence liaison service, a foreign service, or obtained by my hypothetical patrolman on the beat from a grocer on the corner.

One is going to have to find out a way to get that out and have people be able to have access to it in a way that the governor and Ms. Baird have suggested.

Some of the things we do and have done in the historic intelligence communities are, for example, called terror lines. In a classified document, we will have something—not a lot, often—but something about the source of intelligence, because it is almost always the case that you you can do a better job of making a judgment about intelligence the more you know about the source.

That is why the president's daily brief is so important. We are completely candid about sources in the president's daily brief, whereas the material that goes out to hundreds or, in this government, thousands of people will be very vague, often, about sources.

If you have nothing about a source, sometimes you can get information out and someone, let's say, with a secret level security clearance in the police office, NYPD, may not be able to make as good a judgment about how valid that is. But if he is told, "We have a serious threat of such and such a type in New York over

the course of the next two weeks," and he does not know anything about the source because it has just come to him below a tear line, still he can do a lot if the information is useful to him and it is something that he can act on.

That is the kind of thing, I take it, that we are talking about trying to do with the networks that The Markle Foundation has talked about and, in a slightly different context, the Gilmore commission has talked about.

But people who are consumers of intelligence are perpetually demanding to know more and more about sources and methods. It is just very frustrating to be told, "Listen, all I can tell you is you got a serious risk to the bridges of New York over the course of the next two weeks." Well, why do you say that? Why should I believe that? I mean, if you are a normal person, you ask that question. And the answer for large numbers of people is going to have to be, "I am sorry. We cannot go into that."

So if you can set up a system where the substance is largely, almost entirely—best of all, entirely—extracted from sources and methods and separated from it, I think a lot of this can be done in a useful and interesting way.

But it will be a constant struggle, not only with people in the NYPD, but in the Department of State and elsewhere. People always want to know more about source and methods. And for widely disseminated information, they are just going to have to be told "sorry."

Ms. BAIRD. Yes, I share the frustration of your constituents, wondering why it is we cannot do this better.

The answer, though, is not to have one commandant telling every agency what to do and making them march to the same drum. The diversity of America is its great strength.

But the answer is having a common vision. And we have recommended that common vision be set in a presidential directive. And we have also said though that, that common vision could be set by DHS.

With an inter-agency and a public/private process, this committee could play a real role if it wanted to give everyone a vision to march to that is a common vision. So that when we invest in that local communication it not only is interoperable between police and firemen, but it in fact is interoperable with a larger system, because we cannot predict who they will need to talk to tomorrow—they may need someone at the CDC, they may need someone who is an expert on bioterrorism at a university.

The other aspect of that is that, by having some kind of common vision, we can use a sort tear-line system, a system of stripping out sources and methods, but, nevertheless, give people common rating tools.

So instead of asking the name of a source in order to find out if the source is very good, you can have an eBay-like or an Amazon-like rating button on the information, where the originator of it says, "This is urgent," "This is of high value," "This is a reliable source."

And then everybody in the network can rate the rater. If he is not really good, if he puffs, you know, his own source, promotes his own sources, but nobody else has found the information useful, you

could have a second button which says, you known, "This guy is not to be trusted as someone who is putting the information from our government into the system."

So there are a lot of tools we can use that are used every day by your constituents in their own homes, in their own small businesses, not just big companies. And our government needs to get as smart as our people are and use those tools.

Mr. GILMORE. Well, I will add something to that. I think that the danger at the local and state level is that information is gained because of the superior assets at the federal level, and the state police and the local police never know anything about it at all.

The feds do not trust the states and locals. They are afraid to give them anything. There have, in fact, been some examples, as a matter of fact, where unfortunate governors have made public statements they should not have made based on federal information, which then makes the feds even more suspicious.

The answer, it seem to me, is the setting up of an appropriate structure to share information, to create a culture that places trust, whether you have a hierarchal ability to deal with that, which, frankly, I prefer, because I think that it gains more accountability, or a decentralized type of approach, which I think would have to be scrutinized to make sure there is appropriate accountability. No matter what it is, you have to have some willingness to actually do it.

And the problem here is that I think you have to go to a system that calls a clear idea of what you are doing, and then training.

Remember that in, I think, yesterday's paper, there was an example that someone in American Online has been accused of getting access to information then selling that out. Well, they have been charged with a crime, a crime, under the statute.

And, indeed, if someone is going to give information to a state or local official properly cleared, who has a need to know, and then they turn around and misuse the information or spill it out, you would do with them what you would do with Hanssen or some with other person, the FBI or CIA, you prosecute them.

And you train people to understand that that is going to be the rules of the game. And I think that opens the key to, at that point, actually diffuse information so you take advantage of all of the aspects of information and intelligence-sharing in this society.

Mrs. LOWEY. Thank you, Mr. Chairman.

I hope we can gather next year.

Chairman COX. I thank the gentlelady.

I thank the witnesses for their answers.

The time has expired.

The gentleman from Nevada is recognized for, how many minutes? Eight minutes.

Mr. GIBBONS. Thank you, Mr. Chairman.

And to each of our witnesses today, thank you for your appearance here today. Your testimony has been enlightening. It has been valuable to us, in terms of our discussion and our effort to make heads and tails of what we have before us. So we appreciate that greatly.

Chairman COX. I wonder if the gentleman would yield just for a brief announcement.

The committee has scheduled a briefing that begins at 1 o'clock. The witnesses have asked us that they be excused by 12:45. We have three members who want to ask questions. And that should just about work if everybody, including our witnesses, is compact in their answers and questions.

Thank you.

Mr. GIBBONS. Well, Mr. Chairman, in that vein, I will try to ask just three very simple, direct questions, one to each of the witnesses so perhaps we will not have to belabor this process much longer, especially for them. They have been here very patiently.

That said, perhaps I should direct my first question to Director Woolsey.

I mean, listening to your comments about the reorganization proposals of the CIA and whether this is going to end up in a structural change with a new head of the national director of intelligence or perhaps just a simple, new and improved DCI, which ever that process is, that individual will end up inheriting what I see as a vast array of intelligence fusion centers and analytical centers, feeding information to and receiving information from various organizations.

And my question would be, is it better to have the hub-and-spoke system, where we have something like the TTIC today at the hub, or should we have a centralized single agency responsible for sharing information to first responders and other agencies? What is your suggestion?

Mr. WOOLSEY. Congressman, the dilemma about intelligence is that, for some things, you want centralization and, other things, you want competition.

The reason we have a U–2 and satellites and a lot of other things is because different parts of the CIA and the Defense Department historically, in a sense, competed against one another to come up with new approaches toward collection. And the richness of the intelligence where it is available to us is, in part, because things were not centrally directed.

Also, in analysis, it is a good idea to have more than one set of eyes on a problem and to have people come at things from a somewhat different perspective. The Bureau of Intelligence and Research at the State Department, as I mentioned before, sometimes has a different point of view than other parts of the intelligence community. And they have done a good job of presenting that view. Sometimes they are right, sometimes they are wrong. But DCIs and presidents and secretaries of state are well served by having that disagreement.

What you do not want competition in is organizing things, pulling them together, making sure the right people are informed, making sure the judgments are made properly about need-to-know access and having sort of one system for pulling things together instead of lots.

Mr. GIBBONS. So, to analyze it quickly, because I want to the other three questions here, and I hate to interrupt you, and I understand basically.

What you are saying is the hub-and-spoke system that we have today, with the multiple series of fusion centers and intelligence

and analytic centers feeding into a central organization, is probably the most efficient way to deal with intelligence?

Mr. WOOLSEY. I am relaxed about multiple sources of intelligence and multiple folks doing analysis. I am not real happy about the idea of having multiple fusion centers.

Mr. GIBBONS. Okay.

Let me jump over to Ms. Baird, because the Markle report or the Markle Foundation's report has urged the creation of system-wide homeland analysis exchange—SHARE, I think that is what you call it—available from commercial vendors of software.

My question is, knowing of course, what we have just seen with AOL, the insider that sold inside information, knowing Hanssen was an insider in the FBI who was in charge of counterintelligence, knowing people like Aldrich Ames, et cetera, in the CIA were insiders, and the complexity and the size and the importance of the information that would be lumped into a common system sharing this information, my concern is the security with this. And you heard Mr. Weldon talk at length about the security of our cyber systems.

How do you assure us that a proposal of this nature, with the value and the sensitivity of the information that is in there, would be secure?

Ms. BAIRD. Well, certainly, I would agree that the insider is the biggest risk, in fact.

The system that we proposed does allow people to withhold certain most critical information from a system like this and only let it be known that they have something. So a source of information that you do not want somebody to be able to tap into, that kind of thing, can be withheld.

The potential, though, for use of aggressive audit processes, aggressive tracking of whether it is only authorized people who are using information, the inability to pass information—that can be done with technology to prohibit others from passing it along or prohibit if from being printed out, these kinds of things can go a long way, with the kind of security and encryption technology that is used in the private sector can—and some, well, by government, the Defense Department and others—can go a long way to providing security.

But I would say that it is a combination of making sure you get there fast, if somebody is misusing information, and of keeping certain kinds of information out of the system.

But we do believe that the overall balance favors this kind of management of shared information and that we can be very, very good at protecting ourselves from people trying to abuse the system and not protect ourselves from terrorists.

Mr. GIBBONS. Mr. Gilmore, finally, let me say that one of the recommendations of the earlier commission that you served on recommended that we develop domestic intelligence agencies, something like MI–5. And I just want to get your opinion.

Is it sufficient to have the FBI and the Department of Homeland Security coordinating closely to protect the homeland security, as we do today? Or do we really need an MI–5?

Because those of us like myself are vastly concerned about the implications of having a domestic government organization spying on Americans.

So I want to know, you know, your ideas. Should we merge or is there a need to merge these functions into a single agency?

Mr. GILMORE. We argued over this for virtually a year, in year four of our five-year commission, in the year 2002. And, again, there was a certain line of thinking, led by Jerry Bremer, of the commission that basically said, "Look, security is everything here. We have to go to something that is not a law enforcement model." And that actually ended up prevailing as our recommendation to the Congress.

Again, my view and that of one or two others on the commission was that the FBI is the better approach. They are properly deployed. They, by virtue of their activity with law enforcement, they understand what the constitution is, what the law is, and the fact that it applies within the domestic homeland. So that is the essence of the discussion that we had.

I think that our commission has devoted continuously, and up until the final report, a serious concern about the risk to civil freedoms and the country as a result of an obsessive overreaction, a hysterical reaction, at this moment in time in our history. We are concerned about it, and that is why I think that the bureau should be forced to do it, should be required to do it, and should be carefully overseen by this committee and other committees and that be demanded in that way.

But what is the thinking behind MI–5? The thinking was that a law enforcement organization is not suitable, that an intelligent organization is suitable. And since we do not have one really domestically, the FBI is fundamentally and culturally a law enforcement organization, that we should go to an MI–5.

I believe you will find that the discussions of our commission for that year should properly advise the Congress of the different elements so you make a decision as to the appropriate approach. I hope that is responsive.

Mr. GIBBONS. Very responsive. Thank you very much.

And to each of you, thank you again.

Mr. Chairman, thank you.

Chairman COX. Thank you, gentlemen.

Mr. Langevin is recognized for five minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman and Ranking Member. I want to thank you for organizing this hearing.

And I want to thank our witnesses for being here today. Your testimony has been extraordinarily helpful.

I probably want to pursue, I guess, a little bit more, in the line of questioning that Mr. Gibbons had begun. And we have talked really about, you know, three different things here: the director of national intelligence, whether it is DCI or DNI; we have also spoken about getting greater information-sharing cooperation among the various intelligence agencies; and then we have talked about the communication and information-sharing with our first responders.

What I would like to do, if I could, just—we do not have time to get to probably all of those—starting with a DNI. We have gotten

kind of a broad outline, but more of a, I guess, it is more meat on the bones.

Can you tell me, how do you envision this working, if we were to have a DCI, DNI, so that it is not just ceremonial? You described it, Mr. Woolsey, as, you know, honorary chairman of the board, as it exists right now. How do we not replicate that? Does this person have budgetary authority? Do the various heads of the intelligence agencies answer to the DCI?

And on that, sir, I would like some more information on that point.

But also on getting the various intelligence agencies to work more closely together. Mr. Gilmore, you hit it on the head, that this is largely a cultural problem, the hurdle that we need to overcome.

And coming from a public administration background, I know how difficult that way is. You either have to replace the people that are there, which I am not advocating at all, or you have to somehow get the people to buy into seeing the value in working together, in changing the culture themselves, being a part of that change.

Is it time for an MI–5 model? Some of our Special Forces, in a sense, work that way. They come from, you know, Army, Air Force, Marines, but the insignias are basically stripped off from where they come from, the various branches of the military, and they work for one purpose.

So why not that type of a model? We have obviously the CIA, we have the intelligence branch within the FBI, we have air force intelligence, army intelligence, naval intelligence.

Should we not have these individuals as part of one intelligence branch, maybe working in different sectors, but budgetary authority and all that is essentially located in one agency?

So, if you could try to handle those, I would appreciate it.

Mr. WOOLSEY. Just a few words on the DCI–DNI one. I referred earlier to Congresswoman Harman's bill. The one aspect of it I did not favor was that it had the undersecretary of defense for intelligence being the deputy to the overall head of the community. And that would, I think, give the Defense Department and that individual too much power, because he then has two bosses, in a sense. And if you have two bosses, I am not sure that you have one at all.

I was once nominally the boss of Hyman G. Rickover when I was undersecretary of the Navy. And one important thing about Admiral Rickover was that he also had a position in the Department of Energy and he also had a lot of support on the Hill, so he really did not have a boss. And I do not think that the notion of having two bosses for the number-two person in this structure is a good idea.

But other than that, I like her bill because using terms and words of correlative authority and associate appointments and the like, what she tries to do essentially is force a partnership between the secretary of defense and the new DNI or DCI, the overall head of the community, on such matters as money and personnel. And those are the two hearts of the matter.

The DCI today cannot hire and fire the head of the NSA, and he cannot move money from NSA into the NRO or vice versa. He can

ask, but that is it. This gives him or her more authority in that direction than he or she has now, but it does not make him the overall head of the community, to the exclusion of the interests of the secretary of defense.

I think that is about as well as one can do under the current interlocking responsibilities that much of the intelligence community has for working directly for combatant commanders, as well as working on more national and civilian objectives.

And on the other aspects of your question, I will let my colleagues answer.

Mr. GILMORE. Congressman, I think I would concur that an overall director of central intelligence or a director of national intelligence is a good idea, to begin to bring these things together.

You can certainly have a much more formalized ability to work with the defense establishment coming into that kind of a structure. I believe he should have budgetary authority, and I think he should have some personnel authority.

I think that this dual-boss problem is a central one that the Congress is going to have to wrestle with. Maybe a construct that tries to draw a distinction between intelligence operations, such as the one I was involved with when I was in the service, in support of military organizations engaged in military activities or preparations for that; more tactical intelligence is one thing and more strategic intelligence is something else. And information acquired there could be dealt with on a more consultive basis under this kind of structure.

I do think you have to deal with the issue of, if somebody does not work for you, you do not control them. And that is a reality. When I was governor, I sought a new policy of accountability for public colleges and sought to appoint people to college boards who would bring actual oversight and accountability to public college education. But the law in Virginia is you appoint them and they are gone; you cannot recall them.

And as a result, I would say that that was not a successful policy implementation, because unless you can actually bring some accountability of the person that is working for you back to the table again, you cannot really expect it to be successful.

These are the challenges that I think lay ahead of this committee.

Mr. LANGEVIN. Thank you.

Chairman COX. Thank the gentleman.

The chairman of the Subcommittee on Emergency Preparedness and Response, gentleman from Arizona, Mr. Shadegg, is recognized for five minutes, or eight minutes, or however many minutes you can get out of our witnesses who are trying to leave.

Mr. SHADEGG. I thank you, and I note that we are already passed your deadline, so I will try to be brief.

Let me begin with an apology to our witnesses. I would like to have been here throughout this hearing, but due to conflicts, including a mark-up downstairs, I have not been able to be here and hear your answers to all the questions, though I had staff here. And I believe you have been very, very helpful.

Let me try to ask just two fairly direct questions, and we could all conclude this.

First, Director Woolsey, if I am not mistaken, at the end of an answer to a question just a few moments ago, you said something to the effect that you are not fond of a great number of fusion centers.

The state of Arizona, a part of which I represent, has created a fusion center, or is creating a fusion center, their state director of homeland security just advised me yesterday that California has expressed an interest in participating in that fusion center and that, indeed, our director would like to get all of the border states, those states that border Mexico, to participate in that fusion center.

I would like to give you an opportunity to give me a little more guidance on your concern about fusion centers.

Mr. WOOLSEY. Congressman, it is fairly straightforward. I think as long as there is a fusion center of fusion centers, we are okay, as the Defense Department talks about the concept of a system of systems.

What I was trying to suggest is that we do not want incompatible software, incompatible nomenclature, lists that have different standards for things going on them and so forth. This all needs to get pulled together someplace.

And the parts of intelligence that I think, as I said, ought to be competitive and come from different perspectives. People ought to have the ability to come up with new ways of collecting intelligence, even if they are different from what exists and not coordinated. They can coordinate them later. And they ought to have the ability to have disagreements and different perspectives on analysis.

But in terms of pulling the information together so everybody is kind of working from a common background, if you have a bunch of different fusion centers and someone has architected the system so that they all work together, then that is fine.

Mr. SHADEGG. The point is very clear. I appreciate it.

My second question goes to you, Governor Gilmore. Let me give you a little background. In a prior life, I worked for the Arizona Attorney General's Office. I was the second-ranking lawyer under the attorney general himself. I had responsibility for a number of divisions of the office.

In a state that had 13 county attorneys, and our job was to try to coordinate with those country attorneys and have them all working together. When you work in a job like that, you learn all the internecine fights that go on between various law enforcement agencies. The chiefs of police do not like the sheriffs. The sheriffs do not like the chiefs of police. And some county attorneys are angry at the AG; some are happy with him. It is a difficult circumstance to be in, but it is one we struggle through all the time.

Ms. Baird talked about and emphasized the importance of architecture, hardware and software, for sharing information. And I think that is extremely important.

But it seems to me what we face in this committee and what the department faces is a human problem, a problem of getting all these disparate agencies that may have motivations, indeed in the past have had intense motivations, not to cooperate to, in fact, cooperate.

And I guess my question to you is, how can we create incentives for each of them to be sharing information? And I think this is a topic on which you have a great deal of knowledge, and I appreciate your thoughts on what this committee can do to create those kinds of incentives and aid the department.

Mr. GILMORE. Boy, that is a complicated question. And I was—

Mr. SHADEGG. You got the rest of the day, so—

Mr. GILMORE. Oh, okay.

[Laughter.]

We will be a while, I think.

And, as you know, I was attorney general of Virginia, and it is a challenge to get all of the disparate people trying to work together.

And we have focused a lot of attention, again, upon the distinction between federal authority and state and local authority and the divides that are created there.

I was amused by your previous question. I am curious to know whether when they create that western fusion center at the state level whether they are going to allow the feds to participate or not.

Mr. SHADEGG. They intend to.

Mr. GILMORE. I would be curious to know.

But I think that the answer is that you have to have a clear plan. I think you have to have a clear structure and an understanding of what are the expectations of the people involved, so that, at a local basis, the sheriffs and the police chiefs need to understand who they are supposed to report to, who is in charge.

And if that is to the local prosecutor, that is fine. If it is to a state police representative at the emergency operation center in Phoenix or someplace like that, then that is fine. But there has to be a clear understanding of what it is.

And then there has to be a culture of liberality, where people can know that they can have access to this information, and the information has to go up and down the chain.

And then you have to be sure that it works together between all of the levels of government: federal, state and local.

If you put structures into place and a clear game plan and a clear expression of expectations, then I think that the personal feuds or turf battles can diminish. Because if somebody sees a clear set of instructions and game plan and rules and they do not play by them and something bad happens, there is going to be hell to pay by that person who is not participating. And I think that that is some incentive for them not to do that.

How can this committee help? It is a challenge, because this committee does not run the states and the locals. There has to be, I think, a vision. And that is why I am so pleased to be here today and participating with this committee, because I think that this committee has the opportunity to create that type of visionary approach. And that, I believe, is the opportunity that is ahead of you.

Mr. SHADEGG. Thank you very much. I thank you for your time, and yield back the balance of my time.

Chairman COX. Thank you very much.

It is seven minutes beyond the time that I promised that you could leave. And I understand, in particular, Ms. Baird, that you

are racing to the airport. So each of you, if you need to leave at this moment, is excused.

We have one more member who wishes to ask questions.

So I want to hold firm to the committee's promise that the witnesses are excused, if you need to leave. If you can remain, you are certainly invited and welcome to do so.

And, in either case, the gentlelady will put her questions, and I would appreciate your willingness to respond to them, in writing after the hearing.

Ms. BAIRD. Thank you. I would just clarify, I have a 2 o'clock plane, so that is my constraint. And I apologize for that and would be happy to meet with anyone individually or if I can give—

Ms. JACKSON-LEE. Mr. Chairman, if you would yield, I would like to proceed with the two gentlemen and put my questions on the record. And if someone can answer it very quickly, I would be delighted.

Chairman COX. All right, Ms. Baird, I think if you need to catch a plane, you are going to make us all nervous if you do not do so.

Ms. BAIRD. Thank you kindly for having me here. Thank you.

Mr. WOOLSEY. Mr. Chairman, if my old friend, the staff director, could call my office and tell them to put off my conference call until 1:15, I would appreciate it. And then I am fine here for the next—

Chairman COX. All right. And, of course, the entire committee is due in the Capitol no later than 1 o'clock. We have a hard 1 o'clock start and a hard 2 o'clock stop. So we only have two minutes, at most.

The gentlelady from Texas is recognized.

Ms. JACKSON-LEE. Let me thank the witnesses for their accommodation on such an important topic.

Let me just simply say this about intelligence: There cannot be a more important part of the infrastructure.

Mr. Gilmore, thank you, Governor, for you great works.

And, Ambassador, Director Woolsey, thank you for your good works.

Let me just ask this very important question. We had a big debate on whether or not you need to respond to the CIA when they ask for full funding of counterterrorism.

Would you suggest that there is a crack in the system, when we cannot give a full funding for counterrorism as one of our most important elements of our responsibilities?

And since I have a short period of time, would you also just give me the effectiveness of TTIC and how we might make it more effective?

I think my colleague, Mr. Turner, said, the dual responsibilities, or the dueling responsibilities. Can you give us, if you would, that idea of how that can become more effective?

And I guess lawyers have more than one question when they say they have two.

I would only ask you, as to whether or not in the sense of where we are today, do we see a function or a viewpoint of an effective interrelated intelligence system? And I know that is a larger question, but maybe a brief answer would be helpful.

So the counterintelligence full-funding question.

Mr. WOOLSEY. Counterterrorism or counterintelligence?

Ms. JACKSON-LEE. Counterterrorism full-funding for the CIA that would help them in countering terrorism.

Mr. WOOLSEY. Well, on those facts, not knowing more about it, and having suffered somewhat from rather substantial budget cuts, both in the executive branch and the Congress, when I was DCI back in the early 1990s, it is hard for me to imagine, under the current circumstances, doing anything other than giving the agency in the other parts of the government anything they reasonably need and require in the counterterorism area.

The CIA's counterterrorism work overseas, as I said in my opening statement, is something that may not be at the heart of our counterterrorism work in terms of dealing with threats here in the United States. Because, as we saw on 9/11, much of work, took place here and in Germany, two places where we do not really spy.

But, on the facts as you state them, Congresswoman, I would really be rather surprised at anything other than a full funding of what they reasonably believe is necessary would be the course that people would take.

Mr. GILMORE. Sure. I—

Ms. JACKSON-LEE. Welcome.

Mr. GILMORE. Thank you, Congresswoman.

I sat with the Congresslady recently at the Ronald Reagan funeral.

The issue of counterterrorism is now quite central, because the issue is going to be, how can we prevent? And there is no way of preventing other than counterintelligence.

And, as for counterterrorism, to the extent that that is different, I believe that that means a response to that intelligence and information by the appropriate agencies.

No, I do not believe that Congress is going to give a blank check for anything. I think you are going to look and see what the money is requested for. But I think it is a national priority, without any question to that.

And, on the TTIC, I do not know how it is working. We recommended that it be a stand-alone agency so that all customers could feel like they could come together in it. And we believe that it should have significant participation by state and local people as well.

But, clearly, that was a major step forward, to create at least a fusion center that could become a model and a hub, if you will, for the hub-and-spoke system on intelligence fusion.

Mr. WOOLSEY. I would only add, on TTIC, Congresswoman, it does seem to me that what I had said earlier about setting up a separate office to head the intelligence community, the director of national intelligence or central intelligence, separate from the CIA as an agency, has positive implications for TTIC.

I think it is more understandable for other parts of the community to have something reporting to the overall head of the community who is not, at the same time, the head of the CIA, and would be, in many ways, a stand-alone agency in that capacity more than it is if it reports to the DCI under its current structure, where he is also the head of the Central Intelligence Agency.

Chairman COX. I thank the gentlelady for her outstanding questions, the witnesses for their outstanding answers.

And I ask that we keep the hearing record open for 30 days so that additional questions that members may have may be submitted to the witnesses in writing.

Mr. GILMORE. Mr. Chairman, I may wish to submit a statement as well, a written statement.

Chairman COX. And, without objection, that will be included in the record as well.

You have been—

Ms. JACKSON-LEE. Mr. Chairman, yield, I am sorry. I did not hear your opening. Members statements may be allowed too?

Chairman COX. Oh, yes, by all means.

Ms. JACKSON-LEE. Thank you very much.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE

I want to thank Chairman Cox and Ranking Member Turner for putting together this vital hearing on information hearing issues. As we learn more about the events the preceded September 11th it has become apparent that if information sharing between our intelligence agencies had been more in tune with each other then we may very well would have been able to prevent the devastating terrorist attacks of that day. To this day information sharing in our nation is not where it should be, the American people need to know that our nation's intelligence agencies are working in sync; unfortunately it still seems that these agencies are often working against each other. This debate is even more timely in my mind because of the fact that the House just took up and passed the Intelligence Authorization Act of 2005, H.R. 4548. I am still of the mind, that our intelligence agencies, one of the cornerstones of Homeland Security is not being properly funded. However, proper information sharing between and also within intelligence agencies is the only way our nation will be secure, no matter what the budget is.

I am shocked and even appalled that almost three years after September 11th there are still not effective avenues of communication in place. The GAG has found that officials from states, cities and localities do not consider the current process of sharing information to protect the homeland to be effective. Indeed, a major GAG survey noted that only 35% of these respondents reported that sharing information with the federal government was "effective" or "very effective". These numbers are very disturbing, especially when we consider that they come from people at the local level, those who understand their security risks the best and those who will be most directly affected by a terrorist attack in their community.

In addition to a lack of proper communication is the fact that our intelligence agencies are not properly divided with clear distinctions as to roles and responsibilities. This confusion has often led to the fact that certain incidents and cases are being looked by multiple agencies while others too often fall through the cracks. A Markle Foundation Task Force Report uncovered major weaknesses in how the Executive Branch defines the respective roles, responsibilities, and authorities of the Federal agencies involved in assessing and disseminating homeland security information. The report concludes that the roles of the TSC, TTIC, the Director of Central Intelligence's Counterterrorist Center (CTC), the Department of Homeland Security, the FBI and its JTTFs, and the Defense Department's Northern Command are not clearly defined. Inevitably, this will sustain continued turf battles among agencies, gaps in information sharing and analysis, and limit attempts to protect civil liberties.

Lack of proper communication and undefined roles are only two of the many problems that face our intelligence agencies in dealing with information sharing. Our national security will not be ensured until all agencies can properly share and disseminate information. It is unfortunate to me that in the near three years since September 11th, that more substantive steps to cure information sharing gap have not been taken. We needed proper information sharing a long time ago and we desperately need it now, time will only tell if we get it in the future.

Chairman COX. The gentlewoman's statement will be included in the record.

I want to thank, again, our three witnesses, although Ms. Baird had to leave early. And we look forward to continuing to work with you on these vitally important questions.

There being no further business, the chair, again, thanks the members who are here, the staff who worked on preparing this hearing.

Without objection, the committee stands adjourned.

[Whereupon, at 1 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS AND RESPONSES

REPONSES FROM ZOË BAIRD TO QUESTIONS FOR THE RECORD FROM THE HONORABLE SHEILA JACKSON-LEE

1. If the events leading up to September 11th were to happen today, how would the new information sharing capabilities be able to prevent the terrorist attacks? Specifically in relation the information about suspicious foreign nationals who were taking flight lessons, that was not properly shared between intelligence agencies.

ANSWER: The *Markle Taskforce on National Security in the Information Age* has suggested the creation of a distributed, decentralized network (SHARE or System-wide Homeland Analysis and Resource Exchange Network) that would prevent the stove-piping of information such as the FBI Phoenix memo that indicated that suspicious foreign nationals might be training at U.S. flight schools in preparation for future terror activity against civil aviation targets.

The SHARE Network is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants (with the suitable permissions) in the system. The SHARE Network allows for vertical and horizontal co-ordination and integration. Information would be able to flow not just up the chain of command, but also to the edges of the system.

In addition, the information shared may not be the data itself, but pointers to the person who controls the data, such as the FBI local agent, or who is informed about a topic, or who has access to more classified information. This allows for an object-oriented and self-organizing approach to the information. Participants are able to identify, contact, and engage their peers through robust directories and identity systems, and access useful and relevant information by using comprehensive querying and analysis tools.

The SHARE Network would enable, facilitate, and at times, demand two-way communication. As such the SHARE Network would ensure that users never reach a "dead end" on the network, such as the FBI Phoenix memo. Individuals who contribute to the network, based upon a "write to share" concept of operations, instead of the current 'need to know' model, would also receive information and feedback from the network and other participants, ensuring that participants, who have the adequate permissions and authorizations, at the edge of the network remain engaged and motivated. As such the SHARE Network moves from a classification system to an authorization system.

Participation in the SHARE Network can take many forms. Communities of practice—groups of participants in fields like aviation security—would also collectively act in a network. These communities benefit greatly from increased connections to those with similar roles in different organizations or at other levels. In addition, the collective community may come together as ad hoc workgroups, mobilized for specific tasks or identified threats (such as the threat of terrorists using airplanes to attack). Participants are not distinguished by their relationship to a central gatekeeper, but by their relationship to one another and the need to share.

In our SHARE Network, participants can, will, and should form unique and utilitarian relationships in order to best support their particular role in national security, whether in prevention, analysis, response, or protection. Such a peer-to-peer collaboration allows federal, state, and local participants to draw upon the collective expertise of the community. In an environment of such great risks, empowerment of local actors will lead to better prevention or response management. And this can a be done while protecting privacy and other civil liberties interests through anonymization of information, audit trails and other tools.

Information—managed through information technology—is the key to enhancing security. Information-sharing itself is not the goal; rather, it is the means by which

we can most effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information.

2. Explain to me regarding the current system in place how hypothetically an intelligence item discovered in Houston would find its way to the proper national intelligence officers in Washington in order to prevent a potential terrorist threat in Seattle?

ANSWER: Answering this question correctly would require further details about what kind of intelligence item was discovered by whom and when. Yet, below, I provide an illustration of how our envisaged information sharing system (SHARE Network) could operate in this hypothetically case.

Say a field agent at the Houston FBI office and a CIA operative in Kabul become aware of separate leads that if put together might point to a bio-warfare attack in Seattle. Under the current system, reports from these two agents are unlikely to have enough actionable information to be moved through the system. However, using the SHARE Network, these reports would be linked through similar key words such as "virus" and "Seattle" or other linking tools. Instead of being housed in classified files and filing cabinets at the CIA and FBI, these reports would be distributed electronically to people who should see them. They also would be posted and available to be pulled by network participants with a particular interest. An analyst at TTIC, for example, might see both reports, contact the CIA and FBI agents and others to discuss their reports, begin to connect the dots and define actionable objectives. The FBI, CIA, and TTIC players could form "a virtual task force" by reaching out to other relevant agencies and individuals, perhaps at Department of Homeland Security, the Centers for Disease Control or a local police department, for more information. And they could organize the work themselves, without losing time or going to their superiors in Washington for approval.

Based upon their discussions, this group could now create actionable intelligence for their agencies: the CIA might elevate the information to a higher level, to the director, or perhaps up to the president. Through local contacts in Seattle, the FBI would have the option of notifying local police, so they could watch for activities related to a potential plot.

3. In a joint press conference on May 26, 2004 with FBI Director Mueller, Attorney General Ashcroft informed the public that Al-Qa'ida is "almost ready to attack the United States" and that "disturbing intelligence indicates Al-Qa'ida's specific intention to hit the United States hard." Attorney General Ashcroft added, "credible intelligence from multiple sources indicates that Al-Qa'ida plans to attempt an attack on the United States in the next few months." However, on the very same day Department of Homeland Security (DHS) Secretary Ridge noted that the "continuous stream" of threat information is "not unlike what we've seen for the past several years." He added that "We do not need to raise the threat level to increase security. Right now, there's no need." My question is what kind of oversight can be done to make sure that the dissemination of contradictory information from even the highest levels of government can be prevented in the future, so that the American public is not left to make vital decisions based on completely conflicting information?

ANSWER: A streamlined and reliable Threat Advisory System is a critical information tool to communicate with the public-at-large. Our Taskforce has so far mainly focused on information sharing within government and the intelligence community to prevent another terrorist attack, yet the same principles can be applied to an appropriate response system. As indicated above, we envisage the creation of ad hoc (or virtual) taskforces across agencies that would facilitate a co-ordinated and united response, including threat information to the public at large.

QUESTIONS FOR THE RECORD FROM THE HONORABLE SHEILA JACKSON-LEE FOR THE HONORABLE R. JAMES WOOLSEY, AND THE HONORABLE JIM GILMORE

1. If the events leading up to September 11th were to happen today, how would the new information sharing capabilities be able to prevent the terrorist attacks? Specifically in relation the information about suspicious foreign nationals who were taking flight lessons, that was not properly shared between intelligence agencies. **No response has been received.**

2. Explain to me regarding the current system in place how hypothetically an intelligence item discovered in Houston would find its way to

the proper national intelligence officers in Washington in order to prevent a potential terrorist threat in Seattle? No response has been received.

3. In a joint press conference on May 26, 2004 with FBI Director Mueller, Attorney General Ashcroft informed the public that Al-Qa'ida is "almost ready to attack the United States" and that "disturbing intelligence indicates Al-Qa'ida's specific intention to hit the United States hard." Attorney General Ashcroft added, "credible intelligence from multiple sources indicates that Al-Qa'ida plans to attempt an attack on the United States in the next few months." However, on the very same day Department of Homeland Security (DHS) Secretary Ridge noted that the "continuous stream" of threat information is "not unlike what we've seen for the past several years." He added that "We do not need to raise the threat level to increase security. Right now, there's no need." **My question is what kind of oversight can be done to make sure that the dissemination of contradictory information from even the highest levels of government can be prevented in the future, so that the American public is not left to make vital decisions based on completely conflicting information? No response has been received.**