AMERICANS AND HOMELAND SECURITY

A Conference Report of the CSIS International Security Program

Editors
Amanda J. Dory
Shawn Powers

December 2003

About CSIS

For four decades, the Center for Strategic and International Studies (CSIS) has been dedicated to providing world leaders with strategic insights on—and policy solutions to—current and emerging global issues.

CSIS is led by John J. Hamre, former U.S. deputy secretary of defense. It is guided by a board of trustees chaired by former U.S. senator Sam Nunn and consisting of prominent individuals from both the public and private sectors.

The CSIS staff of 190 researchers and support staff focus primarily on three subject areas. First, CSIS addresses the full spectrum of new challenges to national and international security. Second, it maintains resident experts on all of the world's major geographical regions. Third, it is committed to helping to develop new methods of governance for the global age; to this end, CSIS has programs on technology and public policy, international trade and finance, and energy.

Headquartered in Washington, D.C., CSIS is private, bipartisan, and tax-exempt. CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

ISBN 0-89206-442-0

Center for Strategic and International Studies
1800 K Street, N.W., Washington, D.C. 20006
Tel: (202) 887-0200
Fax: (202) 775-3199
E-mail: books@csis.org
Web site: http://www.csis.org/

Contents

Preface

The shock and horror of September 11, 2001, raised powerful questions for Americans—what did the tragedy mean for our nation, our future, and for ourselves? Although life has gradually returned to normal for many in the last two years, the threat of future attacks continues to loom.

The Bush administration's National Strategy for Homeland Security (July 2002) outlined an ambitious approach to homeland security based on "shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people."

In line with this approach, the "Americans and Homeland Security" conference hosted by the Center for Strategic and International Studies on September 25, 2003, explored ways to further the partnership with the American people. Expert panels highlighted the attendant challenges and opportunities by focusing on a series of critical homeland security issues as they relate to the general public. These included:

- Assessing risk—threat, vulnerabilities, and priorities;
- Balancing security, privacy, and civil liberties;
- Communicating with the public before and throughout a crisis; and
- Protective action responses—shelter, evacuation, quarantine, and medical countermeasures.

This conference report provides important insights from multiple perspectives—Congress, the federal government, academia, and the private sector—and assesses where we have been and where we are heading as a nation. What is clear is that our nation's preparedness depends on the extent to which individual citizens know what to expect and what to do in times of great crisis. What is also clear is that the homeland security partnership with the American public requires a more concerted effort to ensure our resilience as a nation in the face of future attacks.

To address these and other related issues, CSIS has established a Homeland Security Program to provide research, critical analysis, and policy advice to government, business, and the international community. The mission of the new program is to advance new thinking, operational concepts, and partnerships in support of our nation's homeland security.

In support of this mission, I commend the results of this important conference to your attention.

David Heyman
Director, Homeland Security Program
Center for Strategic and International Studies

Acknowledgments

The “Americans and Homeland Security” conference would not have been possible without the cosponsorship and generous support of the Alfred P. Sloan Foundation and the National Association of Chain Drug Stores (NACDS) Foundation. We are particularly grateful to Paula Olsiewski at the Sloan Foundation and Larry Kocot and Ed Staffa at the NACDS Foundation for their assistance.

The conference benefited from the tremendous teamwork that is a hallmark of Center for Strategic and International Studies activities. John Hamre and Kurt Campbell made key introductions. Arnaud de Borchgrave, Jay Farrar, and Anne Witkowsky skillfully moderated panel discussions, while David Heyman served as a substitute speaker on short notice. Amy Smithson provided a trenchant wrap-up of the proceedings. Laura Wilkinson was an invaluable help liaising with Capitol Hill, while Robin Niblett and Margaret Dobrydnio adeptly facilitated interactions with our cosponsors. In typical “can-do” fashion, the International Security Program provided last-minute surge support with conference logistics and details, including the assistance of Margaret Cosentino, Jessica Cox, Morgan Courtney, and Stephanie Julmy. Janet Granger did her usual excellent job of ensuring that the venue and catering arrangements were flawless.

An exceptional thank you goes to Amanda Dory for her tireless effort in coordinating every facet of the conference. She was integral in receiving support of both the sponsors and the participants, as well as orchestrating an extraordinary agenda, moderating a panel and countless other responsibilities associated with the event.

Finally, a special thank you to Shawn Powers who was enthusiastic and unflappable in his support of the conference effort and did a superb job serving as rapporteur for the conference report.

Introduction

KURT CAMPBELL: It is my pleasure and honor to welcome you this morning to our conference on the role of Americans as citizens and individuals in homeland security. Obviously, for Washingtonians this is an issue near and dear to our heart after floods and snipers and anthrax and hurricane winds and other phenomena of biblical proportions.

We are extraordinarily pleased to have all of you here with us this morning. I want to just say a couple of words of thanks, primarily to Amanda Dory; we are grateful for all her help on this effort. We are also particularly grateful to two sponsors, the Alfred P. Sloan Foundation and the National Association of Chain Drug Stores, for their support in this endeavor. We have a tremendous list of folks from Congress, from the federal government, and from interested groups that will be appearing this morning.

We are particularly grateful that, to lead us off this morning, Representative Jim Turner of Texas, ranking member of the House Select Committee on Homeland Security, will be talking about legislation that he introduced yesterday, the PREPARE Act, H.R. 3158, and about his goals for basically invigorating the role of citizens in this enormous task of preparing the United States for challenges ahead in homeland security. Let me ask Representative Turner to come up and address us. Welcome.

JIM TURNER: Thank you, Kurt. The Center for Strategic and International Studies does such a great job of organizing events like this and trying to educate all of us about the challenges that we face internationally. Everybody understands that the war on terror is a tremendous, perhaps the greatest, challenge that we face in this generation. When I look back in my lifetime, I was in the Army during the Vietnam era and we all understood what a challenge that was. I know my father, when he talks about World War II, views that as the greatest challenge that America faced.

In both of those occasions and in earlier occasions, Americans have always risen to the challenge—whatever it is. We have been able to overcome adversity. I am very confident that we can do that once again. But, in order to do it once again, we are going to have to be sure that we understand the challenge we face, that we have a clear strategy for addressing it, and that we have the national commitment and public support to get the job done. I think it is critically important that we are very careful about how we define this war on terror because it is in how we define it that we will fashion our response and the development of our strategy to deal with it.

The president recently said that the war in Iraq is the front line of the war on terror and that we must defeat terrorists there so that we will not have to fight them here at home. That perspective is helpful in building support among the American people for the conflict in Iraq, a conflict that I personally believe we must be successful in. We cannot fail. We have made a commitment and we must stand by that commitment and try to build a stable and democratic society in Iraq. But that description is not helpful in gaining a greater public understanding of what the war on terror is really about.

There are many front lines in the war on terror, front lines abroad, in far-off places, in mountain caves, and in major cities around the world. Terrorism will strike us from points that we may not anticipate, and the driving force behind terrorism, the radical fundamentalism, the belief that Americans are infidels, is a concept that is little understood by the American people. In order to win the war on terror we have got to base our strategy on understanding the reality of the enemy: who they are, what they believe.

This battle is not only fought with military might, but it is fought also with good international policy. It can never be won, in my judgment, without strong international support, and it cannot be won unless we are willing to defend against terrorism here at home. We all must be very careful about how we define the war on terror. How we meet the challenge here at home will, of course, determine our security and what kind of nation we pass on to the next generation. How we meet the challenge abroad, of course, determines our relationship with the world, a world that is growing smaller all the time.

Some would say that we are safer today than we were on September 11, 2001. And that is probably true. Some question that. The actions we have taken surely have provided us with some degree of safety in certain areas that we did not have before September 11, but that is really not the question that we should be asking.

Are we safer today than we were before September 11? The question is, are we safe enough to protect America from terrorist attack? With regard to that question, the answer is we are not. We are not as safe as we can be. We are not as safe as we must be in order to ensure the security of the American people. You have heard many examples of gaps in our security that are out there: the fact that we do not check all the cargo that comes in containers. We actually inspect—physically inspect—about 3 percent, maybe up to 5 percent in some ports, of our cargo containers. Airfreight that goes on passenger planes, stored below us as we fly, is not screened as our bags are when we board the planes.

We have great vulnerabilities around the country at chemical plants. Some have reported that an explosion or incident at chemical plants could harm as many as a million people. Our reports from the front-line troops—firefighters, police officers, emergency personnel, and medical workers around the country—say they do not have all the equipment or the training they need to respond to a chemical, biological, or nuclear attack. We see signs of our slowness in preparation when here we are, two years after September 11, and we still do not have a single unified terrorist watch list. We still have 12 or so different lists out among a host of agencies. You would think by now we could have gotten that done.

So we have a lot of work ahead of us. We have a critical task at the new Department of Homeland Security that we have some great people working on. The task that they are facing is to develop this comprehensive threat analysis and comprehensive analysis of our vulnerabilities so that we can know what we should be prioritizing in terms of hardening our targets and protecting us against terrorist attack. Without that comprehensive threat and vulnerability assessment we really cannot have a sensible plan to protect America.

We continue to balance from threat to threat. We obviously have spent a lot of money on airline security because that is what the terrorists used two years ago to attack us. We had the anthrax attack, and it is still unclear as to exactly who did it, but the reaction to the biological threat has not been near what the reaction has been to the threat of using airlines to attack us.

The biological threat is the most serious one that we face. Some would say terrorists do not have the capability to do that and that their efforts are rudimentary. Yet, we should accept the fact that as we move forward in the decade ahead, we need to be fighting this war, not just in terms of what the threat is today, but what the threat will be ten years from now. We have to accept the proposition that terrorists will try to use biological weapons against us. Biological attack, as we know, could be catastrophic and we are ill prepared to deal with it.

In fact, when you look at this effort to try to develop this full threat and vulnerability assessment, the Department of Homeland Security has suggested it may take five years to get that done. What we need in this nation is a greater sense of urgency and a more defined sense of purpose about winning this war on terror. Clearly, as the greatest challenge of our generation, we must move faster. We must be much stronger in closing the security gaps and developing a national strategy to win this war on terror.

Most of the conversation we hear today is how we are going to defend ourselves against terrorists. We do not talk a lot about what the strategy is to win this war. What do we have to do as a nation to get this behind us so that our children and grandchildren will not be having the same kind of conference that we are having today?

To identify and close the security gaps, my colleagues on the Homeland Security Committee, as well as my colleagues in the democratic leadership, have developed what we call our strategy on homeland security. We put this document together and released it last week. This is a document that obviously can be refined and improved upon.

I hope all of you will look at it and offer your suggestions to us. This is our first effort to try to develop a comprehensive strategy on homeland security. It has five main components to it. The first one is preventing terrorist attacks. The best way to handle this problem is to prevent it from happening in the first place, primarily through improving our intelligence collection and analysis and our efforts to go after the terrorists. Secondly, it has a section on strengthening our borders on the land, sea, and air. Third, we have a section on protecting vulnerabilities inside America. The fourth section is on preparing our communities and a final section on protecting our country and our constitution, specifically talking about protecting our civil liberties and our way of life. It would be helpful if you would

offer up your suggestions on this because this is an effort to create a road map for protecting America. There are other pieces to it yet to be developed: the military piece, the international policy piece—all of which are an essential part of winning this war.

For one of the sections that I referred to, preparing our community, we have actually drafted legislation to implement. We introduced it yesterday in the House, cosponsored by more than 125 of my democratic colleagues. I hope that the bill that we have introduced will be heard by our Homeland Security Committee. The chairman, Christopher Cox, says he plans to put together a similar bill. What I hope will happen is that we will take the best ideas from both and move them forward and see them enacted into law.

This bill that we introduced yesterday is called the PREPARE Act. It is a piece of legislation that implements the recommendations of the Council on Foreign Relations. The Council on Foreign Relations issued a report just a few weeks ago; many of you probably have seen it. That group is a bipartisan group chaired by former republican senator Warren Rudman. It talked about how we are dangerously unprepared to deal with terrorism.

We took the recommendations in that document and tried to address them in a legislative form. A lot of the ideas that are in that recommendation talk about—in fact the cornerstone of the legislation is a section that talks about our need to spend our money more wisely, to be smarter about how we disperse these millions of dollars on homeland security.

Right now, we have a multitude of grant programs that have been enacted since September 11. We passed out money based on formulas that do not seem to make a lot of sense, and, in many ways, we are funding based on where the squeaky wheel is squeaking the loudest. In order to fund homeland security, you need first to make a determination as to what the essential capabilities for every community in America should be. The way we would like to make that determination is by calling upon not only the experts in the Washington think tanks but also the local first responders who are out there in the field who know what their needs are.

We created a task force that local responders are a part of and we asked them to make a determination and to recommend to the Department of Homeland Security what the essential capabilities of every city, community, and area in America should be. After that determination is made, and it is adopted by the department, then we hope that Congress can fund those needs. In the legislation, we recommend a single emergency preparedness grant program that will begin to fill the cups that we establish by determining what the essential capabilities should be in every community.

That is the logical and smart way, and an efficient way, to spend our limited tax dollars. What it means is that no longer would you rely on some formulas for distributing money, no longer would you fail to account for the differences in threats and vulnerabilities because as you determine the essential capabilities you will find that in a city like Las Vegas, you may find the population to be so many thousand people but in truth there are twice that many people there every day. You may find that in New York City you have serious vulnerabilities in the subway

system or on the bridges. Those things will be accounted for in the determination of what the essential capabilities for those cities should be. You eliminate the necessity of trying to have a special grant program for high-risk areas or a special grant program that is based on some formula where everybody gets a certain amount of money and instead you fund to the actual needs that exist.

There are other sections of our bill that we think are important contributions to improving our security. We call for refinement of the threat advisory system. We have a requirement that the Department of Homeland Security establish standards for training and equipment upon which first responders around the country can rely. Many of our first responders tell us that they have no idea whether a piece of equipment that is being offered to them for sale is really up to standard or whether it is not. We need to give them the help they need by going through the process of determining what equipment meets the standards to deal with a chemical, biological, or nuclear threat so they know when they make a purchase that it is a wise purchase.

We also have a section in our bill that deals with one of the most critical issues that I think exists in homeland security: the lack of ability of first responders to talk to one another on communication systems. The interoperability of communications equipment is an essential part of allowing our first responders to get the job done in the event of a terrorist attack.

There are other provisions of the bill that I will not mention, but I invite you to take a look at it and offer your suggestions. I hope that when Chairman Cox introduces his bill we can take the best ideas from both and move them forward.

Homeland security is a bipartisan issue. There are no democrats and republicans on protecting America. As we move forward, we need to remember that. I was very proud in those days after September 11, as you were, when we all saw those homemade signs popping up in front yards and by the sides of the roads all across our country that said, United We Stand.

I remember standing on the steps of the Capitol the night of the attack. All the members of Congress thought we ought to have a press conference because we had been run out of the Capitol. Some members thought we should not do that. They thought we ought to go back in. All the security folks said, “No, you cannot do it.” So we said, “Okay, we will have a press conference on the steps of the Capitol and let the American people know that we are still here, ready to work.” Spontaneously, the members of Congress started singing “God Bless America.” It was amazing to me to see the spirit of unity and bipartisanship that arose in the days following September 11. That is the spirit we have got to hold on to. That is the spirit that makes America great. That is the spirit that will allow us to win this war on terror.

We have got to be honest with the American people about the challenges that confront us. We know the price of securing the homeland is high, but the cost of not doing so is even higher.

Yesterday, I had the opportunity to go out to the National Defense University, Fort McNair, with about a dozen other members of Congress where we went through a crisis simulation exercise. They called it “Impending Storm.”

We gathered there with some of the representatives from the Department of Homeland Security and its various components, the Coast Guard, border security, the FBI, and the Department of Defense. All the various players in defending our homeland were gathered around the table and we went through a simulation of a terrorist attack on America through the use of explosives in cargo containers. Over a two-day period, there were five separate incidences that occurred. It was our job to try to respond to those attacks.

After the exercise was over, they gave us a rundown of the cost estimate to the economy of those attacks. The cost was tremendous. The destruction of our economy would occur from only a few explosions around the country. The halting of the movement of goods results in billions of dollars of loss, not to speak of the loss of life that occurred from the incidents themselves.

It was so clear to me and to those there that we cannot afford to let that happen. No nation can be strong and broke. When we talk about winning the war on terror, we have to look at the broader picture of what we are doing in Washington to keep our fiscal house in order. We are facing the largest deficit in the history of the country this year. It is going to be over $500 billion.

Yesterday, we passed the conference report on homeland security and the homeland security appropriations bill. We increased homeland security funding in that bill 2.5 percent over what we appropriated last year—about a $553 million increase—hardly keeping up with inflation. When we look at what we are having to invest in rebuilding Iraq, the president asked for $20 billion for rebuilding—probably just a down payment. That means that we are going to spend 40 times more rebuilding Iraq than we are willing to increase funding here at home for homeland security.

When you look at our increase in spending on homeland security in light of the deficit that we have created this year, the amount of increase in spending in homeland security is only one-thousandth of the size of the deficit that we have this year. After we get through passing the homeland security appropriations bill, and the next one to go to the president will be the defense appropriations bill, all of the remaining eleven bills to run the federal government will all be paid for this year with borrowed money.

No nation can be strong and broke. In order to put this country in a position where we can deal with homeland security, as well as the other big financial problems we face, whether you talk about Social Security or Medicare, we have got to get the financial house of this country back in order. We have got to be able to respond in the event of a catastrophic event. No nation can be strong and broke.

All these challenges are ones that we have an obligation to inform the American people about. I hope that as you talk about the issues facing us in this meeting today, you will do your part to educate your friends, your business associates, and your colleagues about what we need to do in America to win this war on terrorism. Each and every one of us has an important role to play. We can all enlist the support of those around us. This is the challenge that we must face and that we must win. Thank you very much.

Panel 1

Assessing Risk: Threats, Vulnerabilities, and Setting Priorities

Executive Summary

Mr. de Borchgrave of CSIS began with a description of several potential terrorist attack scenarios. Immediately after September 11, Osama bin Laden warned the United States that the real battle was yet to come. Despite losing territory in Afghanistan and losing top leaders, Al Qaeda has been able to strike and to metastasize like a cancer. Now, international troops in Iraq attract Islamic militants answering the call to jihad. De Borchgrave said that although the Bush administration and next year's U.S. presidential elections are imminent targets for terrorists, it is the long-term wish of Al Qaeda to "turn the war on terrorism into a clash of civilizations between the West and the rest." Guarding the United States' easy-access society from threats has become imperative in light of the recent arrests at Guantánamo Bay and reports of U.S. prisons acting as hotbeds for radical Islamic recruitment.

David Heyman of CSIS quoted Thomas Jefferson in saying that a well-informed citizenry is essential to a properly functioning democracy. He continued by saying that a well-informed citizenry is also essential to the defense of our homeland. However, private citizens are in need of affordable tools to assess new risks from terrorism—similar to those already in place to assess threats imposed by weather, fire, and traffic accidents. Mr. Heyman advised citizens, government officials, and businesses to take a step-by-step approach to understand the threats, the vulnerabilities, and the consequences of acts of terror. First, we must identify the key assets, then assess the nature of the threat, determine the vulnerabilities, analyze the cost and consequences of loss, develop measures to mitigate risk, and implement strategy.

William Parrish of the Department of Homeland Security explained that the United States ought to remain vigilant and flexible in the war against terrorism because of terrorists' decentralized demands and methods. Dr. Philip Anderson of Lucent Technologies/CSIS and Mr. Heyman stressed the importance of building a comprehensive strategy to consider threats and vulnerabilities of the United States. Devising a national strategy for homeland security is a complex process—one that requires a systematic mapping of terrorists' capabilities and operational

mindset. What is needed is a threat-based strategy that considers the enemy's multiple and changing methods of attacking the United States. Also, we must prioritize the tens of thousands of vulnerabilities across the country. John MacGaffin, president of MacGaffin and Associates, emphasized that we are no longer at risk in a relatively narrow and finite number of ways. There are myriad ways through which terrorists can attack the United States in this "expanded universe" of international conflict.

To address this, Bill Parrish suggested the importance of information sharing. Hitherto, agencies in the federal government have been unwilling to communicate among themselves because they lack a full appreciation of each other's capabilities. The Terrorist Threat Integration Center (TTIC), for which Mr. Parrish worked, serves to fuse intelligence. With the help of unfettered access to all raw intelligence and all criminal and law enforcement investigations that intersect with terrorism, TTIC analysts can assess and analyze a credible threat by divining the relevant information. Deducing what raw intelligence, or "dots," are needed, producing or collecting those dots from state and local levels, and connecting them in a systematic way helps determine the criticality of future attacks. DHS has the unique opportunity to do this by integrating information from 23 agencies and sequencing the dots with the help of technology. Agents then disseminate information to the appropriate channels. For example, TTIC can request that certain information be downgraded to either the secret or official-use-only level in order to get it into the hands of DHS customers, namely state and local authorities and the private sector who can best prevent, detect, or disrupt a terrorist attack.

In the event that the TTIC recognizes a credible threat, but lacks the data concerning specific targets, dates, times, etc., they investigate the critical infrastructure within the area that is considered to be of high value, and then recommend which protective measures be taken.

Dr. Anderson said that threat vulnerability integration would help determine enemy plans more accurately. Furthermore, a balance must be made between threat assessment and resource allocation in such a way that it avoids adding to the deficit. Dr. Anderson noted that the private sector owns and retains the primary knowledge of our vulnerabilities and consequences for 80 percent of our critical infrastructure. Mr. Parrish said that they have already enhanced their security posture by adopting protective measures for their financial investments and will prove to be vital participants in threat vulnerability assessment. Mr. Parrish advised that the business communities and state and local governments look at risk assessment from the standpoint of loss of life and not the loss of money.

Discussion

ARNAUD DE BORCHGRAVE: Good morning. Osama bin Laden has his own grisly way of commemorating the second anniversary of September 11. In his latest tape released by Al Jazeera, he hailed the 19 terrorists as the most honest and brave jihadis and warned us that the real battle has not yet begun. He may well be

right. Al Qaeda has shown itself to be extraordinarily resilient. It lost its space in Afghanistan, lost half its leadership in successive raids, but still seems able to move and strike and to metastasize like a cancer. Defeat Al Qaeda in Kabul and their allies strike in Bali; round up the Bali bombers in Indonesia and they strike again in Kenya; hunt them down in Kenya and they hit an American residential compound in Saudi Arabia.

And now in Iraq the deeper strategy of Al Qaeda is unfolding. The vast target of the U.S. Army now lies before them. Islamic militants are answering the call to jihad. They seek to do to U.S. and British troops what the mujahideen did to Soviet forces in Afghanistan. If the immediate target of Al Qaeda is U.S. troops in Iraq, the medium target is the Bush administration and next year's presidential elections.

But the long-term target is far more ambitious. Even if justice swiftly overtakes Osama bin Laden and his mountain strolling companion, Al Zawahiri, the real war on terror has years yet to unfold. It is Al Qaeda's objective to turn the war on terrorism into a clash of civilizations between the West and the rest. It must be the primary war aim of the United States and its allies and the most honorable tribute to the 3,000 dead of September 11 to ensure that this does not happen.

The world's only superpower is also a land of countless vulnerabilities, as we all know. The great society is built on easy access to everything and even, as you have noticed, the Guantánamo prison for terrorists was apparently penetrated, and three U.S. military personnel are under investigation. Recruitment of potential Islamic terrorists in the U.S. federal prison system is something that we have barely scratched. But, to explore all of these threats and vulnerabilities, we have put together a blue ribbon panel for you and they are among the very best and most knowledgeable in the business of counterterrorism.

WILLIAM PARRISH: Thank you very much. It is an honor to be here and a privilege to participate in a very, very important full-day session. As we all know, our nation remains at war. We are still at the alert level of yellow, which means elevated. We also know the nature of the enemy and his decentralized methods make us a nation that must remain committed and fully focused on defeating this enemy that threatens our way of life and the lives of American citizens.

As I got into this business at the federal government level after leaving the Marine Corps, one of the first things I realized was the criticality in information sharing. We have heard the phrase as stovepiping. I try to look at the glass as being half-full and I am not so sure it is a lack of people willing to give the information to another agency, but rather people not having the full appreciation of that agency's capabilities or authorities of what they can do with that information once they acquire it.

One piece of information does not yield intelligence. One piece of intelligence does not necessarily yield a threat. These are my challenges as the acting assistant secretary for information analysis. As we look at the threat to the nation on a daily basis, being able to say to Secretary Ridge, we have what we have determined to be a credible threat against which we must take corrective action immediately.

Does this mean we elevate to orange and we go out nationwide causing states, local authorities, and the private sectors to expend their limited resources based on this credible threat that we have determined? It is a great challenge, as you can imagine. So we try to look very carefully and certainly in close coordination, collaboration, with other members of the intelligence community.

The Terrorist Threat Integration Center is where I had the privilege and opportunity to work with John Brennan, who is the director, and who is just a tremendous American and has done so much in short order to pull together a comprehensive center that is fusing together the information in intelligence within the confines of their establishment over at the criminal investigations headquarters right now.

Criminal investigations will lead to critical pieces of intelligence. Agents, whether immigration customs enforcement agents, whether FBI agents, whether detectives in downtown New York City as they begin to delve into a criminal investigation that uncovers a terrorist nexus, must be very quick to recognize that they have some information here and that they have to ask the question, "What do we know and who needs to know it?" And getting that information back into the information flow, into the intelligence channels, helps us to be able to affect that phrase you have all heard: connecting the dots.

The Homeland Security Act of 2002, of which the support of Congressman Turner, other members of the Congress, and the administration was instrumental in passing, gave the information analysis infrastructure and protectorate a very, very broad range of authority. Stating very clearly, it requires unfettered access to all raw intelligence and all criminal and law enforcement investigations with terrorist nexus. That is by law and each time I appear up here on the Hill to our board of directors, I am asked if I am getting all of that raw intelligence and all of those law enforcement investigations? My response is, "I am getting what I know I am getting." I will tell you this, though, because the Terrorist Threat Integration Center and that initiative stood up, we now have a Department of Homeland Security analyst over there working very closely with the other analysts. And while I was there, as I was looking at very sensitive intelligence reporting I was saying, "I need this downgraded to either the secret or official-use-only level in order to get it in the hands of Department of Homeland Security's customers, and they are the state and local authorities and the private sector." Parrish has not been told "no," yet. I have also told Congress that when Parrish is told no he will immediately come back up to the Hill and let them know that.

I see a great deal of success and we are moving forward in the spirit of cooperation. What we do with that information and the assessment of it, we are chartered by law to conduct independent assessments, we look at it and then map it against the threats. The infrastructure protection directorate, with my colleague, Bob Liscouski, the assistant secretary, is responsible for the critical infrastructure piece. So if I could use an example of how this all ties together, I will look a little bit at what we did during Liberty Shield; let me try to summarize that.

Let us say we had a significant piece of intelligence that came in through signal intelligence that we determined is a credible threat, a credible threat to Chicago. That information then is assessed over at the Terrorist Threat Integration Center,

it is assessed by my analysts in Information Analysis (IA), and we agree it is a credible threat but there is no specific target—there is no specific date, there is no specific time—yet it is a credible threat.

Now what does that mean to Mayor Daley and to the governor of Illinois? "Well, thank you very much, Secretary Ridge, for this information. What am I supposed to do?" What we do in IA in working with IP (Infrastructure Protection), then, is we sit down and we look at what is the critical infrastructure within the Chicago area. And let us say we came up with a list of five chemical facilities, one of which sits right on the lake where there is a constant breeze coming off the lake. That wind is constantly blowing into a large populated area. That is a high priority target. We found two other similar chemical plants like that. We have also identified three major conferences downtown at certain hotels, and, by the way, it is the NBA playoffs. Secretary Ridge then contacts Mayor Daly, contacts the governor of Illinois, and advises them that we have a credible threat. In our assessment of the critical infrastructure, what we consider to be high-valued targets are the following, and we would encourage you to take a look at your protective measures you have in place.

We prepared recommended protective measures during Liberty Shield for the critical infrastructure and a lot of the private sector adopted those protective measures and made investments to enhance their security posture. I realize that my background in the military, risk assessment, is a little bit different than the business world. As I planned operations in the military, risk assessment was based on one thing—the loss of life. In the business world, it is an assessment of the loss of money. In the threat that our nation is confronted with today, business communities and state and locals must take a look at that risk assessment from the standpoint of loss of life and not the loss of money. It is a partnership. I am here to access, assess, and analyze the intelligence out there in order to turn that around and get it in the hands of those individuals at the state, local, and private sector who are in a position to prevent, detect, or disrupt a terrorist attack. Thank you. I look forward to your questions.

PHILIP ANDERSON: Good morning. One of the best tours I spent in the Marine Corps was as an operations officer working for Bill Parrish at U.S. Marine Corps Forces Atlantic some years ago. Interestingly enough, in those days, many of the things that we were involved in and many of the discussions we had generalize to this new environment that we find ourselves in post–September 11. Secretary Parrish talked to some of that in his comments.

I would like to take this up a notch to a somewhat higher level and look at strategy. The thing that probably strikes me as most odd is that we have in the past two years spent tens of billions of dollars, we have established a Department of Homeland Security, we have done numerous things to protect ourselves—to make the nation safer, more secure. But we have done all of that without a comprehensive sense of the requirement.

What is the requirement? The requirement truly has to be focused on what our enemies are capable of doing to us. Not only that, but what aspects of our infrastructure—what aspects of our society—are most at risk? What things are

critically vulnerable? Certainly there are thousands, if not tens of thousands of vulnerabilities across the country, but not all of those things are likely terrorist targets. Clearly there are some things that are far more attractive to terrorists than other things.

Now, granted, getting at the requirement is far easier said than done. It is not an easy thing to do with tens of thousands of potential vulnerabilities. There is no real clear understanding—although we can get close to a fairly clear understanding today of what Al Qaeda is capable of. But it is still problematic.

Some would argue that there is no way to define what Al Qaeda is capable of doing to us. I disagree with that in the strongest terms. We have 20 years, at least, of experience in observing this enemy. We have 20 years worth of data. We understand to a certain extent their operational mindset, how they think. We understand a lot about their capabilities and we have seen their capabilities demonstrated time and time again. Certainly, there are no absolutes. Certainly, they may possess capabilities that we are totally unaware of.

In all of the work that we have done at CSIS over the past couple of years we learned a great deal, but we learned a great deal in an open-source, unclassified environment. And only Bill Parrish, and maybe there are a few others in the room, who know what is going on behind the scenes in a classified environment and certainly that knowledge base is much broader than the one that we amassed over a couple of years, but we nonetheless learned a lot.

What we learned points to the requirement—and it is clearly spelled out in the national strategy for homeland security—to systematically map terrorist capabilities or means of attack—the ways in which they seek to do us harm—against our vulnerabilities. Again, it is much easier said than done; it is in fact, a very complex process. We developed a little framework, though, and I would commend it to you, you can probably find it easily on the CSIS website. There is a white paper there and a slide presentation. It is a very simple framework and the thing that we did not share publicly are the variables that were very carefully designed and extremely well-defined that we used to conduct this analysis that supported a very large executive simulation exercise that we called Silent Vector. But this is just one among many things that we learned about threats and vulnerabilities.

There has been a lot of strategizing over the past couple of years. Congressman Turner talked about strategy and he suggested that they have pulled one together, but I have not yet seen what I would call a threat-based strategy, something that actually drives a stake in the ground. Certainly it would not be static—the threat is going to change. It is going to change week-to-week, month-to-month, year-to-year.

I think it is safe to assume at this point that Al Qaeda in particular seeks to acquire the means to physically destroy us, not just to create widespread disruption—to hurt our economy. Those are all things that they seek to do, but ultimately they seek to possess weapons of mass destruction, the means to physically destroy us. So anything that we do with regard to threat assessment over time will certainly have to take into account new capabilities that they might acquire.

With regard to vulnerabilities, you hear people talk about any number of vulnerabilities: ports, borders, shipping containers, certain aspects of aviation, certain aspects of the transportation infrastructure, aspects of energy and energy related infrastructure which our Silent Vector exercise focused on—chemical facilities, nuclear power plants, etc. And it is very easy to say that something is vulnerable, but there always needs to be a follow-on question: vulnerable to what? I have heard any number of experts and, as Bill Parrish alluded to, I am a "the glass is half-full" guy. I have sat on many panels beside numerous experts, and I am getting ready for Dave Heyman, he is going to take the shot at me here in a few minutes, but I have heard people talk about the coming cataclysm, those horrible things that are going to happen just any day, that terrorists potentially possess all kinds of horrible, terrible capabilities to do us harm. You hear lots of talk about chemical and biological weapons. I do not discount any of that. I think that those are things that we certainly need to be concerned about, but we always need to ask the question, how will this enemy do us harm? I think that in the wake of September 11 we assumed, or many of us did, and some of us still do, that Al Qaeda is almost omnipotent in their capability to do us harm. I do not believe that is the case. So the follow-on question should always be, how exactly are they going to do it? It is easy to suggest that they are going to be able to attack a nuclear power plant and create a situation where radiation escapes into the atmosphere, but how are they going to do that? Tell us how they are going to do that. Now, certainly some of that is pretty sensitive but it is an important question to consider as we work through this whole process of threat vulnerability integration, as we start to think about not just strategies, not just things that basically are going to address every vulnerability out there, but how, specifically, we are going to address this threat.

I would like to end with one other thought. This comes from a friend of mine that many of you know, Randy Larson. He has said time and time again that the real threat is not Al Qaeda, but the real threat is overspending. The real threat is allocating far many more resources toward this problem than we need to. There is a direct relationship. It has come up numerous times.

Several very prominent public officials have talked about the connection between threat assessment and resource allocation. Secretary Ridge has mentioned it on several occasions. Governor Pataki mentioned it in a discussion where he was concerned about the amount of money that was allocated, on average, for each citizen of New York State, as compared to the average amount for each citizen of Wyoming or Montana. It was like $1.00 in New York and $8.00 in Wyoming—clearly a problem.

There is something wrong there. Clearly the citizens of New York, because of New York City primarily, are at far greater risk than folks in Montana. But we need a process that gets us to the point where we can absolutely say that. So there is a direct connection between threat assessment, threat vulnerability integration, more appropriately, and I refer you to the national strategy for homeland security, page 17, left-hand column, which defines threat vulnerability integration. It is unreasonable at this point that it has not been at least started.

There were numerous and enormous challenges that had to be addressed in the wake of September 11, passenger airline security, ports, borders, containers, all kinds of things that were clearly vulnerable that had to be addressed. We have reached a point, we have a Department of Homeland Security, it is coming together, it is time for us to try to further this process, such that we have a framework that will allow us to effectively allocate resources and hopefully not break the bank in the years ahead. Thanks very much.

JOHN MACGAFFIN: Thank you. I like the way this conversation is progressing, it sets me up for exactly the things I wanted to talk about and your notion of centrality of threat vulnerability integration is something we need to hold up real carefully and think about in the following sense. I would like to do two things, I would like to talk about criticality, which will be the focus of my views on the notion of integration of threat and vulnerability and then move onward to the notion of dot collection versus what are the dots we really need, dot production, dot connection. And finally spend some time on technology. The sequencing is important because I would suggest, among other things, we have got some of the sequences wrong.

Let me start first with the notion of threat vulnerability integration. In the Cold War it was really quite clear. We had a finite number of enemies, we thought, the Soviets, the Chinese, who were going to attack us in a relatively narrow, would put us at threat, at risk, in a relatively narrow and finite number of ways. It is really clear that both of those things no longer apply.

There is an infinite number of vectors through which an infinite number of potential hostiles can come at us. It is not just the X number of people who are part of Al Qaeda. It is an expanded universe. They can do an infinite number of things to us, which is getting to where both the previous panelists were. So, if that is true, then there is a radical shift from the Cold War paradigm of a finite number of bad guys that we can watch. When I was at the bureau, a friend once said to me, "We watch the brick and mortar that is the former Soviet, now the Russian embassy, and we watch it real close. And if it were to move over the night, we'd know it. But that is about all we'd know because that is looking at the finite." The financer, an intelligencer officer comes out the door, follow him. If a terrorist comes out the door, follow him. So, point one, if there is a fundamental change, what does that tell us about what we do? I think it goes to the notion of vulnerability threat integration—that you cannot start there. That way lies madness, to start there you have got to step back first before you get to that and deal with the notion of criticality, which is the first thing I want to talk to you about. If you do not start with criticality, it is the infinite number of threats, and with an infinite number of threats, you are going to do nothing. If you will permit me, a very simple-minded explanation that conveys this is the problem of a plastic knife and the linen napkin at the front of an airplane. You come on, you sit down, they give you a glass of wine, you open up your napkin and out falls a plastic knife. Why? Because somebody, probably someone in this town, said, if I was Osama bin Laden, I would take that knife, that metal knife right there, and I would go hijack the airplane. So, at some minimal cost, but at cost to the resources, the airline, the

passengers, we swap that sucker out and now we have got plastic knives. And you open your napkin a little further and what falls out? Four very sharp forks, which all of us know could do more damage.

Apologies for the simplicity of it, but I think it makes the point that there are an infinite number of things. So you got to figure out what is the criticality involved here and then work yourself through what is an issue. I would suggest a criticality involved in this scenario is something to do with airlines; airplanes must not be used as guided missiles. I think if you back up, then that is going to be your criticality. Then you think of what are the vulnerabilities, because you know the whole system is not vulnerable. You cannot deal with every aspect of airline security. So you have to say, we cannot have airlines used as missiles. How do we do that? Well, we have done that. We have done the aircraft door, the cockpit door. That is really good. Now, are you saying there will be no aircraft ever involved in terrorism? Is that really a realistic goal? Do we really believe that there is not going to be—to take that to the national level, are we really going to stop all terrorism? That brings me back to the point that if you do not start with criticality, we have got a real problem.

Let me move on to the second thing I wanted to touch on for a later discussion, and that is this notion of connect-the-dots analysis. National Security Adviser Rice said, not so long ago, that she understands this business about connecting the dots, but, let me tell you, there were precious few dots before September 11. I am one of the ones who believe that September 11 was preventable. We just did not connect the dots we had. There were not enough dots.

Now, if we had been doing some of the other things we have claimed all along in the federal and the state and local level that we were doing, we might have produced enough dots because we would have been interacting differently than we are now. But, the fact remains, it was preventable, but it was not preventable by simply connecting the dots. It is not a question of dot connection, but where do we get the right dots for dot production? And that is pretty hard.

Dots come in all sizes and shapes and, real quickly, they come first and foremost. And the best thing about DHS is we are taking the 23 agencies that have a whole bunch of dots and we are struggling mightily to get them together. But, I am afraid that we have got to divide this into a couple of categories.

The first category would be, what are the dots that the Coast Guard has that are clearly a value to this process? That is real easy for the boat sailing to the shore with a big sign that says, "I am a terrorist." They are going to have that—they know they have that information; they are going to get it. That is the one that you know they are going to get to who needs it. Below that, there are those things that are there that we know, and, of course, we still know they are relevant. This is, again, what both of you touched on.

And then the final category of things is, what are those dots that they could acquire if they did things differently? Three different kinds of dots that are embedded in the 23 agencies we have already got. Again, that is going to drive you crazy unless you start from criticality. Once you understand the true criticalities of systems, that will help you understand which dots really make a difference in a

system, in an infrastructure, for instance. And the same sort of three categories can apply relative to what the state and locals can produce. Start with the 23 agencies that are DHS, go to state and local information, go to what the CIA, the federals, the federal listees can do, the CIA, the FBI, the Department of Defense, the NSA.

Relative to that sort of array of issues, I would state that if you were Secretary Ridge, and you could only have two piles of information, state and local information that is available to them now in those three categories or CIA, FBI, and NSA data, which pile would you pick? There is no doubt that you would pick the first one, the state and local pile. We spend an awful lot of time on the TTIC and other arguments about access to raw intelligence. I spent 30-plus years as a CIA station chief and if you have a human source that can tell you that his bola is going to attack something at a particular time, that is wonderful. But, do we want to base the national security on the fact that MacGaffin is going to deliver that kind of secret? You are banking on the wrong thing. So, I think we have to bring our focus on how to bring state and local stuff in, because that is where the real value is going to be. Again, you have got to get us back to a notion of criticality.

The final point I wanted to touch on was the notion of technology. I put it at the end because that is where it ought to be until we really understand criticality relative to threats to homeland security. Only then can we go on to the pieces of threat vulnerability integration that we have to do. With all the dots that come, and they come in various sizes and shapes and various places, only then can you truly understand the technology that we need to utilize them. And, in fact, the technology can help you sort through dots to figure out which dots are more important. But we are rushing headlong for both good reasons and some less good reasons to decide what the technological solution ought to be. We need a timeout in all but the most essential technology until we have worked our way through criticality.

And then the last note I wanted to put on the table here, and I clearly do not want to set foot in the treacherous swamps of Terrorist Information Awareness (TIA), but, having said that, for someone who has been in operations all his life and understands these kinds of threats, you cannot do the work that is laid out for DHS without the ability to sort through the massive kinds of information across the sector that give us all the heartburn from being concerned about privacy and civil liberties. You cannot do it.

And I know it is counterintuitive, but my final point would be, but for these problems, you need to put more hay on the stack to find the needle, not less. And that was the heart of this notion of TIA. Until we get through the fact that there has to be more hay, we are walking in the wrong direction. Less hay hurts. It does not help you find the needle.

DAVID HEYMAN: Thank you. The problem with going last with the three smartest people in Washington is there is not a lot left to say. But, let me try to connect some of these dots. I will try to add a couple, too. This conference is about Americans and homeland security, so I just want to start off with the question of how many people went to the gym yesterday? A show of hands, we have got a lot

of people that went to the gym. And how many people have car insurance or wear a seatbelt, carry an umbrella? Okay. These are all personal calculations we make based upon threat of disease, the threat of car accidents, the 40,000 accidents we have a year, and we choose to mitigate these threats by employing these countermeasures. Now, let us get to some more serious questions. How many people here have a supply of water, canned goods, and flashlight batteries at home? Okay. That is pretty good. How many people have a safe room? How many people have a safe room or own an escape hood to counter biological and chemical agents? Oh, a couple of people here. These are also risk assessments that we make, but the tools for us private citizens to assess risk against terrorism are far less-developed than those for things like weather and fire and traffic accidents.

The reality is, however, particularly for the escape hoods, members of Congress and employees at the Pentagon have all chosen to buy them. So the question is, why do not you have yours, particularly if you are working downtown, particularly across the street here? Is it because they are too costly and you do not have the resources? Is it because our military and legislators are more valuable to society and thus require greater protection? Or is it because they know something we do not know? The reality is, it is a risk that we do not want to take for these folks, or maybe it is the cost that we are willing to incur. But given what we are lacking today, the question for society is, how do we mitigate against risk in a world where every day there seems to be a new threat against new targets and new vulnerabilities?

Arnaud talked about the attack patterns of Al Qaeda. If you go through some of them over the last year and a half or so, it is almost every aspect of society across every continent. Our energy infrastructure was attacked when the Limburg, an oil tanker, was attacked off of Yemen. Tourism in Bali with the hotel attack, transportation with shoulder-fired missiles in Kenya or potential cyanide attacks in London. And, of course, whether it was Al Qaeda or not, the health effects of anthrax attacks here in America. Not to mention, beyond those terrorist threats, the ones that we really think about on a day-to-day basis, things like forest fires, SARS, blackouts, mad cow, monkey pox.

So how do we assess how we will manage in a society filled with new risks and new challenges? We cannot in all reality protect against all things at all times. So, what do we do? John talked about how we do not start with threat vulnerability, we start with criticality. We start with criticality, we go to threat vulnerability, but it does not stop there.

The decisions that we make today regarding risk requires a systematic approach, a comprehensive approach of what warrants the most immediate attention and consequently how do we guide the decisions that we make in terms of investments for priorities? They must be made in terms of all of the things that have been said before me, in terms of our basis of understanding the threat, understanding the vulnerability, understanding the consequences. So, six key steps to doing that.

John talks about criticality. First we have to understand and identify the key assets or, as the secretary said, the high-value targets. What are our crown jewels? Second, we need to assess the nature of the threat. We have talked about the

threats and vulnerabilities. The second and third thing is determining the vulnerabilities, but before determining the vulnerabilities, we must ask, do the bad guys have the resources to do what it takes? What is it they are going to do? What are the skills and knowledge it takes to do that? Do they have the operational capability to impose that threat against us? We cannot assume all threats at all possible costs. We have to do this based upon what a real assessment of the threat reality is. Determining the vulnerabilities is the third step. Are there assets that we have identified? Are they vulnerable to the kind of attack that we have realized might be possible? As I said, not any and all imaginable attacks are possible, but we must look at those that are based on the threats that we have identified as real.

Fourth, and this is the most difficult part that we face, analyzing the cost and consequences of loss. Not all targets are of high value and we have to estimate, but it is not just the estimation of casualties. Remember, the folks in the Al Qaeda network want to undermine our economy and, as a Congressman said this morning, a broke country is not a strong country. That means if they undermine the economy we do not have the resources to move forward. So we have to look at not just the estimated casualties, but also the economic consequences, the political consequences, and the psychological and symbolic impact. The folks who do this best, the insurance entities, have just recently begun looking at incorporating terrorism into their analysis and we need to do more on that.

The fifth, once we have gone through this type of analysis, is to develop and plan our measures to mitigate risk. Should we, in fact, establish a national stockpile for pharmaceuticals? What goes in it? Do we need new vaccines? Where should we locate the stockpile? These questions need to be answered. And, finally, implementing the strategy, which takes more resources.

Let me just try to jump to the end here and talk about the five or six new truths that we need to accept if we are going to go forward with this. Number one is, fundamentally, we have had a significant change in the manifestation of international conflict. It is no longer armies facing each other on battlefields. The front line has moved from the battlefields and tanks to our cities and urban centers and the combatants are no longer the armies and the military, the combatants are terrorists, our first responders, our citizens. Second, that means that we need new partnerships among the people who are working to defend us—new partnerships between the federal, state, and local governments, between the public and private sector and between the government and private citizens. Third, we have to recognize that security is a balance of resources that are limited and risks that can never be eliminated. We cannot possibly imagine all possible threats and try to counter them. Consequently, my fourth truth is that the decisionmaking both for investments in homeland security and for crisis management must be made within a limited context, a context of limited, ambiguous, and evolving intelligence.

That leads to five, which is that intelligence is no longer the sole purview of the federal government. This is a concept that both the federal government and the private sector are having difficulty reconciling, but the private sector owns and retains the primary knowledge of our vulnerabilities and consequences for 80 percent of our critical infrastructure. They understand the threat better than we

do. The state and local officials have the visibility of what is going on on the ground. So there needs to be, in order for us to have effective risk-based analysis, communication between the two. And, lastly, we need to view the public as an asset, not a liability. Jefferson said that a well-informed citizenry is essential to the proper function of democracy. It is also essential to the defense of our homeland. I will leave it there and look forward to your questions.

Panel 2

Balancing Security, Privacy, and Civil Liberties

Executive Summary

Moderator Anne Witkowsky observed that significant advances in technology have vastly improved the government's capacity to collect and use private sector information for the purpose of gathering intelligence on terrorists. Enhanced data mining and pattern recognition for intelligence gathering and analysis, advances in surveillance technology and improvements to biometric capabilities for access control and authentication of individuals all potentially give us a greater capacity to defend ourselves at home. But we know from past federal government abuses of domestic intelligence gathering on U.S. citizens that this kind of activity can pose a threat to our civil liberties. Our current intelligence needs and advances in our technical capabilities create huge challenges for privacy protection. The objective of this panel was to lay out some of the key challenges and opportunities our nation faces in enhancing national security and homeland security while ensuring that our citizens remain protected from abuse of these new security and intelligence systems.

Representative Jane Harman focused her remarks on the need to embed privacy tools in the new investigative tools and technologies being developed in the pursuit of terrorists. She expressed concern about the scope and breadth of some of the new investigative tools that Congress has enacted for law enforcement and that have been enacted by regulation, but emphasized that it should not be presumed we have gone too far. Rather, she argued, we should focus on the question of how much unfettered access the government should have to intimate details of our lives, and that we must seek to answer that question as a prerequisite to the design and employment of new data-mining tools and other technologies and systems. She underscored that new tools and the new safeguards need to be developed together.

She observed that civil liberties and security are mutually reinforcing. Security clearly ensures the freedom to exercise our liberties, but it is also true that the exercise of civil liberties and our way of life contributes to our strength and security.

Protection of civil liberties also promotes the kind of relationship between government and the governed that keeps the nation strong and secure. Community policing, for example, has built trust between local police and

citizens, a trust critical to crime fighting and now to fighting terrorism. If our country is going to be successful in the war on terror, we need much more nuanced strategies to reach for help from communities, rather than targeting total communities. Similarly, building a comprehensive watch list that can draw from different databases has to be designed carefully. Controls, access to information, and targeting of the information gathering have to be carefully thought through on the front end.

She believes that it is premature to discuss changes to the Patriot Act until we fully study how well the existing law is working and correct problems with the existing law. She also argued that homeland security implementation could be done much better if we were more strategic about it and if we were to maximize the privacy and civil liberties function in the Department of Homeland Security.

She hopes we will wean ourselves from the zero-sum paradigm of partisanship on homeland security; terrorists will not check party registrations before they blow us up. The strategies that we design have to be designed together because we are all in this together.

Nuala O'Connor Kelly encouraged striking the word "balance" entirely from the vocabulary around privacy and security. She prefers language such as "imbed privacy and civil liberties." Secretary Ridge's sense of the privacy officer's role within and without the Department of Homeland Security is one of equal standing to the other component parts of the department. The goal at the department is not only to protect borders and airports and other tangible assets of the United States, but also to protect the intangible qualities of the United States that make our country great and the envy of so many around the world—the freedom that we experience in our daily lives.

She reviewed the role and functions of the Privacy Office. Among other responsibilities, the office must ensure that the use of technologies by the department enhances, not erodes privacy. The office also oversees Privacy Impact Assessment Requirements under the Government Act of 2002, as well as Privacy Act compliance under the Privacy Act of 1974. Ms. Kelly has also taken on work in the Freedom of Information Act area. Beyond the Department of Homeland Security, she must review legislative and regulatory proposals across the federal government and, as needed, will act as an advocate for people working on privacy throughout the federal agencies. Most uniquely, the statute provides that her office, and the privacy officer in particular, report directly to Congress. It thus provides an important level of autonomy, but also a challenge in that the office is both within and without the organization at the same time.

The Privacy Office is responsible for the overall scrutiny of the collection of personal information in all of its many forms, whether in its basic form or through new and cutting edge technology, such as the biometrics envisioned for the U.S. Visit program. Structurally, the office is focusing on education and training of DHS employees. That means training everyone from policy analysts to data collectors to employees at airports to border patrol agents to Coast Guard midshipmen.

Some of the hardest issues the office faces are in the area of use of private sector data and how it is transmitted into and out of the federal government space.

Another important challenge is working internationally with privacy officers and commissioners. The U.S. framework is second to none, although far harder to explain than a simple, single privacy statute in the federal space. We have several dozen statutes in the federal space that protect privacy, of financial information, of health information, and of children's information.

The privacy officer also works within a range of communities that are both supportive of and critical of the department. Certainly there are many in both camps and the Privacy Office is working hard to hear all voices as it crafts a new paradigm for what it means to be secure in this century.

Joseph Onek discussed issues related to video surveillance technology, as just one example of surveillance and database technologies. Video surveillance is going to become more important in part because of technological developments; digitalization makes it easier to use and store tapes and we are likely to succeed in the future in developing workable face recognition technology. The Supreme Court, in the past, has held that there is no expectation of privacy in a public place, but those kinds of doctrines will have to be revisited when the government or the private sector may have the ability to retrace a person's entire public life.

Some of the legal issues that surround the use of video surveillance are: When do you use cameras and what do you use them for? What do they focus on? Who authorizes it? Under what circumstances? Do you need a warrant? Do you need a warrant to put cameras in particular places? Do you need a warrant to use the face recognition technology?

How long do we keep the videotapes? The District of Columbia has a policy that the videotapes it takes of the World Bank demonstrations and so on are kept for only ten days, unless the tapes seem to have evidence of criminal conduct or police misconduct. That seems very reasonable and very protective of privacy for that purpose. But if your purpose is to prevent somebody from blowing up the Brooklyn Bridge, ten days is not going to be good enough.

Who has access to the tapes? Technology can possibly be a help in this instance because if access is digital, you can have electronic audit trails, which may be difficult to get around. Technology is not always the problem; methods of technology, including audit trails, can, in fact, protect privacy.

How and when is the videotape disseminated? This is a problem that we face in many areas. To give one example, if there are several members of a mosque who have been convicted of terrorism, an agency of government might want to get the names of some of the other people in that mosque, particularly people who were known to be friendly with the terrorists. A lot of these people are not terrorist suspects, they are just people whose names the government would like to have, but they could be implicated. Rules for disseminating and segmenting information are very difficult issues.

As with other technologies, we have to go through the methodological and systematic approach of asking why we need video surveillance and if we are going to use it, what kind of protections, both judicial and technological, we should set up to assure that unnecessary incursions against privacy are avoided.

Stewart Baker articulated private sector constraints that need to be kept in mind as we try to construct new programs. It is not so much fear of scandal that

drives the private sector; it is driven by the need to avoid losing money or getting sued. That is what worries the private sector when the government comes calling and asks for help in gathering information. Law enforcement officials have told Mr. Baker that a particular client ought to give the government information as a good citizen. But he is yet to hear this from somebody who is working for free. If they are asking the private sector to get involved, the intelligence community is better than law enforcement about reimbursing people their costs.

The most obvious situation in which government needs to worry about the possibility of lawsuits against private sector cooperators is in the international arena. It is possible to pass laws. Generally, most of the laws that are in place do provide for immunity for people who respond to proper process. It is not possible, however, for the U.S. government, on its own, to provide immunity for international actors from lawsuits by data protection authorities around the world who think it is their business to determine how the government of the United States uses information about their citizens in the fight against terrorism. We have seen in this area, particularly in the context of CAPPS II, a remarkable degree of aggressiveness on the part of the European Commission. Their data protection authorities say that we are going to hold anybody who does business in Europe liable for privacy violations if they share this information with the U.S. government. Whether they actually have that authority, and whether that authority is justifiable under even European law is not much of an issue in Europe because of their absolute determination to try to reign in the United States on almost any issue that they can get a little bit of purchase.

As new data systems are constructed, one needs to ask how they are going to be justified under European data protection law, which now, because of the way Europeans have enforced that law, includes Canadian, Mexican, Argentine, and Japanese data protection laws. Those laws have spread everywhere and are going to cause trouble for any U.S. company that does business abroad.

Discussion

ANNE WITKOWSKY: Welcome to the second panel of today's program. As our first panel today underscored, it is clear that we need to do a much better job of understanding the terrorist threat, assessing our vulnerabilities, and then setting priorities. Nothing is more important to these tasks than good intelligence and analysis.

As we all know, gathering intelligence on terrorists often involves collecting private sector data, including within the United States. Significant advances in technology have vastly improved the government's capacity to collect and use this private information. Enhanced data mining and pattern recognition for intelligence gathering and analysis, advances in surveillance technology, and improvements to biometric capabilities for access control and authentication of individuals all potentially give us a greater capacity to defend ourselves at home. But we know from past federal government abuses of domestic intelligence

gathering on U.S. citizens that this kind of activity can pose a threat to the civil liberties of Americans.

Our current intelligence needs and advances in our technical capabilities create huge challenges for privacy protection. Our laws, regulations, policies, and oversight structures must keep pace. The objective of this distinguished panel on balancing security, privacy, and civil liberties is to lay out some of the key challenges and opportunities our nation faces in enhancing our national security and our homeland security while ensuring that our citizens remain protected from abuse of those new security and intelligence systems.

JANE HARMAN: Good morning everyone. I always enjoy participating in CSIS forums. CSIS is, among the other groups out there, probably the one that is most helpful and most relevant right now to the very tough issues that Congress is addressing.

When the House Intelligence Committee held a recent public hearing, the first on our review of prewar intelligence on Iraq, John Hamre was one of our witnesses and his testimony was insightful. In fact, it was very special.

I also want to introduce Suzanne Spaulding, who has joined the House Intelligence Committee staff as its leader. And as Suzanne Spaulding and I have been focusing on how to prepare a review of what went right and what went wrong in terms of our intelligence products prewar in Iraq, we have been looking at Hamre's testimony because it really is helpful.

So, thank you John Hamre in absentia and thank you to CSIS for once again pulling together a terrific forum and giving a chance for me to say "hi" to Joe Onek, whom I have liked for 30 years and do not see very much.

Since September 11, "law enforcement" has a very different meaning than it did on September 10, 2001. The scope and breadth of some of the new investigative tools that Congress has enacted for law enforcement and that have been enacted by regulation is a source of concern to many civil libertarians, and, frankly, to me. Indeed, it was also a recent subject of another rare public hearing of the House Permanent Select Committee on Intelligence.

That hearing focused on how to protect civil liberties as we employ new tools like data fusion and data mining, TTIC, TSAs CAPPS II profiling system, biometric databases, and other technologies to connect and share intelligence information. The march of technology in the pursuit of terrorists raises difficult questions.

Some believe that the pervasive reach of information technology in biometrics has already killed the right to privacy, but privacy is not the only goal. I am thankful that my credit card company recognizes unusual purchase behavior and puts a hold on my credit card. It may be inconvenient for the moment, but I do want to know if somebody is abusing my credit.

The more difficult question is how much unfettered access should the government have to intimate details of our lives? Answering that question is a prerequisite as the government designs and employs new data mining tools and other technologies and systems. The new tools and the new safeguards need to be developed together.

Unless this is done, the outcome is likely to remind us of the words of Louis Brandeis, who said that: "The greatest dangers to liberty lurk in insidious encroachments by men and women of zeal, well-meaning, but without understanding."

To gain that understanding requires a reframing of the debate, a recognition that the traditional debate implies that security and liberty are competing values and are mutually exclusive. That is wrong.

The debate also assumes that our liberties make us vulnerable, and if we give some of them up at least temporarily we will be more secure. That is also wrong.

In fact, civil liberties and security are mutually reinforcing. It is not a zero-sum game. It is a positive-sum game. Security clearly ensures the freedom to exercise our liberties, but it is also true that the exercise of civil liberties and our way of life contributes to our strength and security.

Many officials, for example, are suspicious of nonconformity. I live in Venice, California. If you go out my front door onto the beach, you are in a community that does not exist in Washington, D.C.

Americans are instructed to watch for activity that is different or outside the norm, yet some nonconformity, particularly thinking outside the box, is critical to fashioning innovative strategies to fight terrorism and protect homeland security.

Pressure to conform, and John Hamre made this point very clearly in testimony before our committee, is not only contrary to the pursuit of individual happiness, but can also be counterproductive to our quest to be more secure.

Protection of civil liberties and our way of life also promotes the kind of relationship between government and the governed that keeps the nation strong and secure. Community policing, for example, has built trust between local police and citizens, a trust critical to crime fighting and now to fighting terrorism. As such, it is an increasing source of concern to many police departments.

I heard an earful yesterday from the sheriff of Los Angeles County, the largest metropolitan county on the planet. They are being asked by federal officials to undertake some activities like enforcing immigration laws that are directed at communities in which they have spent considerable time and effort building relationships.

Roles matter, trust matters, and thinking through what you are asking people to do, especially government people, has to be a very, very careful exercise.

The targeting of some communities for special attention, for example, the Arab-American community, also poses enormous problems. Many law-abiding Arab-Americans live in my congressional district. They want to volunteer to serve and to help our intelligence community. A lot of them are turned away at the door because they have relationships with people who live in some countries that are part of the "axis of evil" or that have other unattractive relationships with America. This is difficult. It poses enormous difficulties because those are precisely the people who could bring language skills, cultural understanding, and expertise to help us.

So finding much more nuanced strategies to reach for help from communities rather than targeting total communities is obviously required if our government is going to be successful, if our country is going to be successful in the war on terror.

More broadly, the pursuit of policies that otherwise deter lawful activities and increase pressure to conform may have the subtle effect of creating a sense that the government is casting a wider than necessary net. That chilling effect is what drives good information and good people underground and is obviously unhelpful to the effort to create the right policies and the positive-sum game that we are trying to create.

This is particularly true when we bring technology into play. It is not just asking people to do things that may have a chilling effect on the effort that we are undertaking, but once we bring technologies to play then the whole game changes because technologies have a reach that human beings operating on their own do not.

There are lots of people on this panel who can talk about this more carefully than I can. But something of enormous concern right now is the move to create one comprehensive watch list to catch people before they enter our country or find them when they are here. I applaud this move. I believe if we had had this on September 10, we might have been able to find at least several of the hijackers who boarded planes.

In fact, if we had had it on August 10 when we were looking for these folks in the country (they had already entered our country), we might have been able to find them and to unravel the plot much earlier.

But building a comprehensive watch list, not one integrated watch list, but a comprehensive watch list that can draw from different databases, has to be designed carefully. Controls have to be part of this and the access to the information and the targeting of the information has to be carefully thought through on the front end.

Many officials and citizens are skeptical about the government's ability to create a sufficiently accurate profile that can detect only terrorists. Many fear that the profile will miss terrorists and instead catch or inconvenience too many non-terrorists. They are correct. It is a huge concern.

Some good news is that private sector groups, like the Markle Foundation, have thought through enormously creative ideas for procedures, policies, and technologies that address privacy and civil liberties concerns raised by increased government surveillance.

I also strongly believe and urge you to support the creation of privacy and civil liberties advisory councils for agencies like TTIC. Remember, TTIC was not originally part of the concept of a homeland security structure.

The legislation that Congress wrote and passed, and that the White House, somewhere in the middle, got on board with, built in some civil liberties and privacy protection in the Homeland Security Department, which had its own intelligence fusion capability.

Later, in his state of the union address earlier this year, the president announced that by executive order he was setting up a different agency reporting to the CIA that was now in charge of fusing information.

There were some good reasons to set up that agency, but the executive order contains no protection for civil liberties. And that is why in this year's intelligence

authorization bill some of us, including me, are inserting language, which may or may not survive in the ultimate product.

We still have a conference to go through to add advisory councils to TTIC to make sure that it pays attention just as the Homeland Security Department does to the civil liberties issues involved in using human beings and databases to collect information on Americans and others in our country suspected of terrorist activities.

Protecting civil liberties must be an integral part of any homeland security strategy and is not something that can be tacked on as an afterthought. If it is tacked on as an afterthought, then we lose the positive-sum game. It becomes the zero-sum game because we are adding something on the front end and taking something away on the back end. That is an absolute recipe for getting nothing out of either end, neither security nor protection of liberty.

Any talk of expanding current law such as the Patriot Act is premature until we fully study how well the existing law is working and correct problems with the existing law. I do believe, and I think those of you who have carefully studied what legal authorities we need in the twenty-first century believe, that modernizing old law was necessary. I supported Patriot One. I did not support it because it was perfect. It was not. But Congress made a massive effort to ensure that there would be court review of these expanded authorities in Patriot One. We have to see how that is working.

I do not support taking courts out of the process, period, or any further expansion that might do that. But I do support course corrections in making modernized law work better to accomplish the goals.

Forums like this one afford us an opportunity to discuss whether narrowing the scope of new legal authorities, providing procedural or technological safeguards against abuse, or simply doing a better job of educating the public on implementation might significantly reduce the harm from new measures without significantly reducing their effectiveness against terrorism.

We must swiftly and dramatically improve America's homeland security and we must not do so at the expense of the freedoms and values that define us as a nation.

I believe we can do a much better job of homeland security implementation, a much better job, if we are more strategic about it. That would be a complaint I would level at my friend Tom Ridge. If we are more strategic about it, and if we maximize the privacy and civil liberties function in that department as we become more strategic about it.

The rights described in the Declaration of Independence and enshrined in the Constitution cannot be viewed as a luxury of peace and stability. Indeed they were expressed as the best hope for people embarking on the dangerous and daring task of creating a new nation. They are no less essential to the nation's security today.

Let me just close on this note. One of the other zero-sum paradigms that I hope we will wean ourselves off of is the incredibly unnecessary partisanship that permeates this town. I am fond of saying that the terrorists will not check our party registration before they blow us up. The terrorists' goal, as we said in the

Bremer Commission, on which I served and where Suzanne was executive director, is not to get a seat at the table, it is to blow up the table.

Let us understand that. This is a vicious attack coming our way and the strategies that we design have to be strategies that we design together because we are all in this together. It is so terribly frustrating to sit at the table in Congress and watch some of the nonsense and the games that are played and some of the nonsense and the games that were played during enactment of the homeland security legislation. So, let me just pitch this, what I believe is a bipartisan group, certainly I know CSIS is a bipartisan, nonpartisan organization, to work together to try to overcome lots of obstacles.

Turf is one obstacle, partisanship is another, and I suppose a third is the absence of creativity. If all of that is addressed at the same time and if the goal is to create a positive-sum outcome, very tough issues will be thought through for the first time in 200 years in ways that make us stronger. That is the goal. Not balancing, but dealing with, realigning security and civil liberties at the same time will make us stronger. That is what we want to come out of this.

We want to win the war on terror with enlightened policy, beyond mere toughness, with an expansion of what makes America great, which is the openness of America and the heart of America to reach out and improve the opportunity for everyone in the world. That will be ultimately how we win the war on terror. And as one little rapidly aging member of Congress, this is how I spend my daytime; this is what my experience has trained me to focus on.

You can count on my continued interest, with your continued help, to try to get this realignment right and to try to keep in everybody's mind that a trade-off is a reduction in our ultimate security.

Thank you very much.

NUALA O'CONNOR KELLY: I applaud Representative Harman's comments. She has definitely been reading and thinking about the same issues I have, and she and Suzanne and I probably are all on the same wavelength when we encourage people to strike the word "balance" entirely from the vocabulary around privacy and security. I would say, working on it from the inside of the department, that if you are doing a balancing test between the two in an environment such as this one after September 11, privacy would lose.

So I am certainly far more optimistic about the goals of my office and my ability to affect change and to affect the lifestyle and the culture of the department. So I would rather use language such as "imbed privacy" and "civil liberties" into the psyche of the department, into the culture and the structure and the function of the department. That is very much how I see it and I am very grateful that Governor Ridge sees it the same way.

In my conversations with him leading up to my joining the department, he articulated to me his sense of the privacy officer's role within and without the Department of Homeland Security. And that was one of equal footing and equal standing to the other component parts of the department in that our goal at the department is not only to protect borders and airports and other tangible assets of the United States, but also to protect the intangible qualities of the United States,

the things that make our country so great and the envy of so many around the world, and that is the freedom that we experience in our daily lives.

The freedom to move about the country, the freedom to be free from unwanted government intrusion, the freedom to think and act and pray and work in the way that we wish to, again, without government or private sector intrusion. So he very much articulated to me a sense of the department that was something I was far more excited about than other people who perceived this job as impossible. I was far more optimistic, even after meeting with him, than before because I believe he truly understands the issue and it is my job, then, to work not only with him but with the rest of the 180,000 employees that we have at the Department of Homeland Security to make that vision a reality.

I was going to step back just for a moment because Anne asked me to talk a little bit about the daily life of the privacy office and how it came to be. And, of course, we must thank Representative Harman and other members of Congress who were so supportive of the idea of a privacy office. As many of you know, this is the first statutorily required privacy office in any federal agency in the United States.

We are extraordinarily fortunate to have the support of so many members of Congress. Let me talk a little bit about the role of the office as is contemplated by the homeland security statute. It is a five-part program, essentially, in the minds of the statute drafters. The first, as I heard talked about a little bit on the previous panel, is to ensure that the use of technologies by the department does not erode privacy, but rather enhances it.

The statute also requires, obviously, some very important structural components of my office, and that is the implementation of the privacy impact assessment requirements under the government act of 2002, as well as oversight over privacy act compliance under the Privacy Act of 1974. I have also taken on work in the Freedom of Information Act area since so many of our employees who work on Privacy Act are also FOIA officers. That has also afforded me a staff of more than 300 in the department. So I was certainly willing to take on that role to have the additional resources, which really reflects our secretary's and our administration's commitment to privacy in this very important area. The statute also requires that I review legislative and regulatory proposals across the federal government and hopefully act as an advocate and as an ally for people working on privacy throughout the federal agencies. But, most importantly and most uniquely, the statute provides that my office, and that I particularly, report directly to Congress on findings, on complaints, on the resolutions, and on programs analysis, which is an incredibly unusual thing. Some of the inspectors general have a similar language in their statutes. But, it provides a level of autonomy that is important in the international community, but also an important psychological autonomy to my office. It also provides a difficulty in that we are both within and without the organization at the same time, certainly not an easy place to be, but an important one. One that, again, is slightly different from the concept of a privacy commission in other countries, but in a very good way.

Operationally, we report to the secretary in that I am outside any of the directorates and therefore can investigate and oversee without interference. But, again, with the separate role of reporting to Congress, it is a unique function whereby we both have to be educators and trainers of our employees, but also vigilant outside analysts of their activities. It is certainly a difficult position, but one that I am increasingly comfortable with because I think as internal educators we have the opportunity to truly affect the culture and the structure of this brand new organization.

The department opened its doors officially on March 1 of this year and my office opened its doors on April 20. We were not far behind the very first day of the department. When better than at the very beginning to imbed this culture, to imbed this function, to imbed this value into this department than at the very beginning as people are engaging in all the things that Representative Harman described—of figuring out what their mission is and how these new agencies relate to each other. This agency represents 22 former federal agencies. So it is not an insignificant task, it is both start-up and also huge government operation at the same time.

Anne asked that I talk about the priorities from my office. Obviously you have seen some of them in the paper already. It is the overall scrutiny of the collection of personal information in all of its many forms, whether in the basics or some things that we all think about: name, address, phone number, and social security number, or in the more new and cutting edge technology, such as the biometrics technologies that are envisioned for the U.S. Visit program. That is a fascinating conversation internationally as well, where we are talking about fingerprints and photographs and other parts of the world are talking about iris scans and DNA chips. So that is a conversation that we all need to be vigilant about, the use of new technologies to collect and disseminate information about ourselves in new ways. And, of course, the CAPPS II program that Representative Harman mentioned is incredibly important and also an incredibly challenging task of making our air safer while minimizing the impact on the individual. And, of course, the U.S. Visit Program, which is the collection of data about visitors to our country who are seeking visas.

But, structurally, we are focusing on education and training of our employees across the department, which means training people, everyone from policy analysts to data collectors to folks who work at airports to border patrol agents to Coast Guard midshipmen. That is quite a challenge of translating privacy into easily understandable and manageable and actionable items for people whose primary vision and primary goal is to find that contraband in your suitcase or prevent the transmission of dangerous people or goods into the country.

In talking about this at another event recently, we all came up with the concept of—those of you in the technology arena will know P3P—P3T, which is people, procedures, policies, and technologies. All of these elements have to be used by a privacy office in expounding on our vision and encouraging people to understand what it is to respect the dignity of the individual, whether a U.S. citizen or a visitor to this country.

Some of the hardest issues we have been working on are the use of private sector data, how private sector information is used, is leveraged, is transmitted into and out of the federal government space. I am actually quite optimistic that some of the decisions we are and can make can both leverage the incredible assets of our private sector, but also create really strong and meaningful firewalls and real walls between the databases in the private sector and databases in the government space. We all should be vigilant and concerned about the use of private sector databases, but we should not be afraid to be as smart as our private sector when doing something as important as protecting our homeland.

Another incredibly important challenge for my office is working internationally with privacy officers and commissioners throughout the world. Our framework is second to none, although far harder to explain than a simple, single privacy statute at the federal space. We have several dozen statutes in the federal space that protect privacy of financial information, of health information, of children's information. There is a multiplicity of statutory and regulatory activity, for example, the Federal Trade Commission, as you have seen in the news with the Do Not Call List, in their many efforts to enforce in the private sector. At the state level, the state attorney general has private rights of action on some regulated industries. It is certainly a harder and more complicated framework to explain, but not one that is lacking in enforcement.

The last part of my job is working not only within the United States, but also within communities that are both supportive of and also critical of the department. Certainly there are many in both camps and we are working hard to hear all of the voices as we craft a new paradigm for what it means to be secure in this century.

JOSEPH ONEK: I would like to talk primarily about video surveillance, both because it is going to be an increasingly important technology and because looking at video surveillance illuminates other surveillance and database technologies as well.

There is already a great deal of video surveillance, perhaps more in the UK than here. In the UK, there are estimates that there are more than a million government surveillance cameras. Government use of surveillance is also increasing here. The District of Columbia now uses video surveillance for special events and demonstrations. And, as in other cities, there is also massive private video surveillance, which covers in some cases just private and small areas like an elevator, but also covers in many cases public areas as well. And certainly there is a lot of interest in this. In terms of technological development, the focus on DARPA (Defense Advanced Research Projects Agency) and TIA (Terrorism Information Awareness) was on the use of various databases, but, as those of you who have studied it know, part of the DARPA-TIA program is large expenditures and research in the video surveillance area.

The reason video surveillance is clearly going to become more important is in part the technological developments. Digitalization makes it easier to use and store tapes, of course. And, we are likely to succeed sometime in the future in developing some very workable face recognition technology. If such technology

were fully developed, then we could simply take a picture from a driver's license and then run it, à la Google, through a vast array of government and private databases, which the government may have subpoenaed or secured in other ways, and in a sense, get a total picture of a person's life, to know everywhere that person has been for the last year or two years or three years. The Supreme Court, in the past, has held that there is no expectation of privacy in a public place, but I think that this doctrine will have to be revisited when the government or the private sector may have the ability to retrace your entire public life, including every doctor's office, every political institution, every religious institution that you have visited.

Let me take a look at some of the legal issues that surround the use of video surveillance and try to compare them to very similar questions with other modalities. The first question is, when do you use these cameras and what do you use them for? It is a crime to spit in Singapore. It is a crime to jaywalk here. Are we going to use surveillance cameras primarily for those kinds of offenses? Obviously we are using a lot of them now for traffic related offenses, for running red lights and so on. Are we going to use them for major felonies? Are we going to focus primarily on terrorism? How do we make those decisions? These questions, of course, arise when you have other kinds of surveillance, including ordinary physical surveillance. We have had controversies about the FBI guidelines on surveillance. The previous guidelines said that FBI agents should only go into mosques and other First Amendment implicated institutions if there were reasonable suspicion of criminal activity. Ashcroft removed that limitation and made it easier to engage in surveillance. Is that good or bad? We are going to have similar questions about video surveillance. What does it focus on? Who authorizes it? Under what circumstances? Do you need a warrant? Do you need a warrant to put cameras in particular places? Do you need a warrant to use the face recognition technology? Before, for example, you can plug in my picture and get my life story do you have to go to a court and demonstrate a need for it?

Another question is how long do we keep the videotapes? The District of Columbia has a policy that the videotapes it takes of the World Bank demonstrations and so on are kept only for ten days, unless the tapes seem to provide evidence of criminal conduct or police misconduct. That seems very reasonable and very protective of privacy. But if your purpose is to prevent somebody from blowing up the Brooklyn Bridge, ten days is not going to be good enough. You are going to have to have a much longer time span so you can see people who are repeat visitors and people who seem to be staking out or measuring or whatever they are doing at the Brooklyn Bridge. Yet another question is, who has access to the tapes? This is a key question. All of us have seen TV and movies where the private detective who used to work in the police force gets his friends on the police force to give him information about somebody that he should not have. How do we protect against that when you have incredibly sensitive video surveillance information on people? Now technology can possibly be a help here because if access is digital, you can have electronic audit trails, which may be difficult to get around. Technology is not always the problem; methods of technology, including audit trails, can, in fact, protect privacy.

Then, how and when is the videotape disseminated? This is a problem that we face in many areas, including one that Representative Harman talked about—watch lists. Watch lists serve many different purposes. You cannot disseminate one watch list to all people when you are using it for many purposes. To give one example, if you have several members of a mosque who have been convicted of terrorism, let us say in Lackawanna, it makes sense to me that some agency of government might want to get the names of some of the other people in that mosque, particularly people who were known to be friendly with the convicted members. A lot of these people are not terrorist suspects, they are just people whose names you would like to have because you want to see if their names show up again in some other context, for example, some suspicious phone call from Afghanistan. But those names are not the same as names of known suspects or people for whom there is an arrest warrant out. Presumably, they are not the kind of names that you want to ship out to every local policeman. A poor guy, whose only offense is that he went to a mosque with a convicted person, should not get thrown in the clink when he is stopped for a traffic violation. It is a very difficult issue how you disseminate and segregate information and what rules you create. This will be true for video surveillance; it is also true for all the other types of information that we are dealing with.

With video surveillance, you have to be careful about thinking of technology as a magic bullet. Obviously we have all heard of cases where video technology has been used to solve crimes. Most recently in the horrific murder of the foreign minister of Sweden, which took place inside a department store, they got two very good photos and have captured somebody who may well turn out to be the assailant. But the data with respect to crime prevention in England is somewhat ambiguous and we should not overstate the value.

There was a hearing we had at the D.C. City Council about the District's potential use of video surveillance to fight street crime. And one city council member got up and said, "There is a woman in my district and she keeps calling the police because there are drug deals right in front of her apartment and they never come and they never do anything." He said that is why we need video surveillance. But, if the police are not responding to a citizen's call, why are they necessarily going to respond any better to something they may or may not happen to pick up on a video camera? The same barriers to action may still exist—a lack of resources, other priorities, and in some cases, maybe corruption. Video cameras are not a magic solution.

To conclude, video surveillance is an increasingly important technology. There is likely to be a tremendous push to use it and perhaps to overuse it. As with other technologies that we have already alluded to and that Stewart Baker may talk about, we have to go through the methodical and systematic approach of saying, what do we really need this for and if we are going to use it, what kind of protections, both legal and technological, do we set up to assure that unnecessary incursions against privacy are avoided? Thank you.

STEWART BAKER: I thought I would talk about two topics under the heading of practical constraints in the private sector and in government on the kinds of

information sharing that we are talking about. I will start with a sort of more general discussion of the constraints that operate on government officials.

We all recognize, at least those of us who have been in government, that the first thing you have to make sure you do as an official is not lose your job. It is scandal avoidance or scandal management, depending on how long you have been in office. And, we had what I think is fair to describe as one of the worst government screw-ups ever on September 11. We lost 3,000 Americans because of government failures. So, in the two years since then, as we have struggled to find ways to deal with the problems we have had, who has lost their job? This is a scandal. One person—Admiral Poindexter. That tells you a lot about the way in which the American people are responding to what happened on September 11 and why some of the privacy issues are as important as they are. It was government screw-up, and I know some people would say that that is a little harsh, but it is actually quite proper to describe it as that.

We knew weeks before the September 11 attacks that the people who we now know were the ringleaders of it had entered the country. We knew they were, as one internal memo described them, major league killers who had been identified as Al Qaeda terrorists. They were here and we did not find them, even though we started to look for them. The failure to find those folks is the real scandal that has emerged over the last two years. And there were two reasons for it. One was that the FBI did not use its law enforcement capabilities. It only used its intelligence capabilities to go looking for those folks. It did that because of an accumulation of prior and phony scandals, which were built around privacy issues, the notion that law enforcement and intelligence had to be strictly separated, and investigations that had caused people to lose their jobs over a failure to keep those two roles separate. The other reason that they could not find them is that they did not have good information technology tools that would simply go through public records. These guys had not hidden themselves. They were renting under their own names. They were using California ID's and the like. We did not have the IT tools.

We have started to build those capabilities and we are still in the process of building them and we have certainly knocked down a lot of the legal barriers between intelligence and law enforcement. But, it is important to remember that a much bigger scandal, it turns out, than this kind of failure are things like the TIPS program, TIA, the phony debate over Section 215 and its impact on librarians. Those are the issues that are being covered in the press and the American people are coming to believe they are characteristic of the government's response and the hard issues raised by September 11. Most of them are phony, but they are part of the context in which you are going to be operating. And this is certainly a bipartisan failing on the part of Congress. I describe this as: the Democrats supply the noise and the Republicans supply the votes to kill these programs. This is an issue that you will all have to struggle with as you try to build effective responses to terrorism.

Now let me turn to the private sector constraints because they are also things that you need to keep in mind as you try to construct programs. It is not so much fear of scandal that drives the private sector. There are a couple of fears that operate there. First, you should not lose money and you should not get sued.

Those are the things that worry the private sector when the government comes calling and asks for help in gathering information. I give a lot of advice to people about responses to law enforcement and intelligence investigations and within the last month I have had law enforcement officials say, "Well, your client ought to give us this information as a good citizen. They should not charge for their costs." Although I have heard that many times from law enforcement, I have yet to hear it from somebody who is working for free. It is very important, and the intelligence community is better than law enforcement about this, that you make sure that you are, in fact, reimbursing people their costs if you are asking the private sector to get involved. And this is a continuing failing. There is an amendment pending now in the two intelligence authorization bills that would expand the scope of national security letters to financial institutions to cover not just banks, which are already covered by the ability to gather this information, but casinos and pawn brokers and a whole variety of people who are subject to other legal constraints, to drag them into this statute that authorizes national security letters for gathering information. Whoever drafted this—I suspect it was the FBI—carefully amended the definition of financial institution in the one clause they cared about, which is where they get to write the national security letter and who they get to serve it on. Right next to it there is one that provides for reimbursement. They did not change it. There you are not a financial institution if you are a pawnbroker, a casino. And right after that there is a provision that says you cannot get sued for complying with these orders. And they just did not see any reason to amend that one either. There is a kind of failing to understand what is motivating the private sector when they are approached by government, and that is going to hurt this effort for the long run.

That brings me to the last question, which is, when government shows up and asks for information, in the back of the mind of the private sector and maybe increasingly at the front of what they want to discuss, is, am I going to get sued over this? To the extent that you are helping government try to build these systems, you have to find ways to provide reassurance that this is not going to result in lawsuits. This is not just the private sector's obligation. The government has got to take action to prevent those lawsuits as well. The kinds of concerns I see—for example, I have had intelligence agencies come to my clients and ask for assistance that could be provided under law enforcement authorities that have immunities from later lawsuits. And I regret to say there is still enough residual turf-ism that they would really rather expose the private sector to the risk of lawsuit than go ask their buddies in law enforcement to gather the information and then share it. That is really not the right solution.

The most obvious situation in which government needs to worry about the possibility of lawsuits against private sector cooperators is in the international arena. It is possible to pass laws and by and large most of the laws that are in place do provide for immunity for people who respond to proper process. It is not possible for the United States government, on its own, to provide an immunity for international actors from lawsuits by data protection authorities around the world who think it is their business to determine how the government of the United States uses information about their citizens in the fight against terrorism. We have

seen in this area, particularly in the context of CAPPS II, a remarkable degree of aggressiveness on the part of the European Commission and their data protection authorities, to say, we are going to hold anybody who does business in Europe liable for privacy violations if they share this information with the United States government. Whether they actually have that authority, and whether that authority is justifiable under even European law, is not much of an issue in Europe because of their absolute determination to try to reign the United States in on almost any issue that they can get a little bit of purchase on.

That is a highly effective tactic and as you are constructing these systems you have got to ask the question, how is this going to be justified under European data protection law, which now, because of the way they have enforced that law, includes Canadian data protection law, Mexican data protection law, Argentine data protection law, and Japanese data protection law? Those laws have spread everywhere and are going to cause very much trouble for any U.S. company that does business abroad, which is any U.S. company that has data that you want.

Panel 3

Communicating with the Public Before and Throughout a Crisis

Executive Summary

One of the most important aspects of civil security is communication. In fact, communicating with the public in times of crisis, or in preparation for crisis, might be the most critical component of civil security. In addressing this issue, CSIS assembled qualified experts to look at communications from four very important vantage points: within the government at the federal level, the medical and medical support community where it intersects with the public, at the grassroots level of citizen involvement with local communities and governments, and from an analytical and behavioral perspective.

Tasia Scolinos, deputy head of the Office of Public Affairs at the Department of Homeland Security provides an in-depth explanation of how the department views its communications responsibilities and how it works to implement those responsibilities through a variety of outreach efforts. Key to this effort is treating situations as incidents, not crises. The point being that there may be any number of incidents, and none of them would necessarily rise to the level of being a crisis. The department is approaching its communications responsibilities with three corresponding strategies.

First is public education. Obviously foremost in such an effort is public information. Here the department is working to provide the public with information that will help them respond to various incidents. Broad-based in nature, this effort is designed to give people the tools beforehand, before they are confronted with an incident, so that they have put some thought into how they might respond should an incident occur. Next is an effort to test the department's plans. This Incident Communications Plan is only as good as its effect on the public, and the public's willingness to respond to it. So the department is working to ensure that everyone, across all strata and levels of government, are on the same sheet of music.

The third piece of this is relationship building before there is a crisis and communication. The Department of Homeland Security is reaching out to establish liaison functions now so that it can immediately go into action should another crisis occur. The department has created the Incident Communications

Emergency Reference Guide (ICER), which is a concrete guide, a handbook, on how the federal government will respond.

Ed Staffa, representing NACDS, presents a compelling illustration of the role of medical professionals in communicating with the public during periods of crisis. Most people do not think of the myriad details that go into effecting the proper response to a critical event. But most often, medicine is involved in some way. And local medical professionals are the key to adequate and correct reactions to particular incidents. From local doctors and nurses to emergency responders to local pharmacists, these practitioners usually are the first to identify critical abnormalities in the population that demand comprehensive responses.

Jim Pebley, recent past president of the Arlington Civic Federation, brings the discussion to the citizen-action level by providing insight into the dynamics of emergency communications at the local level. And by local, Mr. Pebley means counties, cities, and neighborhoods. During a crisis, the public needs information; in fact people demand to know what is taking place. Unfortunately, there is no "system" in place to take care of this need. So forward-looking communities are working to create emergency communications plans for their citizens. That way, information can flow down to people through a credible network of facilitators who are "vested" in the neighborhoods, boroughs, and counties and seek to provide the best, and most current, information. Jim points out that the key here is redundancy, or a "system of systems," as he calls it. Communicating with the population cannot rely on one conduit. Such reliance is risky at best, and doomed at worst. His efforts in Arlington County, Virginia have proven that multiple avenues of communication are required to satisfy the demand for information.

Finally, Dr. Jody Lanard presents the psychology of fear that transcends all communication during times of crisis. She talks about four risk communication strategies that can be useful in talking to the public early on in a crisis and as a crisis evolves. The four she describes are—and these are sort of commandments in the risk communication field—do not over-reassure, acknowledge uncertainty, treat emotions as legitimate, and do not over-diagnose panic. She lays out, with clear examples, the very real consequences of miscommunicating with the public when officials do not employ proper communications techniques. Here the results are palpable, and sadly all too real.

Discussion

JAY FARRAR: Good afternoon. I, Jay Farrar, am the guy at CSIS who is in charge of all our external relations. That is a double duty because it involves not only dealing with Congress, but also with the media. I have spent most of my professional life dealing with the media. I had a little help doing that early on in my career because I was a Marine Corps officer so we could kind of corral the press the way we wanted to. We did not have to wear kid gloves very often. But in spite of my "rough" background, Amanda asked if I would moderate this panel on communicating with the public during times of crisis and after times of crisis. I agreed immediately to do that because it is one of the most critical and important

aspects of civil security, in fact, communicating with the public might even be its most critical aspect.

It does not matter how well you are prepared or what sort of mechanisms you have in place, if people do not know about those mechanisms or they do not know what is going to happen, they tend not to be able to be one of your best allies or assets. Now, communicating may seem to be a pretty obvious issue, but if you step back and look at various past disasters, not to mention mundane activities involved in preparedness on a daily basis, you can see that communication is often a weak link in the chain. In the context of homeland security, our efforts in communicating have been a mixed bag, some good and some bad. But, with a bit of effort, and all the members of our panel today work in communicating with the public, we all can do a much better job. In fact, we have to do a better job, because when our citizens are left in the dark, left not knowing what the situation around them is, they tend to believe the worst, and that makes the situation worse than it has to be. Case in point, just with what has happened in the recent hurricane. In my neighborhood we were without power for five or six days, depending on what side of the street you lived on, and it was more of the fact that people did not know what the power companies were doing than it was not having power. So, just in a very minor situation of little consequence, people became frustrated because no one was talking to them about that issue.

For today's panel we have people who are more than qualified to speak to this issue of communicating with the public. They all have a deep appreciation for the power of communication, as well as the need to keep citizens informed. But before I turn this over, I want to take you back to September 11, two years ago in New York City, and what is one of the most memorable aspects of media coverage of that very terrible day. Most people would realize it was Mayor Giuliani on the TV on a very regular basis. There was not a time that I had the TV on where a couple hours went by and I did not see Rudy Giuliani talking to the people of New York City. He did not always have the right answers. Most times he did not even have full information about a situation. He did not always know what actions were going to take place or what they were going to try to do to solve part of the problem, but he was an authority figure. He was the authority figure for New York City and he knew that the public had to get information and they had to get information from somebody they recognized and somebody in a position of authority. And the public responded. In fact, they responded very well. As we all know, Rudy Giuliani's stock in people's eyes went up even higher than it had been. It is interesting because a new mayor was about to take office, Mayor Bloomberg. But the people of New York took comfort in the fact that he was regularly speaking to them and providing what information he could.

Well, as we all know, it is a lot more complicated than just having somebody standing up in front of you speaking, and so this panel is going to get at some of the various aspects of communicating with citizenry and the public during times of crisis and afterwards.

TASIA SCOLINOS: Thank you, Jay. I am really excited to be here today. Crisis communications is actually a pretty critical part of the Public Affairs Office at the

new Department of Homeland Security. I appreciate the opportunity to talk to you a little bit about how we approach the topic and some of the strategies that we are putting in place to move forward on this front. As most of you know by now, one of the key reasons why the president set up the new department was to consolidate previously scattered parts of the homeland mission. One of those key parts was actually FEMA. Up to this time, they had, on behalf of the federal government, done a lot of the risk communications and crisis communications work. So, at the department we actually inherited a pretty good starting point and we are attempting to build off of some of the good work that they have done.

I want to highlight that this is very much a priority at the department. In fact, within the Public Affairs Office, we have actually set up a suboffice that just deals with incident communications. Their sole focus is to come to work every morning thinking about how to increase coordination, increase communication, improve relationships, and so it is something we take very seriously.

Another quick footnote is the way that we are approaching this topic is to call it incident communications as opposed to crisis communications. A lot of times when different incidents happen, it is just that, it is an incident, and it may or may not ever escalate up to the point of a crisis. So, the department's approach is to term these things incidents and if it escalates, then it escalates. But this allows us to approach any sort of event that is happening that impacts a large number of people and put the same processes and the same approach into place regardless of whether or not it actually ever would amount to a crisis. That is an important footnote to share with you about how we envision these things.

I would like to cover three different strategies, if you will, of how the department is looking at incident communications and then just chat with you about what we are doing on each of those fronts. The first would be the public education piece of this. Second would be planning, putting plans in place and testing plans. And the third would be developing communications and relationships before there is an incident so that when there is an incident, those channels are already in place.

Just to give you an overview, I would like to touch on each of the three of those and what we are doing to move forward on them. The first one I mentioned was public education. Our thinking is that, and I am sure that many of you would probably share this sentiment, by the time an incident or a crisis actually happens, people are really looking for two things at that point. One, they are looking for timely information about what is happening with the event. What caused it, just the general facts of what is going on on the ground. The second piece that forms our perspective is, given the nature of the event that is happening, what are the steps that people need to take? If it is protective measures or if it is just turning off the gas in their house or that whole range of different actions that people may need to take in response to an incident. So we view our mission as homing in on those two things, providing timely information and also timely steps that people need to take in response to that incident, and we have broken it down into kind of three chunks. That first is public education. I would lump into this category information or input, steps, resources that you can give the public before an

incident ever even happens. I would like to particularly highlight our Ready Campaign as an example of what we are doing on this front.

As some of you may have been aware, Ready Campaign was a public information campaign that we launched with the help of the Sloan Foundation. It consisted of a website, brochures, and public service announcements featuring Secretary Ridge. The whole impetus behind this project was to get out terrorist-related information to the public now, before, in preparation for another attack, if it were to happen. It is things like: if a bio-attack were to happen, what types of steps would you take to prepare your family? If a nuclear incident happened, what would you want to do in response to that? If an incident actually ever did happen, there would obviously be a lot of people flapping around looking for information. Our viewpoint is, we can give these tools and these resources to people beforehand, before an incident ever even happens; and as some of you are probably familiar, we have suggested making a kit and making a plan and these are things that people can do in preparation so that if an incident ever did happen, there is the groundwork already laid there. That is a real and important part of that. What we are doing right now is we are expanding the Ready Campaign. Up to this point, it has just been focused on terrorism preparedness, but we are in the process of expanding that to include all hazards. And, that would go back to my comments about an incident versus a crisis. There would certainly be things that would not fall in the crisis category, but may fall in the incident category that would be man-made situations. Recently we have had the blackout up in the northeast, and things like that, and we are trying to update the materials so that people have that information before anything ever happens.

That is one piece that we are attempting to move forward on. Another way we are expanding it is we are going to be developing a business section of the Ready Campaign. This would particularly apply to people that would be in the workplace and if something were to happen while they were in the workplace, what steps should they take. Again, it would be a lot of the same things that we have recommended in the Ready Campaign. It would include having a kit on hand, having a communication plan with your family when people are at work, and then also just finding out as much information as you can beforehand about potential types of attacks or natural disasters that could happen. So we are definitely moving forward on that kind of proactive public education front.

The second kind of area that we are looking at in hopes of furthering our two objectives of getting out timely information and also steps that folks need to take is basically running exercises and testing our plans. When stuff happens you cannot just be flapping around with everybody looking at the other person saying, "Who is in charge and who is saying what?" On the federal level, with a lot of different players, obviously you are all in Washington, and know how that can be, but there can be a lot of cooks in the kitchen on these things. One of the reasons for setting up the department was to kind of earmark DHS to take the lead on the federal level with orchestrating that kind of incident communications response. We have really attempted to do that. I have referenced earlier, we have an Incident Communications Office and they basically put together an Incident Communications Plan. In other words, when something happens, what are the

steps that we are all going to take to make sure that everybody is on the same page, the information is being shared, the information is going from us to the media, that it is accurate, that it is fast, and how are we getting all of our federal partner's on the same page with that. So we have put together a plan that involves immediate coordination with our other federal partners and—the best part about that, why we feel that the federal communication is better than it has ever been before—is that we have actually been able to test this in a couple of different, both real life and also fictional scenarios. The northeast blackout was great for us. It gave us a real life test run to see how our plan would work when there was actually an incident happening. And then we were able to go back and refine some of the steps that we took on that.

Another thing that we had was, and some of you may be familiar with, the Top-Off Two exercise. This was a real-life exercise that played out in Chicago and in Seattle. There was a pretty significant media component to that. There was something called VNN, which was a mock television network that basically covered the crisis from start to finish. We basically really played it out. We were booking people on VNN. We were putting out press releases. We were holding inner-agency conference calls. It was just a very instrumental exercise in that, not only did we have a bunch of steps written out—and we were able to test it with the blackout—but we were also able to test it with the tabletop exercise in Top-Off Two.

I keep referencing tabletops, we have actually done several of those as well with our inner-agency partners where we have gotten around a table and we have walked through a couple of scenarios. We did one actually with the top communication folks at the White House about two weeks ago with the heads of each of the federal agencies tasked with incident communications. We sat down and we ran through a pretty realistic scenario and who would be doing what and when. Okay, hey, we are working through our plan here. What needs to be tweaked to make sure that this information is getting out faster and better? And, we are leaving state and locals out, so we need to work them into the plan. When you test these things, it really brings to the surface areas what might need to be honed and refined a bit. I am here today, too, to say that we have been extensively testing the processes that we have in place. Hurricane Isabel was one that we all just dealt with last week. We have been real pleased with the feedback that we have gotten with how the communication response went, at least on the federal level. We got everybody on the phone and on the same page pretty quickly.

The third piece of this is relationship building before there is a crisis and communication. This is so important. When a crisis happens, that is probably not the time to be talking to somebody for the first time on the phone. You need to have pre-existing relationships, both on the federal level, and also on the state and local level. I cannot underscore enough the importance that the department puts on that. Traditionally, the federal government has done their thing, state and local has been up here, and there has not been a whole lot of coordination. That is always going to be a difficult area where they are on the ground and we are in Washington, and there are definite challenges there. But that is something that we definitely are prioritizing at the department, going forward. We have really tried to

take some real steps. The department has an office dedicated just to state and local affairs, and that has very much increased our coordination with them.

Another thing we are putting together is something called an ICER. We are the federal government, we have acronyms for everything, and that is the Incident Communications Emergency Reference Guide. We are in the process of developing a guide that we are going to try to push out through our state and local channels to all of the public information folks that would be on-site, on the ground, handling various incidents around the country, just to make sure that everybody is on the same page. We want to make sure that the state and local folks out in Toledo or Detroit or wherever know how the federal government is looking at these things, how we are approaching these incidents, the processes that we are going through back in Washington to make sure that we are on the same page. This is a concrete guide that can give the state and locals a say, here is a handbook on how we are responding, just to increase the communication flow. We feel it has to go both ways. We want to make sure we are communicating with them and we obviously want to make sure that that channel is going both ways and that we are getting information up from them in the middle of a crisis, as well. So, we have really tried to lay some groundwork in that area. We have reached out beforehand, tried to cultivate the relationships with the different press secretaries and the governors' offices in the large cities and the mayors' offices. We are putting together this guide. When we did Top-Off Two, as I mentioned that was in Chicago and Seattle, we roped in with the PIOs on the ground there and the state and local definitely played out the scenarios that we were enacting at that time. Down the road we are looking at possibly doing a tabletop-type exercise with some of our state and local partners. So I am excited about some of the movement that I see in that particular area.

On the federal level, we interact with those folks a little bit more on a regular basis, but we are trying to institutionalize this to make sure that those relationships are solid before an incident and so we have got a quarterly forum that the department is actually taking the lead on. This is a four-times-a-year meeting just dedicated to crisis communications with each of the top federal players who have a piece of the incident communication pie, just to walk through, here is the plan that we currently have in place, do we need to refine it? Do we need to test it more thoroughly and work out some of the kinks there?

So, that is just kind of an overview of the three areas that I think we are moving forward on. We are excited about it. We feel it is an important priority and I look forward to hearing other thoughts.

ED STAFFA: It seems that we all have our own small areas of specialty when it comes to bioterrorism, emergency response planning, and so forth, and that the challenge for us all is to coordinate all of those efforts coherently. My world, as you heard, is community pharmacy, and we are interested in raising the awareness as to the role those community pharmacists and pharmacies can play in helping communicate important emergency information to patients. With a discussion like this, it is important to recognize that the pharmacist is the most accessible healthcare professional. There are days, nights, holidays, weekends, there are no

appointments that you need; pharmacists have been advising and interacting with patients for many, many years. For the past 20 years, pharmacists have ranked at the top or near the top of every annual Gallup poll of the nation's most trusted professionals. So when we need to communicate to the public about emergency healthcare topics, the pharmacist is a very credible and trusted source for patients and for the public, and for large populations to be able to get this kind of information.

There are 55,000 community pharmacies in the country, 46,000 of them are located in metropolitan areas. Virtually every household in the country is within just a few miles of a community pharmacy, which can really be viewed as a community healthcare resource. In many states, such as Virginia, pharmacists are authorized to administer vaccinations, which would come in very handy in cases where some incident would occur where large populations of people would need to be immunized against any type of agent. All pharmacists are specially trained in educating patients about medications and healthcare issues. These skills could be put to use when the public needs to know information and, as Tasia said, hopefully before an incident occurs rather than after. But, in either case, the pharmacist and pharmacy should play a strong role in that.

Many pharmacies have sophisticated sales reporting systems and are currently contributing those sales figures to government agencies or other entities that track those sales. A spike in the sale of one particular item could indicate that there is, for instance, a diarrhea medication or some type of remedy all of a sudden being sold in one place, and that could indicate some early outbreak or some early sign of an attack. So the data that pharmacies can contribute can be very helpful to bioterrorism preparedness and response. Also, because pharmacists are so closely in contact with patients, they could be trained to recognize early signs and symptoms of diseases or conditions that might be due to some type of terrorist attack. So, again, there is another potential role for a pharmacist and for the community pharmacy in general.

We did learn quite a few things from both of the terrorist attacks in the fall of 2001. During September 11, pharmacies, especially in the Manhattan area, reacted, as did many people, in immediate ways. But we also learned about the incredible ripple effect of the incident in New York, throughout the country; when the airways shut down, people were stranded all over the country, many without their medication. We learned of a pharmacy in Las Vegas that normally filled about 200 prescriptions in a normal day, which is a moderately busy store, which began filling around 1,000 prescriptions per day for all these people that needed their medicine. We learned that pharmacists across the country were limited in what they could do. For instance, there need to be more emergency regulations that would allow for, say, if there is a big need for pharmacists in Virginia, for pharmacists in Maryland to come over and be able to practice there and help out. But right now there are no emergency regulations like that. Additionally, technically you need a prescription to fill someone's medicine or you need to be able to talk to the doctor about that, in an emergency we need more regulations that say, "Hey, you use your judgment and fill that medication if you need to." There could have been ways that pharmacists could have helped more if the

regulations were a little bit more flexible or geared toward emergency preparedness. I would imagine that might be the same for nursing or other healthcare professionals, too. So some of that may need to be addressed.

When it comes to the anthrax attacks, we learned that the pharmacy supply system could react very well to an incredibly short, fast demand for a single item, in this case, namely Cipro. But we also learned that the system could be improved quite a bit. At that time of year, going into cough and flu season, Cipro would have been dispensed at roughly 250,000 prescriptions per week across the country. During the anthrax attacks, that shot up to 360,000 prescriptions a week. But, that does not really describe the extent of the pressure of the demand for that product because a typical Cipro prescription is for 20 tablets. To treat anthrax, you need 60 tablets. So the amount of demand for that product was very high. Pharmacies were put into a communications role where they were very effective in trying to educate the public. Do not take this antibiotic prolifically. Do not get a supply just in case. And we believe we were very effective in that role, however, it is so hard to measure how many people obtained a Cipro prescription unnecessarily, how many people used it unnecessarily, or how many people got it, stuck it in their medicine cabinet and then went off like three months later and took it because they thought they had an infection. This is a very powerful antibiotic. There are some significant personal and public health concerns to using an antibiotic inappropriately like this, not to mention the financial costs. One prescription for Cipro, 60 tablets, is roughly $400. Who knows how many people just got it because of panic. In the large cases nowadays, most people get their medications like this covered by insurance, but that is quite a burden on the healthcare system in terms of cost. The main problem is (a) people might have been using it unnecessarily and maybe to the detriment of their health, and (b) they may have been getting this product and not needing it at the expense of somebody who needs it. So, this type of information is something that we could learn from. If those attacks were a little bit more widespread—the demand, for the most part, was met. There were some shortages, but the demand could have easily outpaced the supply for this type of drug.

One other thing of note on this one particular product that we learned, all along there were two products available that could have been used in place of Cipro. They are called oxycycline and good old penicillin. Both of them were readily available, plenty of stock, relatively inexpensive, and equally capable of treating the condition. The problem was that their labeling did not specifically say, treats anthrax, as did Cipro. So, physicians, the public, people did not want anything that was not specifically labeled for it. We, as a pharmacy group, and a lot of other healthcare groups, knew that these products could effectively treat anthrax exposure, but the communications message did not really come across well. We were not the definitive source for that. What we needed was somebody to step up, like someone in the CDC or the FDA and just simply say, these products can be used to treat anthrax, plain and simple. Eventually that did happen, it probably took close to two weeks. Once it did happen, it was amazing how the strain on the supply system went down and how these other products began getting prescribed and dispensed. So there are some lessons to be learned in terms

of communicating information to the public that we learned from the Cipro event.

In the case of a nuclear event, there would be a run on potassium iodide tablets far beyond what there was for Cipro. But there would be a great deal of misperception by the public as to what those tablets really can do. Many people in this room, being that you have bioterror exposure, know that potassium iodide tablets are only effective against radioactive iodine, per se. They would probably not be effective for most materials used in a dirty bomb. So potassium iodide would not be of any use in that case. If it were effective for a particular type of radiation, it would only be to protect your thyroid and not other parts of your body. But I would venture to say that the vast majority of the public would clamor for potassium iodide as some type of a product that would render them immune to a radiation event of any type. There is just a public psychology, a lot of misinformation, and as Tasia said, it is important to communicate to the public ahead of time. This is only one example of types of medications that could potentially be used in the cases of bioterror events that we probably all would do well to begin educating people now about the proper use of them and when it is appropriate to use them, how to use them and so forth. Let us just use that as an example.

Just a couple of other things that I wanted to mention in terms of the pharmaceutical outlook of bioterrorism and how it all blends in with other things. We all recognize the high price of prescription medications, the reasons why people get their medications from Canada and other foreign countries, but we are concerned that the more this happens, the more the likelihood that bioterrorists can capitalize on that lower level of regulation and somehow get tainted medications into our medical supply system because of all of the importation into our country. We have seen some incredibly sophisticated examples of counterfeiters and their abilities to counterfeit medications and it may be that terrorists might want to taint the drug supply. It may also be that they would want to get into the counterfeiting drug business. There is huge money to be made in that. And there is evidence that bioterrorists are funding some of their effort by counterfeit drug activities.

Those are just a few of the thoughts that we have from the pharmacy perspective. The pharmacist, in our view, is the healthcare professional that can really interact closely with the public, be a trusted source of information for the public, and the pharmacies themselves can be easily accessible healthcare centers in times of emergency or in times of the need for public education.

JIM PEBLEY: Just to explain how a guy that is working in system engineering got involved in public communications, it was during my second tour as the Arlington Civic Federation president. I made the mistake of commenting to the nice lady with the blonde hair that I felt we needed more emphasis on public services in public safety. Along came September 11, it happened in Arlington, not just in Virginia, but also in Arlington. It was our fire department that got there first, a lot of our citizens that stood outside and scratched their heads and said, “What do we do?” And we were confounded by a communications problem

between the government and the public. After about four months of looking at how things worked, I talked to Kim and I said, "Kim, we need to recruit Jackie Snelling," who is sitting right next door in the black dress, who is the head of our Citizen Corps Council. But Jackie is a formidable force in Arlington and she twisted enough arms, beat on enough doors, and talked enough ears off that we have a national active Citizen Corps Council, the kind that the president had in mind when we talked about that. To get even, after the fact, Jackie decided to break the Council's work into four pieces: volunteers, resources, education, Kim's been tapped for education, and she said, "Jim, why do not you handle the effort of public emergency communications?" I said, "Okay, no problem"; I should be able to knock that out in a couple of months. I work with engineers and we have a different way of looking at the world. You think the glass is half-full or half-empty, we say the glass is twice the size it needs to be.

So, we gathered together a group of individuals from across the county, a ham radio operator, a lady that is hearing-disabled, a former SES from DOD, and myself as chair, and we set off to try to find what we needed to better communicate after the fact, in an emergency, when the system and the infrastructure is stressed. What I have is the product of our work: a couple of letters that we have written to the county manager, the most recent is a draft—so I can disclaim any credit for it in case I wrote something down wrong—that said, "Dear Mr. Manager, after working on this from January until this month, this is what we think you need to do to make communications more resilient, more reliable and more redundant in the county."

I would like to get into a couple of things about how you do a public emergency communications planning because we learned it as we went and it would be nice if we could save a lot of other people. Jackie's original task was to involve the community in developing and testing plans designed to reach all the members of the community, including those with visual impairments, physical and mental disabilities, and people with limited English proficiency. I have a member who works for the Federal Deposit Insurance Corporation who made up a spreadsheet of where everybody is, what they are doing, and how easy it is to communicate with them. And when you start going through this spreadsheet, you realize you have to deal with people that are working in the county, but they are not in the county after work. You have got people that are in the county, live in the county, and work in the county. You have people that are hearing disabled, you have people that are blind, you have people that speak any number of languages. I would challenge you to guess what the third most-spoken language in the county is—and it involves Ethiopians and Somalis. The challenge of just getting the right language to get a communications message out is pretty tough.

What are the public expectations? The public expects us in an emergency to find a way to get to them and tell them what is happening and what they should do about it. They expect us to have planned ahead on this. It is my experience, in looking across most of the United States, that we are not in real good shape. I will explain and talk a little bit at the end about lessons learned from Isabel. What I discovered is, as we went through, that there is no system. There is no magic system out there that will insure that you can reach out and touch the public and

talk to them. Every one of them has at least six "yeah, but's." We'd like to have sirens. Yeah, but, what if somebody is deaf? Or, yeah, but, what if they are in a building that is medically sealed, like we see a lot of them, and they are three walls in? You can go through that. What we discovered was you need what we called a system of systems. They have to overlap. They have to repeat. They have to be redundant. And you have to come at the public from a number of different ways because, as we found out in Isabel, there is a county cable TV channel that puts out information, and there is a county website that puts out information. We also have an Internet website that puts out information. This last Sunday when we wanted to tell people that they could go to one of the high schools and get ice, the people that needed it did not have any power and could not receive the message. That is the challenge, as you have to think about all the different possible combinations and types of disasters and incidents and attacks out there to make that system resilient. And so it becomes an expanding and difficult problem to try to figure out how to lace together a set of systems to make it work.

There are two basic types of emergency communications. There is the alert that says, something has happened, you need to go get more information. That second part is the information. Some systems will do both, some systems will only do one. A siren that goes off is an alert system. The EAS, that is the Emergency Alert System scroll that you see on your television, the one that sounds like a combination of a little kid scratching his fingernails on the chalkboard and a belch, gets your attention. And then there is this scroll that tells you what is happening and what you should be doing about it. That is an information system. The problems are that you have to look at that in its entire context and see what percentage of the population you are going to be able to reach. Having gone through all of those, I will walk you through what we decided after seven meetings and eight months of looking at the different systems and what we could do and talking to people. Please remember, these are all volunteers, they all have different interests and many times in many of these meetings it was like herding cats.

Advanced reverse 9-1-1. This is the new system that is able to take a message and dial through all the phone numbers in the county in a relatively short period of time and alert people and tell them a very brief message. Obviously that takes a lot of computing and telecommunicating power. It is not as efficient and as fast as you would like, but it is a very, very effective system because what it does is it takes the computerized message and it goes out to the Arlington County system and grabs phone lines coming in that can be used to send out the message. Right now the system we are looking at buying purportedly could get through somewhere in the neighborhood of 10,000 calls in a matter of 10 minutes on an ideal day, and that includes scenarios with the power and the phone lines being out. We are interested in that system and that is our top priority. The fax blast we added in there was so that that system could also take a message and immediately transmit it to all the doctors offices in the county, because doctors always put you on hold when you call, but whenever the HMO sends a sheet over the fax, they grab that right away. We hope that the fax blast will say, "Hey, there has been a biological incident, here are the symptoms, here is the treatment, here is where the county is operating."

Advanced technology siren system. Whenever we went out to the community and talked to the citizens, their first question was, what happened to the sirens? We thought we still had sirens. The Dacono red sirens went away in the seventies and were replaced by the Emergency Alert System. The sirens are not out there anymore. There is a lot of technological prejudice against sirens. A lot of people say, that is old technology, it will scare people, and we can do better than that. Well, we went out and we got some of the manufacturers of siren systems for nuclear power plants and sirens have gotten an awful lot smarter. Sirens can be dual-powered from battery and from line voltage. They can be dual-operated from radio wave or via telephone line. They can link and you can just alert a region. You do not have to set all the sirens off. They self test and you probably will not hear them because it is a three-second blast of white noise. And, not only that, but they are smart enough that if they break and you have a maintenance contract, they will dial up the manufacturer and say, "I am broken, please come and fix me." And for the population that is most at risk, that is the population that is out of doors at a soccer game or they are walking down the street or they are going shopping, that is the population that you would like to get through to the fastest, a siren may be the best way to do it. A lot of the new siren systems are speaker-based, and therefore you could put out a message to the county saying, "Hey, get back inside, shelter-in-place, take the following steps, goodbye." The best part about the whole system, from a taxpayers point of view, is that we could rig the whole county with ten sirens, which is twice what we need, so we have the overlapping feature, for under $400,000, which, in this day and age, certainly sounds like a bargain.

Acquisition and licensing of a county radio station for emergency information. We wrote this five days before Isabel, and Isabel has proved the case for us on the fact that if you are going to wait for WTOP to roll all the way through what is going on in your county and you have fallen out of the mix on how high of a message you want to get out, having your own radio station would be extremely helpful, especially if the phones are powered by that little transformer and it is not working at your house. The chances are that you are going to still be able to listen to a radio because the kids have one, you have one, there is one available, or you have planned ahead and you have got spare batteries. We think that a radio system would be the best way to communicate with people. And with the new FCC move to allow the licensing of low-power FM, that is 10- and 100-watt, we think that we could cover most of the county with a 100-watt radio station used for exclusive county use for emergencies or multi-use with the schools for probably under $40,000, which is a very cost-effective way to spend your money on communications.

Finally, I have put in RSAN with no charge emergency messaging. RSAN stands for the Roam Secure Alert Network. The county went right out after September 11 and their first purchase was a system that would allow the Emergency Communication Center and the director of Emergency Management to send a message out through text messaging cellular phones, on the Internet, and through pagers. If the county signed up, if the populous signed up, they could receive those. That turned out to be our best messaging system after Isabel when

the power was out and we wanted to talk to people. The problem was that we only had 3,000 people sign up and many of those were county employees who were encouraged to sign up. Our sign-up has jumped 25 percent since people got their power back, but we want to try to expand that. The other thing that we are doing is a petition that the task group has endorsed saying that we really think that we should consider asking that there be no charge for emergency text messaging. Right now, on a cellular phone, you have to pay a fee for enabling it and you have to pay for some sort of plan on how many messages you can receive. We should be able to enable that on those phones. It would be much more effective because what we need more than anything else are what we call passive systems. You are most effective at communicating with the public when the public does not have to do anything. In other words, if you could get to them on the phone, if you could get to them while they are watching the TV, they are not having to sign up for anything. They are not having to buy anything. They are receptive to communications.

We made a number of other recommendations. I am not going to go all the way through them for the sake of time. We had quite a talk about how to handle the problem with the hearing impaired. That is probably our biggest challenge right now. And we are looking at free or subsidized pagers, text-messaging pagers for low- and fixed-income hearing disabled, as a potential solution.

Finally, future systems. If I had unlimited funds and I were going to build some new technology, I would build the two following items. I would build into our telephone system the capability to ring every phone in every house inside, let us say, a zip code. If you could ring that phone for 30 seconds, and if the public knew that a 30 second continuous ring on their phone meant an emergency, that would be your magic bullet for getting to most of the public. Now you say, "Yeah, but, what about cellular users?" On the other side of the technology wish list would be the ability to ring certain cells. In other words, reach the cell phones within a certain cellular area and you could expand that and send them an emergency message all at the same time. So, for anyone who is here from the FCC, come talk to me afterwards, I will buy you dinner.

We found out a couple of important things. Number one, one size does not fit all for every kind of community. We looked at a lot of different models, probably the best model was the Midwest model for tornado alerts. In the case of the Council of Governments here, our county manager has said that what he wants to do is to do what the rest of the region, that is the Council of Governments, is planning on doing. Unfortunately, we need to look at that as more of a toolbox, we need the Council of Governments to say, "Here is a set of remedies and steps you can take"; and we realize that not everything fits. Because, if Fairfax looks at us and says, "Sirens?" They have to spend millions and millions of dollars to cover sirens and they have got lots of trees that are going to knock down the transmission of that siren noise. Whereas it would certainly work for Arlington, it would probably work for the District.

Education on communications. I have talked today about all the mechanics of trying to get through the message of what you say and in a second you are going to hear the right way to say it. It is going to be extremely important and you need to

do a lot of it. Also, one of the things the task group has looked at is the need for a nationwide exercise on emergency preparedness. Sound the sirens, ring the bells, tell everybody that on this day, at this time, where you live or where you work, we are going to have an exercise and that is the time we want to see if you can hear us. That is the time we want you to stop and think about whether or not you are prepared. And then give everyone some time to go back and look at the lessons learned. As far as Isabel goes, if there was anything good about Isabel, and I know I am talking to a lot of people that have been blacked-out for a while, we had a chance to see what worked in our system and what did not work. The county managers asked our task group to go back and help lead a postmortem to see where we need to go. That is my pitch.

JODY LANARD: I am going to tell you about four risk communication strategies that can be useful in talking to the public early on in a crisis and as a crisis evolves. Most of my risk communication examples are about how the public health community and the public communicate about crises. It is not really about defense and intelligence, but there is one example from most of your field that I would like to start off with.

The smallpox vaccination program is an area where better risk communication between the homeland security community and the public health community might actually help. As you know, there is a wide split between the two communities. The homeland security proponents of large-scale smallpox vaccination did not learn enough about the reservations, fears, grief, and anger in the public health community. The public health community had long celebrated the eradication of smallpox as its proudest achievement. All their misery and anger got displaced onto the liability, compensation, and adverse side effects issues, which were very much a red herring. Perhaps the homeland security and defense community could at least use one of the risk communication strategies I will describe in working with the public health community in the future, and that is the strategy of learning about your stakeholders' fears and acknowledging their anger and their misery. This morning, Stewart Baker spoke about the need for agencies to understand the motivations driving the private sector. Agencies need to learn more about each other's inner motivations as well and two-way risk communication may help with this a bit.

I am going to describe 4 of 12 main risk communication strategies and then at the end, if I have time, I will just read the rest of the list. The four I am going to describe are, and these are sort of commandments in the risk communication field, do not over-reassure, acknowledge uncertainty, treat emotions as legitimate, and do not over-diagnose panic. In recent months, I have gotten some questions that I will use to discuss these issues. Sean Kaufman, from the CDC Office of Terrorism Preparedness, and Amy Weir, from the Northern Virginia Community Resilience Project, asked about communication before and during a crisis. They wanted to know, how do you convince colleagues that it is necessary to stir people up? And they were not talking about you people. You know it is necessary to stir people up. But in the public health community, and on the very local level, there is a lot of resistance to stirring people up. Amy and Sean wondered, is it still

critically important to keep saying that there will be future terrorist attacks? Are we at risk for scaring people and drawing criticism for doing so? And then Dick Thompson from the World Health Organization in Geneva wanted to understand the public's response to SARS in order to craft communication during different phases of the outbreaks. Like most organizations, WHO found it hard to achieve the exact right to grieve public alarm. They discovered how frustrating it is, especially when the public overshoots and starts taking unrecommended precautions. And, of course, this happened in the United States with Cipro, also.

Here are a few of the principles of my brand of risk communication with good and bad examples from real life to illustrate how they can work in practice. The first principle is, do not over-reassure people. If anything, err on the alarming side. Do not express overconfidence about data you do not have yet. This is the first thing that usually goes wrong in crisis communication and it usually has the best of intentions to try to allay the public's fear and prevent panic. But since genuine panic is rare, and I mean genuine panic, people rampaging in the streets, premature reassurance is unnecessary and over-reassurance backfires badly in two quite different ways. If people are worried, the over-reassurance leaves them alone with their fears. And if things get worse, the over-reassurance damages institutional credibility. Mayor Bloomberg over-reassured New Yorkers in the first hours after the recent blackout when he said, "I can tell you 100 percent sure that there is no evidence as of this moment whatsoever of any terrorism." How could he have known that so quickly? It was days before anybody had a clue what was going on in that blackout. And even though the mayor used hedging words, CNN ran a caption underneath his speech with the words "100 percent sure" at the bottom of the screen.

Former EPA administrator Christie Whitman did the same thing on September 18, 2001 when she told New Yorkers that the air near Ground Zero was safe to breathe. It turns out the EPA did not have nearly enough data to know this. Now an expensive epidemiological study is about to start and a very skeptical public will eventually receive it. One more bad example and then I will at least tell you how somebody can do it well. Former British agricultural minister John Gummer over-reassured the public when he told everyone that mad cow disease could not be transmitted to humans. He said that hamburgers were perfectly safe. He fed his daughter, Cordelia, a hamburger on television to show his confidence in beef. This is the most famous picture of his whole administration. A few years later, dozens of young Britons began dying of mad cow disease. He thought that not eating beef was panic. It was not panic. It was pausing. The public was pausing to wait for the data to catch up. It was devastating for the beef industry, but it was not panic and it was not irrational.

An effective alternative to premature over-reassurance is to acknowledge uncertainty and help people bear it. The master of the universe at doing this, as far as I am concerned, is CDC director Julie Gerberding. She regularly demonstrates one excellent way to convey hopeful but uncertain information before all the data are in. Dr. Gerberding typically puts the positive, hopeful, good news in a subordinate clause and then emphasizes that the fat lady has not sung yet. It goes like this. "While we have lots of reasons to think that the SARS outbreaks are not

due to terrorism, we are keeping an open mind and being extremely vigilant." And then later this summer she said, "although we have not seen community transmission of monkey pox, we are not out of the woods yet." And she uses, "we are not out of the woods yet" a lot. It is almost like a tick. It is a way of not over-reassuring the public. And if you think her rhetorical structure is an accident, listen how Dr. Gerberding responded when asked about a fringe crazy hypothesis that SARS came from outer space. It had to be a very quiet day on the news front when a story like that made the papers. At a CDC press conference, Anita Manning from USA Today said, "Dr. G., I just have to ask you about this outer space thing. What do you think?" And Anita Manning was really embarrassed to even ask this question. Dr. Gerberding answered with a wicked twinkle in her eye, "although we have no evidence that SARS is from outer space, we are keeping an open mind." I attended every one of their telebriefings by call-in and I talked to Anita about this afterwards, the reporters in the room roared with laughter in recognition of Julie Gerberding's intentional conscious rhetoric of uncertainty. And the CDC's CDCynergy Emergency Risk Communication training program actually lists this as one of its recommendations. Put the good news in a subordinate clause and then tell people you do not have all the information yet.

The next two principles are to treat emotions as legitimate and to stop over-diagnosing panic. I recommend that you acknowledge that the situation is scary when it is and show that you can bear it. This is what Mayor Giuliani did so superbly in New York, among all his other talents, when a reporter asked him how many people had died on September 11. He looked miserable, he looked completely destroyed, except for the fact that he was coping, and he said, "more than we can bear," but he was bearing it.

Public officials in general, however, are very intolerant of public fear, which they see as joined at the hip with panic. Typically, leaders see public fear as joined at the hip with panic, but fear ranges across a wide spectrum. Most fear is tolerable, some is even useful because it motivates you, and only a little bit of fear is joined at the hip with panic. Typically, leaders and public health officials tend to box with the public's fear as if trying to knock it out. Risk communication, however, in a crisis, is more jujitsu than boxing, respecting the public's fear, allying with it, helping the public pivot on its fear toward appropriate vigilance, attentive learning, and productive preparedness. Too many crisis managers simply believe that it is wrong to frighten the public. In a very widely-cited article from *Lancet* on May 7 about the ever-worsening data on SARS case fatality rates from 4 percent to 6 percent to 8 percent to 10 percent, Donnelly et al. wrote, "This epidemic has shown the need for a communication of risk that will inform and warn the public…without inducing raised anxiety and fear." This is the holy grail of risk communication, to inform and warn the public, to get them to respond appropriately to scary new information without actually scaring them. Telling people about a frightening situation without scaring them is like trying to break up with your boyfriend without hurting his feelings. It cannot be done. I have tried. So, instead of rebuking people for their fears, validate and share the fears to the extent that you can.

Now I want to tell you my very favorite example of good risk communication that acknowledges the public's fears, and, just for the sake of brevity, I am going to give you one that not only acknowledges the public's fear but also uses the subordinate structure for the good news. This is my favorite story. When North Carolina had a case of Eastern Equine Encephalitis, state epidemiologist Jeff Engle said the following at a press conference, "even though there have only been 12 or 13 human infections since 1964 in our state, fear is appropriate. I mean, my God, here you have a mosquito that can kill. What we are trying to do through you guys, the media, is use that fear in a positive way. We are trying to get the information out there." Now, I am very sure that Dr. Engle did not generate any panic. He generated preparedness. And the way I know this is that he told me the next day that all the local Wal-Mart's sold out of insect repellent after the press conference.

What is the opposite of "there is no need to panic?" Officials should stop defensively misdiagnosing the public's emotional rehearsal and panicky disobedience as panic. And this applies to some of the Cipro stories, too. I thought that was disobedient. I did not think it was panic. The public did not know whether those pushpacks were going to arrive. They had never been tested. They did not trust the system. They were sending a signal of distrust, not a signal of panic. Never, ever accuse the public of being irrational or hysterical if a reporter is within earshot. They will put it in the story and it sounds insulting, even when it is occasionally true.

Here is what I think happens. The public sometimes acts as if a potential future crisis is already happening right now. This is emotional rehearsal. In exact parallel, officials sometimes think that the public is already panicking because that is what they are most afraid of. When the public is merely practicing, like wearing masks in advance of a feared epidemic, pausing, avoiding travel, maybe even avoiding Chinatown while you wait to see who is going to get sick, and, generally, just emotionally rehearsing. In psychiatry we call this an adjustment reaction, not panic. And an adjustment reaction is the moment when officials have the maximum chance to have an impact on how the public adjusts. Officials often throw away this opportunity out of their own fear, frustration, and defensiveness. Now fear has a curve. When something bad happens, fear and anxiety go way up and then people pay a lot of attention and they do not panic usually, so they have a lot of attention and energy to learn the new stuff you are trying to teach them. And then the fear goes way back down, usually to normal, but maybe now you are just as scared as you always were, but you are more scared of terrorism and you are a little less scared of genetically modified foods because everybody has kind of a set point for fear.

The reason public officials are afraid of scaring people is they are always afraid that it is going to increase the fear burden. But I have never seen that. The main problem is complacency. The initial fear reaction subsides, use it well, teach people, and then if you are lucky, you go into PR mode and you are competing for their fear. You want them to be afraid of your risk. You want them to worry about terrorism preparation. You want them to stop worrying about school shootings or whatever else they are worrying about. People worry too much about public fear.

Now I am going to tell you something that might hurt, maybe not you, but it hurts public health officials a lot when I tell them this, officials often experience public fear as a personal criticism. Once an official takes the position that some particular risk is small or that it is under control or that some precaution that the public likes is really unnecessary, the official's ego inevitably gets invested in people responding as instructed. If the public continues to be fearful and to take precautions the official said not to take, the official naturally feels irritated and unaware of the role of injured self-esteem—and I am a shrink so I have to get injured self-esteem into each speech at least once—unaware of the role of injured self-esteem and his or her response, the official may strike back at the public. So when the public is hoarding Cipro during the anthrax attacks, or when cab drivers in Toronto wanted to wear N95 respirator masks in the early days of SARS, despite your best advice, they are saying to you, the officials, we do not believe you or we do not trust you or you have not convinced us yet that you know what you are doing. This is the public answering you back, not the public panicking. And when you counterattack to the press, people are irrational and the media are fanning the flames of public alarm, that is emotionally understandable, but it is not technically sound or strategically wise. Instead of blaming the public for doubting your reassurance, take their signal as a free consultation telling you that your message is not getting through.

JAY FARRAR: Thank you Jody. And let me also say that you can get this on the Web site at www.psandman.com. I read this yesterday, it is phenomenally good, and I would recommend reading it to all the professionals here, and even the nonprofessionals here.

Panel 4

Protective Action Responses: Shelter, Evacuation, Quarantine, and Medical Countermeasures

Executive Summary

Protective actions—the steps that individuals can take before and during a terrorist attack to save lives and reduce losses—are a critical element of homeland security that necessarily involve the American public. Protective actions include different forms of sheltering, evacuation, quarantine, use of individual protective equipment (e.g., clothing, respiratory gear), and a variety of medical measures (e.g., antidotes, antitoxins, antibiotics, and vaccination). An expert panel composed of Representative Christopher Shays (R-Conn.), Dr. Lynn Davis (RAND), Jerry Hauer (Department of Health and Human Services), and Jason Sapsin (Center for Law and the Public's Health, Johns Hopkins University) addressed issues of concern in the area of protective actions as they relate to the American public.

Representative Christopher Shays highlighted the unevenness of protective action plans for evacuation, shelter, and quarantine at state and local levels. Hearings before the National Security Subcommittee of the House Government Reform Committee have focused on the lack of consistent capacity to respond to mass casualty events and the need to establish national preparedness goals and standards. Representative Shays also noted the deterrent value that medical countermeasures can play in discouraging biological attacks against the United States, in addition to their practical value in a crisis.

Jerry Hauer focused on epidemic control, highlighting recent progress in the medical countermeasures area and in exposure control (e.g., isolation or quarantine). The SARS outbreak showed that isolation and voluntary quarantine can enable disease control without more restrictive measures. Other measures to reduce contact such as restrictions on group events and closing mass transit are

also effective tools to reduce disease transmission. Mr. Hauer further noted improvements in the Strategic National Stockpile (SNS—formerly the National Pharmaceutical Stockpile), which is designed to provide medical countermeasures to the American public on short notice from multiple locations around the country. Since September 11, 2001, the SNS has been expanded to include countermeasures for the majority of the most dangerous biological agents (as determined by the Centers for Disease Control and Prevention). Despite these advances, however, the surge capacity of the U.S. healthcare system to handle a terrorist event that requires mass care is lacking and must be addressed on a priority basis.

Dr. Lynn Davis shared a methodology developed by RAND to determine what individuals can do to respond in the event of a chemical, biological, radiological, or nuclear (CBRN) attack. The approach is grounded in specific attack scenarios and focuses on steps that could be taken to assure personal safety and survival in the absence of guidance from officials or emergency responders. RAND's approach highlights the necessity of tailored responses depending on an attack scenario rather than a "one-size-fits-all" response. For example, in a chemical attack, the greatest need is to find clean air, whereas in a radiological attack, the greatest need is to avoid inhaling contaminated dust particles. Individual Americans must understand in advance what to expect in circumstances involving CBRN attacks and be ready to act on short notice if they believe one is under way, because simple steps can, in fact, make a difference.

Jason Sapsin described work at the Center for Law and the Public's Health to update public health law for emergencies—in particular, quarantine and isolation protective actions—in the aftermath of the September 11, 2001 terrorist attacks. Laws at the state level vary considerably and are in many cases outdated relative to modern disease control techniques. The center's 2001 Model State Emergency Health Powers Act (MSEHPA) represented an effort to update and clarify public health law for protective actions. Some 32 states and territories have updated their legislation based on the MSEHPA initiative. Although each has done something different, continuing the patchwork effect of public health law at the state level, updating such laws is an important element in improving states' capacity to manage an infectious disease outbreak. Many state public health departments continue to have concerns about their lack of access to information about relevant health law, however.

Discussion

AMANDA DORY: What I want to do is put out four challenges, just quickly, as food for thought, and perhaps our speakers will address them, and, if not, in the Q&A. But I think there are four components that we need to consider. The first is planning. The second is communications. The third is decisionmaking. And the fourth is compliance.

In the area of protective actions, it is incumbent to have a plan in place to be able to execute when it comes time to pursue a particular protective action. At the

national level, at the federal level, we have what used to be the Federal Response Plan and now it is becoming the National Response Plan. So there is definitely a plan in place to manage all different kinds of disasters. At the state and local level, those plans are much thinner. Some states and some localities have plans for sheltering, for quarantine, for evacuation, but there are many more who do not. And then when you get all the way down to the individual level, some families have them, but many more do not. But it is really the state and local level that is the connective tissue between the Federal Response Plan or the National Response Plan and what it is that individuals will do in a crisis. So we need to have plans in place.

Now, having the plan is great, but if people do not know that it exists or they do not know what it is, it is not very helpful in a crisis. And so the communications piece is very important, particularly in this area we are talking about—the interface with the public. The public needs to know about the plans, what is planned for them, and how they are supposed to react as part of a plan.

The third piece that is a tremendous challenge is the decisionmaking process for officials. We have heard a little bit about this today in some of the discussions. For example, as we heard from Governor Gilmore in the luncheon discussion, it is a tremendously difficult choice for elected officials to decide whether to recommend to a population that they shelter-in-place, or that they get on the road and evacuate. There are so many pros and cons in terms of: what would save more lives, what is more costly, is it too soon or is it too late to make a recommendation? You may have read in the *Washington Post* this morning, the criticism of some of the officials in Northern Virginia about whether they recommended an evacuation too late in the Alexandria area from Hurricane Isabel. There will always be second-guessing on those kinds of decisions, but for the actual decisionmaking process, we do not have good decision tools at this point to help officials make those difficult decisions.

The final component I would mention is the idea of compliance. We heard a little bit of this in the risk communication panel, which is what do people do when you make a recommendation or direct that individuals take a certain path? We talked about the anthrax mail attacks, usage of Cipro, and whether people were complying with government recommendations.

So, with those four challenges in mind, I would like to turn to our expert panel today. Our first speaker, to my right, is Representative Chris Shays.

CHRISTOPHER SHAYS: Thank you all very much. Let me begin with a general observation as a context for our discussion. Protective responses to chemical, biological, radiological attacks here at home seem to be proving more problematic than anticipated. Now, despite the horrors of September 11, the threat of unconventional attack at home has not been clearly assessed or communicated. So federal strategies to address the vulnerability du jour—anthrax yesterday, smallpox today, SARS tomorrow—are at risk of being lost in the shuffle of more immediate priorities. Specifically, I think the rush to duct tape, some months ago, oversold the benefits of shelter-in-place strategies except, frankly, maybe in New York City. If the average rush hour is an indication, mass evacuation plans appear

unrealistic. Quarantine authority is based on an unwieldy patchwork of antiquated state laws and limited federal authority. And agent-specific medical countermeasures are difficult and expensive to develop for a marketplace we all pray will never exist. So, over the course of numerous hearings on terrorism and local preparedness before the National Security Subcommittee, it became clear the capacity to respond to mass casualty events varies wildly and unacceptably across jurisdictions. Public health surge capacity is limited, trained personnel are scarce, and public shelter and quarantine procedures have neither been explained nor exercised. We already know efforts to prepare for unconventional attacks here at home are demanding substantial resources with little or no sense of the end state we are hoping to achieve without spending.

As a result, response programs remain uncoordinated and unfocused on the most imminent threats. A recent report of an independent task force sponsored by the Council on Foreign Relations (CFR) concluded the nation's emergency responders remain, "dangerously ill prepared to handle a catastrophic attack on American soil." The panel, chaired by Senator Warren Rudman, concluded, "Without establishing minimal preparedness levels and equipment and performance standards that the federal government and state and local communities can strive to attain, the United States will have created an illusion of preparedness based on boutique funding initiatives without being systematically prepared." At our recent hearing on the CFR report, there was a bipartisan consensus that the standard-setting efforts mandated in the Homeland Security Act last year will not produce the overarching preparedness goals needed. We are working on a legislation proposal to unify and accelerate those efforts and we are going to introduce it next week.

With regard to medical countermeasures, deterrence is not deployment. As with nuclear weapons, the value of medical deterrent should lie in not having to use it. The mere existence of the research, development, and acquisition activities, such as those called for in Project BioShield, should discourage biological attack on any massive scale. With regard to the National Pharmaceutical Stockpile, again, based on testimony at our hearings, it appears the National Pharmaceutical Stockpile program is an effective deterrent capability. If properly managed and updated based on current threat assessments, the availability of stockpiles in the hands of a trained and equipped public health distribution network should convince would-be biological terrorists that their efforts are better directed at other means of attack.

Finally, the most effective protective action response is candor. Against terrorism generally, and in this realm specifically, information is the most potential inoculation against the infection of fear. Thank you.

JERRY HAUER: It is a pleasure to be here with you today. I will be brief. I think Representative Shays hit exactly the right issues. I could not agree with him more. He and I have been on a number of panels, TV shows, together, and I think we are of the same mind. Since one of the topics we have been asked to address is countermeasures and infection control, what I want to do is take a little different bent over the next few minutes and focus myopically on epidemic control.

First, one has to realize that we have several goals. With medical countermeasures, that is to treat or prevent disease. And we have made great strides in both arenas, having moved forward both with the smallpox vaccine and anthrax vaccine; we hope to have a new recombinant anthrax vaccine available within about a year. We have moved forward very aggressively in insuring that we have the right vaccines for the right threat agents.

As important as medical countermeasures is the whole issue of exposure control following a bioterrorist event. Exposure control basically focuses on either isolation or quarantine. Representative Shays talked about the patchwork of laws and rules that are available and the fact that the federal government really has very limited authority in the area of quarantine. I will also be the first to tell you that I am not convinced that quarantine will work. Historically, if you look at outbreaks of smallpox, and in talking with people, quarantine has not always been shown to be an effective way of dealing with contagious agents. The ultimate issue is, how do you arrest the transmission of disease? Our goal in doing this is to reduce to less than one the average number of persons to which a patient transmits disease. One of the things that we found with SARS is the fact that if you isolate those that are sick and voluntarily quarantine those that are exposed, you can control disease. In the event that you do have countermeasures like a vaccine for smallpox, you aggressively use your countermeasures in conjunction with those measures that help reduce transmission. Let me just list a couple of examples: short-term home voluntary care curfews, restrictions on group events, cancellation of public events, scaling back or closing mass transit, closing public places, and selective restriction of travel. All of these help reduce contact, help reduce person-to-person spread and that, in combination with either preventative or treatment strategies, will help reduce the spread of disease. Not all strategies need to be employed in every type of an outbreak. It depends on the nature of the threat agent or the agent itself, whether or not it is contagious and how infective it is. The goal is to try to be as aggressive as possible in getting your countermeasures out.

Representative Shays mentioned the stockpile. One of the things that we have done in the last two years is to significantly increase the stockpile of antibiotics in this country. We now have them for pretty much all of the select agents with the exception of smallpox, and we do have a vaccine for that. We are working on an antitoxin, including a transgenic antitoxin for botulinum. Recently, NIH announced that they have made some significant breakthroughs on vaccine for Ebola. We have seen a lot happen. I think as we look at this, probably the greatest challenge that we have in the near term is surge capacity. My greatest concern at this point is that our healthcare system was brought to its knees during an outbreak of flu, as we saw in 1999 in New York City. I received calls asking for ventilators, and that is a really small flu outbreak. Were we to have an outbreak of anthrax or an incident involving anthrax, somebody using botulinum in milk, 48 percent of people that get botulinum require ventilatory support, in children it goes up to about 83 percent. The average length of time on a ventilator is about six weeks. It would bring the healthcare system in this country to its knees.

We have to look at surge capacity. We have to get creative with surge capacity. It is one of my top priorities, the secretary's top priority. We are looking at how to

rapidly deal and mobilize the healthcare system because we can do all the vaccination we want. We can give out all the antibiotics we want. But if 10,000 or 20,000 or 100,000 people show up at hospitals in multiple cities, the healthcare system is not flexible enough at this point in time to manage it. So we have some significant challenges in dealing with this. While I think we have to address quarantine, we have to address isolation, we really have to focus on surge capacity. It is a significant challenge and it is one that near-term we have to resolve. So, with that in mind, I will stop and let you take over. Thank you.

LYNN DAVIS: It is a pleasure to be here to share with you our research report that focused on individuals, how you and I as individuals would prepare for terrorist attacks involving chemical, radiological, nuclear, and biological weapons. (The report is entitled *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks* and is available on the Web at http://www.rand.org/publications/MR/MR1731.)

What I would like to do is share with you just briefly the approach that we developed and then some of the strategy that emerged from that approach. Our approach began by defining terrorist attack scenarios. That is the events themselves where we would find ourselves with needs as individuals. So we looked at the attacks, what kinds of needs would arise to us as individuals for our personal safety and for our personal health, for our survival? And then we turned and tried to define responses, steps, and actions that you and I would take in order to meet those needs in response to those effects. We evaluated those responses and then came together in a strategy that you and I would adopt as individuals. It is displayed here in a reference card that is part of the full analysis that begins with all the scenarios and takes you through how it is we came to our recommendations. What we discovered by adopting this approach is that in most cases you and I will find ourselves in situations in which we will have to act very quickly and without guidance from others, from officials or emergency responders. We will need to take these steps so quickly that we will need to have thought about them and understood them in advance.

The second thing we discovered by starting with the attack scenarios themselves is that it is very important to think about these responses in terms of each of the four types of attacks. That is, your responses need to be tailored to these situations. Finally, we discovered that there are some steps, response actions that you and I can take, that will be effective, even in the most catastrophic of these types of attacks. We can demonstrate that they can be effective because we can take you back to the effects in the attacks and show you how the responses meet our needs. So that is our approach and using that approach we came to a strategy of response actions and then preparatory steps in order to facilitate those response actions.

So let me then return to our panel's topic and just illustrate what we discovered in terms of sheltering and evacuation, in particular. One of the very important points that comes out of our work is that it is not possible just to think of sheltering as a generic concept or precept, or evacuation as a generic concept or precept, but it needs to be thought of in terms of the situations that you are going

to find yourself in if any of these attacks were to occur. So if there is a chemical attack and it is outdoors, the very most important step that you can take to find clean air, which will be your goal, is to move from outside to inside a building. Or, if you are inside a building, stay inside a building. If there is a radiological attack and an explosion is outside, and you are outside, then it is very important to take shelter, again, inside the nearest building that is not damaged. Sheltering, going inside in those two types of attacks, is the best way to protect yourself. Just being inside in a radiological attack helps prevent inhalation of dust that could be radiological. But in a chemical attack it would still be useful to do a couple more things, that is to shut off the airflows, move upstairs, and potentially use your duct tape and plastic sheeting to seal your room. Most of the protection you need comes from simply being inside, but it is important to understand that that is when sheltering is important. The type of shelter that you want to find depends on the type of attack.

Turning to an indoors chemical or radiological attack, you have got to think about where you are in relation to that. If you are inside a building subject to a chemical attack, and you need clean air, then the best step is to open the window and get the air. Now, unfortunately, many of us do not sit in buildings with windows that open. So, in those situations, we are going to say that it is very important to get outside the building, to evacuate the building. There are dangers in moving through a building that has been exposed to chemical agents, but it is better still to get outside and get that clean air where you will be safe than to try to stay inside or shelter. If you see the rhythm of what I am trying to explain, it starts with the situation. In the case of our strategy, what we have done is begin with the situation you would find yourselves in, what your goal should be, and then the specific steps tailored to whether you are inside or outside.

We did this as well for a nuclear attack and for biological attacks, and I can go back to those if we have some time, and they are outlined in our strategy. Let me just say a couple of things about biological attacks because they are really very different in lots of ways. Most importantly, they are different because in most cases you and I as individuals will not identify those attacks ourselves. That is, someone else will tell us that there has been such an attack, probably days after the attack, when symptoms start to show. So, at that time, individuals will learn about such an attack, but also officials will be there to describe what to do, what the character of the medical treatment should be and what you should expect if you have been exposed, what are the plans for responding to this, and what you should do. We include this in our recommended strategy because it is important for individuals to understand in advance what to expect in those circumstances, what they are likely to hear in terms of guidance, what they are likely to be asked to do to think about it in advance. For each of these types of attacks and for the responses that we described, we then go on to focus on the few things that one might do in advance to facilitate them. So we have a short list of things that you might do, preparatory steps, in advance. Most of these focus on thinking about and understanding the situations and the steps that we recommend, and only a few important things that we put in your emergency kit.

So that is how we have come to these recommended response and preparatory steps. We see these as another step as we all think together about how to prepare individuals. We see this as building on the work that is already under way in the Department of Homeland Security, in terms of getting people focused on preparedness and the importance of preparedness. But we have taken it an additional step by using attack scenarios to develop an approach for individuals.

So, in conclusion, by going through this approach, we can say to you that the steps that we recommend in this individual preparedness strategy are ones that can be effective in terms of saving lives, even in the most catastrophic situations. This can help reinforce the sense of confidence and planning that people can have. Second, and this is an important thing to remember, we are not saying in any way that these types of attacks are likely. We are making no judgments about the probability of any of these events actually happening. These are simply steps, prudent steps, that you and I can take as individuals to prepare like we prepare for other things and that would actually make a difference. Thank you.

JASON SAPSIN: I am very grateful to have the opportunity to be here with you on behalf of the Center for Law and the Public's Health. When Amanda first invited us to come along, she asked us to focus specifically on what we termed, some of you may feel euphemistically, personal protective measures, in other quarters these are known sometimes as "quarantine or isolation" and in still others as "the totalitarian oppressions of overreaching bureaucrats and public officials." The bottom line is that in terms of what Mr. Hauer has just shared, none of us at the Center for Law and the Public's Health think that the question of which regulation or which statute we have on the books in a particular jurisdiction is more important than the question of whether we actually have sufficient personnel and facilities in the country to provide the appropriate medical care. That is a theme that runs throughout all of this and that is particularly important in the context of quarantine because if the decision were to be made to quarantine a population, that population or segment thereof has to be taken care of, and that means having a place where they can be asked to go for appropriate medical treatment. Or, if it is an in-home quarantine, as we saw used in SARS internationally, it means having people who are able to go and visit the homes and the apartments of those who are at home to provide them with necessary items. All of this requires a well-established, well-funded, and well-trained infrastructure.

So the issues here are obviously complex. I am going to try to limit my discussion to just a few things, cover with you where we started on public health law for emergencies in 2001, briefly talk about where we are now in terms of the law and public health emergencies across the country, and then touch on some of the issues. The center where I work, the Center for Law and the Public's Health, was established in 2000, funded in part by CDC and in part by the Sloan Foundation. In late 2001, surveying the public health law landscape, we observed three things. The first was that we saw across the country no emergency public health law per se. The second was that of the many different disease control approaches across the states (control of infectious disease except in certain circumstances is primarily a state responsibility), frequently these approaches were

disease-specific within the states. The third point was that, and this is really related to the other two, there tended to be a reliance on older laws and older ways of doing things, older procedures that were hard both for the public to access and to understand, and in many cases were difficult for public health practitioners themselves to understand. So the question that you may ask yourself, and it is a question that I was asked by the state epidemiologist in Kansas two weeks ago, is: why does this matter? The argument for why it matters is that if you believe that public health or public response will be enhanced if people feel a sense of clarity or certainty over what the law is and enjoy a sense of security that the state will provide for them in the event that they have to be quarantined or isolated, and if you believe that those things are also important to the response of public health officials themselves, then it matters very much where the law is, that people know how to find it and that it is clear and accessible.

So, in 2001 we started working on a project called the Model Act, which is, in some ways, better characterized as a checklist, in an effort to move us toward greater clarity and certainty over public health law and logistics for public health emergencies. With respect to the particular issue of quarantine, we struggled to find the right balance of sufficient public health power while protecting the rights of individuals, which is in many people's view, the central dilemma of public health law: balancing the rights of the individual versus the needs of society. We are not sure that we got that balance right, but we tried. There are other approaches, ours is not the only approach. But what we did do was make sure that what was in the act was orderly and it was transparent, that you could go to one place if you were in a jurisdiction that adopted this kind of provision and you could see what the law was and you knew what the options were. The other thing that we did, and this gets back to the point about infrastructure, is we had a section of the act devoted to planning, which recognized the logistical difficulties inherent in trying to control mass outbreaks. It required planning in the states for things like gaining access to facilities, supplies, making sure that the judiciary could still function, vaccination plans and policies. Today, a couple of years later, the legislation has sparked the introduction of legislative initiatives in about 43 states, the District of Columbia, and even the Northern Marianas Islands. Thirty-two states and the District of Columbia have done something as a result of those initiatives. Now what they have done becomes much more difficult to track and I am not sure any one person can tell you exactly what each state has done. There are pockets of that kind of information around.

Which gets us to the point of where we are today, which is maybe of most interest, and that is, in some respects, there is a very similar degree of variability between states now at the end of 2003 that there was at the end of 2001. The difference is that much of the legislation has at least been looked at again by public health officials and by legislators and other policymakers and, in some cases, it is clearer and people know where to find the law related to control of infectious disease and emergency conditions. That was not the case necessarily in 2001. If we look at specific issues like quarantine, we see 21 of the 32 states and the District of Columbia that did something with their law, and that is about as specific as I can get without taking up too much of your time. Twenty-one dealt with things like

isolation and quarantine, 18 of the 21 dealt with due process requirements specifically for isolation and quarantine.

So the issue that we are facing, unfortunately, is still this patchwork. We are still convinced at the Center for Law and the Public's Health of the need for robust, modern, and balanced regimes for quarantine and isolation. Our point has been historically—if two years is "history"—that this is a weapon in the public health arsenal that is frequently employed. And if it is employed, it has to be bounded by controls within a structure that is transparent and accessible. It is not clear that this has been accomplished across the country yet, and it is critically important because of, for example, the fact that CDC's role is primarily supportive in the case of outbreak control. SARS, for example, taught us internationally three important things. One is that societies will resort to traditional disease control mechanisms in the face of diseases that are new, that are dangerous, that are of sufficient magnitude and severity that present some unknowns, some challenges. They do it with varying degrees of success. We know that populations tend to cooperate, we have seen it, but we also know that there have been notable exceptions to that, and that in the case of exceptions, public health systems struggle to respond. A case of noncompliance, or several cases of noncompliance, with public health recommendations at the right time and under the right circumstances can put many other people at risk. And, finally, the third thing that we learned from SARS, and one of the things that helps us see where personal control measures were most effective, is the question of how societies pay attention to the financial and material needs of the people who are asked to restrict their activities.

Now, in public health, they teach us to always be careful about the "*n* of one." The "*n* of one" is the infamous anecdotal experience. It is a set of observations that is really too small to allow one to draw any statistically significant conclusions, but sometimes even worse, reasonable conclusions. I am going to take that risk, to dare the "n of one" with you today and hope that you will give me a little bit of license to do so. One of the things that states talk about now is the lack of adequate access to legal advice. Going back to the theme that public health practice and public health disease control is still in many respects a local and a state effort, and primarily a local effort. One of the most frequent complaints is that they do not know the law and they do not have any way of accessing it. This is a problem with respect to the public because the public needs to have certainty and reassurance that what is being done is happening in a fair way by people who are following the requirements of the law.

The other thing that I sometimes hear from state and local people, and it goes back to this question of infrastructure and planning, is that there is a degree of uncertainty with respect to federal and state plans at the county level and how they work, what their role is. It is particularly important when a discussion comes to things like infrastructure and material support in public health because the people in the county health departments know, based on their existing budgets, that things are pretty tightly stretched as it is. They do not have the people who might be needed to mount a new surveillance program, as was the case for SARS, which is something that they are called upon to do. It goes back to this question of surge

capacity. The good news is that, although the federal government is freeing up millions of dollars, we still have to be vigilant because local officials continue to express concern about where the money is going. Is it going into training programs that they have difficulty accessing? Training programs that are going to go away as opposed to fixed assets that they can use in the event of an emergency? How the money helps them on a daily basis, and what will happen if the flow of federal funding dries up are fundamental questions at the local level.

The American Public and Terrorism

JOHN HAMRE: First, thank you all for coming today to talk about the homeland security from a citizen's perspective. Boy, am I glad to have this conference because I am now entering my seventh day of no electricity in Bethesda. I was in Baghdad for five days and we had more electricity in Baghdad than in Bethesda.

This is a very important opportunity, however, to talk with everyone and we are exceptionally fortunate to be able to have this conference. First of all, let me just thank Amanda Dory for having the energy and the imagination to put this together. Amanda is on a work-release program from the Defense Department and pretty soon we are going to have to let Amanda go back, but she has been great. A special thanks to the Alfred P. Sloan Foundation and to the National Association of Chain Drug Stores for helping us with this. You know, as a poor little think tank, we cannot do this stuff on our own and we desperately need good friends and partners. Thank you, we are really grateful for it.

And, of course, we have been really very fortunate to have so many notable leaders in the area of homeland security here, and I am, of course, very grateful to shortly be able to introduce Governor Gilmore. But we also have Representative Turner, Representative Harman, and this afternoon Jerry Hauer will be with us, and others. So, it is really great. And as I look out through the room, I have been fortunate enough to have a chance to have worked with probably half of the folks here in recent years on homeland security. I am just so pleased that we can do that together. It really is essential.

One of the things that I know we have realized is how fragile American consensus is for its views about government when you are in the middle of a crisis. It really tends to be the overarching challenge. We think that homeland security is really about the mechanics of response, but it is really about the credibility of government. How well have you thought about the problems? How forthright are you about dealing with them when you confront them? How open are you in interacting and understanding where citizens are and what their needs and concerns are? And, by and large, this is a real tough problem for the federal government to deal with. Somebody once described Washington as ten square miles surrounded by reality. And there is really a lot to that. We have become our own bubble. We are a very self-absorbed community. We are obsessed by our own internal dynamic. We tend, when it comes to the rest of the country, to have kind of that old motto, "Why, because I am the mom, that is why." You usually do it my way because I am the federal government.

On a couple of occasions I have had the opportunity to work with Governor Gilmore, and on one of the most recent ones we had him participate with us on a couple of our war games when we were trying to create a simulated National Security Council meeting with a crisis. The first one was Dark Winter, which was the one about a smallpox attack. The second was Silent Vector, and it was where we were looking at the prospect of a highly credible, but inherently unknown tactical threat. At that time, Governor Gilmore played the role of our Homeland Security secretary.

Most recently, we did Bold Sentinel, which was about a North Korea crisis. In each of these three I can remember being caught up in the middle of this simulated National Security Council meeting crisis and having sat through a couple of dozen of those for real when I was in government. These were, by far, the best meetings I have ever attended, the simulated ones. I remember having an observation to my mind, at the time, and I looked around the room, especially on the Dark Winter exercise, and I thought to myself, of all these people that are sitting at the National Security Council table, the only ones that I trust are the politicians. Now that is not the public sentiment in America. But the only ones I really trusted with my life in those meetings were the politicians, people that had been elected to public office. Everybody else that was sitting at the table was there talking about their bureaucracy or their agency or their expertise or their constituents. They always approached every problem with the perspective of that constituent element. But the only people who were sitting at that table thinking about the whole, what will the American people expect? What do I have to do? What are the constraints, the true constraints? If this really is a test about the viability of democracy, what do I have to do to get it right? Frankly, the only people in these exercises who I really felt had that grounded right were the politicians. So, let me just say, thank God we have got politicians. That is not said very much in this country. We are very lucky that we have people who are willing to do that. That is not the only reason we asked Governor Gilmore to come today. He has been tempered in the business of having to get elected and stay elected. You all do not appreciate how important that is. We tend to take it for granted how important this is. To be a credible witness and representative of the structure of life that we take for granted in a time of crisis is incredibly important.

Governor Gilmore, of course, as you all know, was also the chairman of the now-famous Gilmore Commission and looked at all of the issues of homeland security before September 11, anticipating maybe not the precise details of September 11, but the context and the consequences of catastrophic terrorism. We are lucky to hear from him now, especially about this subject, which is: let us look at this problem from the perspective of citizens, not from the bureaucracies, not from, does my office look out over the mall or does it look out over Sixteenth Street or how many assistant secretaries do I have working for me or which part of the regions are organized under my jurisdiction, but how do my mom and dad understand what we are trying to do to protect them?

That is where we are now. That is what this conference is for. Governor, we need to stop hearing me and we got to start hearing you. Thank you very much for coming. We are looking forward to what you have to tell us.

JAMES S. GILMORE III: John, thank you very much. I appreciate the invitation to be here with this distinguished assemblage today to talk about homeland security and where we have been and where we are going. I did do a couple of the exercises with CSIS. In one, I played the governor of Virginia and in another I played the secretary of Homeland Security. I much preferred governor of Virginia, and actually since Governor Ridge has always called himself governor, he probably does too, but that is another story. John has always expressed that same appreciation for politicians and the conclusion was always that John Hamre had a moral problem of some kind that had to be dealt with.

Let us talk a little bit about this. When I was invited to come today and be your luncheon speaker I went on and looked at the agenda here at CSIS for this event. I must say, this is very impressive, the fact that you are able to deal with these essential questions through specific seminars through the balance of the day raises sort of a challenge of the lunch speaker because what I am going to do is discuss the whole big picture and give you some history and background on that. And then we will do some Q&A here after a while and talk about some of this. But this will give me a chance to go over many of the topics you are going to be talking about in detail with the distinguished people who have come in.

Presently I am, obviously, no longer governor of Virginia. In Virginia you get one term and that is it, unless you decide to come back at a later time. I never knew at the end of the term whether to laugh or cry, and I think I did both, but it does give me the opportunity at this point to do some things in business. So I am practicing law at Kelley, Drye & Warren over here in Washington and we are building a homeland security sort of a trade group that can come together in private businesses and address some of these homeland security issues as a group. We are calling it U.S.A. Secure. I am working with some corporate boards and one or two of the think tanks here in Washington, as well. I am staying quite busy. But one thing that has been a consistent part of my life now for just about five years has been my position as the chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities Involving Weapons of Terrorism and Weapons of Mass Destruction. Now you cannot even make an acronym out of that. So nobody in Washington ever remembers it because you cannot make an acronym out of it, but that is what it is. This was actually formed back at the end of 1998. As you probably recall where you were in 1998, there was not a lot of discussion about terrorism during that period of time, or homeland security. Just not a lot of talk about it. But there was a sense of unease in Congress about it. So Curt Weldon asked that a commission be formed to address this question: If we had a major attack in the United States, would we really be prepared to address it at that time? So at the beginning of 1999, I was having a seminar in Williamsburg, together with the governor of North Carolina, on terrorism issues. Dick Clark was, at that time, on the National Security Council for President Clinton, and people from the DOD came down and they basically surprised me a little bit and said this thing was getting ready to be formed, and asked if I, as governor of Virginia, would be prepared to chair it? They wanted somebody from the states to chair it. So I agreed to do it.

Now this commission is not what you would typically see in Washington, D.C. This commission is a commission made up of police, fire, rescue, emergency services, healthcare, and epidemiologists. It does have some retired general officers that are on this commission, and some intelligence people have been on this commission. It is a very distinguished alumni group. Jim Clapper, who now runs the National Geospatial-Intelligence Agency, was on the commission as vice chairman for all the years before he went to that branch. Rich Fairbank has served on it. He is now in the White House dealing with the issues of homeland security. A guy by the name of Paul Bremer served on the commission for four years and resigned from the commission to go to Iraq. We had another fellow by the name of Ray Downy. He was one of the top people in the New York City fire department and was killed at the World Trade Center while he was trying to get people out. So we have had a very distinguished group of alumni and current people who are on there.

The commission has stuck together very well. There has been great longevity and consistency. The way I have tried to run this commission is to treat no member any more importantly than any other. So, as a result, everybody on the commission has had complete latitude to get in their two cents a lot. There has been enormous debate. So let me give you some feel for it.

The first year, in 1999, we were to report every December 15 and present the final report, then go out of business. By the way, this was a three-year commission, 1999, 2000, and 2001. The RAND organization staffs us and we said, "Well, what are we going to do? How are we going to approach this?" The first year we decided that we needed a threat assessment. Nobody was talking about this. We asked "What is the reality here? What is the real danger?

So the first year we did a threat assessment. In the conclusion of the first year, when we reported on December 15 of the year 1999, we basically asked what is the real danger here of a true weapon of mass destruction being used in the homeland? And that is nuclear, biological, chemical, radiological. We did a complete study on it. At the end of the day, we concluded that the chance of a major weapon of mass destruction being used in this country was not probable. But, frankly, some of the staff really urged the commission to write it off 100 percent and move on to other topics. The commission refused to do that. The reason was that we were so concerned about the potential consequences of a weapon of mass destruction that no matter how unlikely it was, we thought we had to continue to address it for the balance of the next two years. But, on the other hand, we also addressed the issue of whether or not there was likely to be an attack in the United States, in the homeland here, with a conventional attack, a bomb, the hijacking of a plane, hijacking of a train—a conventional type of attack.

The conclusion we reached in our first report was that that was highly probable inside the homeland of the United States. Then we basically raised the topic. We said we had better get a national strategy to deal with this because this is probably going to happen immediately so we better get on this. In the next year we probably did some of our best policy work and we reported in December of the year 2000. At that point, we basically said, look, a year has gone by, there is still no national strategy, we better get one, and here is what we probably need to do. We

need to have an office, probably in the White House, that would be in a position to look at this holistically, to make a national strategy and then to force, using the power of the presidency and budget authority, all the rest of the government to fit into that national strategy. And that would be what we thought was the best managerial approach to the situation.

We urged that our strategy not be a federal strategy, but be a national strategy. It would have to be federal, state, and local. Now, this is not understandable in Washington, D.C. They cannot get this, and it is very hard even today. But there is still, today, a lot of discussion about federal, state, and local authorities. It is reality. It is the right thing to do. It was very jarring, though, when we came out and said you have got to, that the federal strategy is not going to work, and that is still true today. We also discussed the fact that the intelligence community was not able to communicate between different organizations—CIA, FBI, NSA, and all the rest of those organizations just simply could not communicate with each other about homeland security problems. We also pointed out that there was absolutely no ability to communicate between federal, state, and local people on intelligence and law enforcement types of issues. Culturally, it was just unthinkable and today remains very nearly unthinkable to be in a position to pass that information up and down the line.

So we pointed out these issues and then we went into the third report, the third and final year, 2001. That year we said, "Okay, we are going to go out of business now by trying to fill out some of the detail of what we think is important for the national strategy within the parameters we discussed." We basically focused our attention on healthcare issues, how to utilize the state and local responders in an attack situation, how to work with them and what their role was, which was absolutely critical and central. And so is the issue of border control and how you get the borders under control so that we would not have this constant danger here in the homeland.

We devoted a lot of attention to the use of the military in the homeland. The sense of the commission was that this was a highly dangerous situation, that to utilize the U.S. military in the homeland would be a violation of *posse comitatus*, although there are legal exceptions, particularly in the case of the use of weapons of mass destruction. But to utilize as a first responder the military for the homeland was highly dangerous to the democracy. And then, finally, we discussed the issue of cyber terrorism. We finished this report and decided we would go out of business early. We would impress the Congress, save them a month or something like that. So we sent this thing off to the printer in the first week of September and got ready to have a big announcement in November when it came back and we had had a chance to review it one last time from the printer.

And then, of course, the attack occurred on September 11, 2001. I was actually still the governor of Virginia at that time. We were one of the two states directly attacked at that time: New York and Virginia. New York obviously, Virginia perhaps less obviously, but the Pentagon is in Virginia. The responders, from Arlington, Alexandria, Fairfax County, Montgomery County, and later on, local responders from all across the country, came in to deal with this issue at the Pentagon. I was in my dressing room when I saw the attack occur at the World

Trade Center. I watched the plane go in, just as I am sure all of you did, and then got my tie on and got across the street after doing all the appropriate notifications and just in time to arrive when Virginia was struck at the Pentagon and we had to deal with that.

Well, the Congress, at that point, decided to extend the commission. So the commission was extended two additional years, last year and this current year. In the fourth report that we issued December 15 of this past year, we focused much of our attention on the issues of intelligence, fusion of intelligence interaction, and how we conducted antiterrorism here in the United States. We recommended that there be a fusion center of intelligence so that all the organizations could co-locate in one place to collect the dots and get the information together and try to break through the cultural barrier that we identified in the second year of our report in 2000. The president adopted a similar concept in his state of the union address shortly thereafter and that has become the TTIC, which all of you are familiar with. What is it? Terrorist Threat Integration Center. So that became the TTIC organization that exists today. That was a fairly consensus position on the commission. It was kind of a no-brainer. The controversy in the commission in the fourth year was this raging debate that went on between two different factions within the commission on the issue of how you conduct counterterrorism operations inside the United States. There was one faction led by me that believed that the FBI was the correct organization and we should build upon their current capabilities and force them to do the job correctly. That was my position. The second faction was led by Jerry Bremer, his position was that it was impossible, the FBI would not be capable of ever doing this, and that it should be removed from them forthwith and put into the hands of a new organization based upon the British MI5 model. And that was the real issue that came out of that fourth report. If you want to read all this, it is on the RAND Web page, www.rand.org. When the web page comes up, put Gilmore Commission in and this stuff comes up. You will find the recommendation of the commission and the MI5 concept.

Now, this year's report that we are getting ready to do will be out this coming December 15 and then we are out of business. By statute, we are obligated to meet and report, and by statute we will go out of business on December 15 of this year, after five years of laborious work on this. If you look at the material, you will see almost everything about homeland security has been dealt with by this commission at one time or another and in detail. You will get a kick out of it if you are looking for some good light reading at bedtime.

In the fifth report that is coming up, we have asked ourselves this question, what contribution can we make at this point? The Department of Homeland Security has been established, it is up and running, there has been a wide discussion of this—we have discussed very little else in this country since the September 11 attacks. So, what can we do as we go out of the door? Our thinking at this point is that we want to try to address the big picture. We want to ask ourselves what is preparedness? Define what it is. Try to get some idea of what an appropriate strategy is. How do you make the decision about what it is you are trying to buy, what it is you are trying to do, what is the purpose of grants? How do you get this stuff into the hands of the states and locals appropriately within a

strategic framework that makes sense and then how do you get them trained and exercised?

I met with the local responders the other day in Seattle. They asked me to come and give a talk to them up there because of their frustration, and they asked me to keynote a little address for them in Seattle. I said, "Look, you are all saying that you are frustrated because you cannot get grants." I said, "Grants to do what? What are you trying to do?" Who cares what your local parochial desire is, whether you need gas masks or something like that. The issue is not that. The question is, grants to do what and to buy what? I told them that if you do not somehow fit what you want to do into a national strategy, then the reason for giving you money disappears. There is no reason to give you any money. So, there has got to be a strategic framework thought about and our commission hopefully will try to add some thinking into that as we go on.

There is another thought about this, which is, we are not going to ever be really secure and we should be cautious about trying to tell the American people we are going to be secure and constantly rolling towards that particular goal because it carries within it certain dangers. We have to decide how much security is appropriate, how much risk we are going to run, tell the American people and then move on, instead of this constant obsession that we have as a nation, which takes us away from a variety of other issues that have to be thought about as a nation. We have got to decide what we are doing, do it, and then tell the American people about it and move on to other things that we have to do as a country. Otherwise, the enemy is distracting us to the point where Lord knows where we are going to end up. And then that takes you to the second thought that we have as a commission for this fifth report, and that is the issue of the civil freedoms of the country. I am a conservative republican so I am not typically using the words civil liberties, but civil freedoms is the identical concept. And we are talking about this quite a bit because I believe, and I think the commission agrees that there is a consensus feeling about this, that this is an extremely dangerous time for the United States.

There are forces that preexisted in the society that have been unleashed by the enemy by their attack on September 11. What are those forces? Number one, this is the most managerial society in the history of the world. You are part of that class, all of you who are sitting in this room today, you are part of the managerial class of this country. We are a people that if we are told that we have a problem, we fix it. That is what we do. And Americans are very impatient people. If we are told we have got a problem, we start to manage through it and we fix it. And then there is a second problem. The second problem is that we are the most technological society in the history of the entire world. As we saw in the Iraqi war, you can win a war virtually on technology alone. And look at what we can do now inside the homeland that has never been able to be done before. We can take data and all of a sudden combine it together and create unified databases and now the government can know everything about everybody all the time. We are in real trouble because you cannot un-invent a lot of these things. You maybe have to pass laws to define it. We have the ability now to have cameras everywhere. Everywhere. In fact, the Washington, D.C. people are very proud about the fact

that they have got some war room where they have got big cameras and screens on the wall and they can watch any street that they choose to.

Let me ask you a question. If you walked across Washington, D.C., do you think you would behave differently if you knew you were being watched? I think you would. I would. You would behave differently. You would feel different. You would know you were being watched. When I was governor of Virginia, I vetoed the red light cameras at various intersections. The localities thought I was nuts because they said, "Governor, that is revenue, we can get that." I said no; young Virginians, with our background and history and tradition, should not have to grow up feeling watched on their own public streets. We should not do that as a matter of principle.

So these are very fundamental and troublesome issues that we have right now. The raging issue right now, is the issue called CAPS II. At our meeting in Sacramento last week, Admiral Loy was invited to come in and present to us, which he did by video, and I am a big fan of Jim Loy. He is an excellent man, but I do not have to agree with everything he says. One thing he said was they are going to put together this program where they will combine together all the databases and they are going to assign a color to everybody that wants to buy a plane ticket. Green, you get on the plane. A yellow, you get hauled off to the side and questioned closely. A red, you do not get on the plane. Have you ever tried to change one of your government records because there is an error in it? Have you ever tried to do that? What is going to happen when some poor guy just hits the profile and he has a red and for the rest of his life he is trying to figure out how to get off of red? If it is you, ladies and gentlemen, and I would say some percentage will be you, you are going to be pretty mad about it, and it is dangerous. There is a lot to talk about here in the civil freedoms area. Our commission certainly wants to address that issue. I am very optimistic about this country. I know what this country is like, just like you do. We are a country that has great strong values and a long tradition and a sense of individualism that exists uniquely in the world.

I was a soldier. I have lived in Europe. I have had a chance to do a lot of reading. I do not think people in the rest of the world look at things the way we do. We look at things better. We, as Americans, think a lot more about freedoms and liberties than anybody else does. Our traditions are not medieval. Our traditions come from the very beginning of prying the British Army off, and men and women who listened to people like Benjamin Franklin who said, at the very beginning of our republic, he who would trade freedom in return for security is entitled to neither freedom nor security. This is the American tradition, the same American tradition of people getting in covered wagons and going across the country whether it was dangerous or not. Think of those women that marched along beside those covered wagons, dragging children with them, because they were part of the American value. And that is what we are. I am very optimistic that when we come through this we will maintain the values that make us Americans. John, thank you for the chance to be here.

Conclusion

AMY SMITHSON: My assignment is to wrap up the day, but since I like putting together puzzles, I was pleased that Amanda Dory asked me to do this. First, I want to thank Amanda for getting everyone together to think about terrorism, preparedness, and response in the context of how those not in the homeland security "business" might contemplate these matters. What a valuable approach to take.

Representative Turner started the day by saying how critically important it was to get the definitions right. "What is the threat?" The response to that question will shape the war against terrorism. Arnaud de Borchgrave then issued the ominous warning that the real war on terrorism has years yet to unfold.

On the first panel, I was relieved to hear Phil Anderson explain that a great deal is actually known about these threats. We have over 20 years of data on Al Qaeda, and, I would add, also reams of data on other terrorist groups' behaviors, activities, and capabilities. Anyone who has worked with the RAND–St. Andrew's data or the Monterey database also knows this. I was intrigued to hear Jim MacGaffin encourage Americans not to get overwhelmed by this problem. That is one of the tendencies that we often succumb to when confronted with a really big problem. Do not get overwhelmed by it, he said, "step back." He asked everyone to look at and define the criticalities first, noting that this would help improve the production of intelligence "dots" and the connection of dots. Given what Bill Parrish described as the challenges of sifting through all these dots and pieces of data to determine credible threats, it would seem that Mr. MacGaffin's council to step back and also not to rush headlong into technical solutions should definitely be considered.

Representative Turner also highlighted Washington's obligation to be honest with the American public about the challenges that we are facing, a point that Governor Gilmore echoed. Tell the truth, he noted, that we are not ever really going to be secure. There will always be risks, and so a national strategy is needed. Governor Gilmore also issued a reminder that a national strategy does not equate to a federal strategy. A national strategy does not just involve the District of Columbia, this 10-square mile area outside of which one finds reality. A national strategy also involves states, locals, private entities and the public. Governor Gilmore urged policymakers to get on with finding that strategy so that the other problems that this country faces can be addressed.

Representative Harman jump-started the afternoon's discussion on security privacy and civil liberties with a reminder that the rights enshrined in the Constitution and the Bill of Rights are just as important today as they were when this country was founded. These rights cannot just be tossed overboard because

we are frightened. These rights cannot outweigh the nation's war on terrorism, but they do need to be considered as strategies are formed. She explained that civil liberties and security should not be thought of as being mutually exclusive, competing values. And, Representative Harman stated that policymakers have to think through what they are asking people to do as they create and implement new measures to try to secure this nation in the face of insidious threats. That is where Joe Onek picked up, with a warning about the need to deliberately evaluate how and why technologies are used, technologies like video cameras. To think that at one point it is possible that everywhere I go I am going to be watched makes me shudder. So I agree that protections against abuse of civil liberties need to be incorporated into technologies, policies, and procedures. Ms. O'Connor Kelly is attempting to do this by imbedding civil liberties into the culture and functions of the Department of Homeland Security, into its people, its procedures, its policies, and technologies. I certainly wish her success. And, finally on that panel, Stewart Baker asked that the government's response to terrorism not be driven by a fear of scandal or the need of government officials to keep their jobs. He asked that the private sector's response not be driven by concerns about losing money or of being sued. If those are indeed the driving factors in our response, then we are going about this in the wrong way.

Now, when it comes to communications, I hope that Dr. Lanard's canons of risk communications are heeded. If not, future crises will be a lot tougher. I would also like to second Jim Pebley's suggestion to hold a national communications drill. Policymakers need to find out if the American public can be reached effectively in times of crises. A drill would also serve the purpose of getting everyone to think about just how prepared they are, or are not. Such thoughts should not just cross people's minds when a hurricane cuts off the electricity or some other disaster comes along.

I would like to continue for a few minutes with the guidance of a familiar refrain and to issue a few challenges. The familiar refrain is that knowledge is a powerful tool, and the challenges involve education. Clearly, we have some educating to do. Two educational challenges involve the public, and one involves those inside the Beltway who design, appropriate, and implement domestic preparedness programs. Following the fall of 2001 and the avalanche of media coverage about terrorism that ensued, it is not surprising that many, if not most Americans have yet to put the threat of terrorism in proper perspective. In fact, this past spring, polls revealed that what Americans feared the most was Osama bin Laden and chemical and biological terrorism. If panic is to be kept to a minimum in the aftermath of a genuine terrorist event, which would certainly help first responders to do their jobs, then Washington needs to do a better job of communicating, which has been one of this conference's main topics. Somehow the phrase "low probability, high-risk event" just is not getting the message across.

Here I would like to echo some of David Heyman's approaches to suggest that perhaps the best way to begin communicating better is to place the risk of terrorism in the context of individual risk that Americans could encounter on a daily basis as we go about our activities. How are Americans most likely to be injured or killed? Certainly not by a terrorist attack. Out of the 275 million or so

Americans, some 5,800 of us are likely to die this year just as pedestrians. Over 700,000 U.S. citizens will succumb to heart disease, another 67,000 to influenza and pneumonia. In 2003, 50 Americans will be killed by lightning, another 5 by fireworks. More than 1,600 of us will become homicide statistics, and another 340 will meet their maker in their bathtub, by drowning.

I do not envy Ms. Scolinos's job of communicating with the American public during a disaster, and she has got to get a head start on it beforehand. The first part of that is to begin putting this threat into perspective. As she said, this begins long before disaster strikes, partly by explaining personal risks and by helping citizens understand what they can do to protect themselves. At the risk of treading on turf covered by Dr. Davis, far too many Americans went out and purchased gas masks in the fall of 2001, masks that do not have canisters that fit them and probably have not been taken out of the box since. As the last panel said, many things can be done to save lives when calamity strikes, and therein is another educational task. Relatively simple, inexpensive things can be taught to people so that they know how to take themselves out of harm's way and to increase their chances of surviving a disaster.

Regarding the likelihood of being in the wrong place at the wrong time if there is a chemical incident, if someone is in an area where sarin or an industrial chemical has been released, it is not just that they need to get out of the immediate area. They can also increase their chances of surviving by shedding their modesty and their clothes. Removing one's outer clothing takes away roughly 85 percent of the contamination hazard. The next thing that should be done to wash hands, head, feet, and any skin that might have been exposed to the toxic substance. Water alone is an effective decontaminant. These simple steps can really increase the chances that people can save themselves, and it should also make everyone take seriously their mother's admonition always to wear clean underwear.

Ed Staffa, who gave everyone a reminder that pharmacists are perhaps an underutilized educational and communications resource before and during disasters, also said that we need to be sure that the public knows what, for example, potassium iodide pills can and cannot do if there is a radiological or nuclear event. The strategies that the last panel raised, such as sheltering-in-place and voluntarily restricting movement in the event of an infectious disease outbreak, need to be as well-known and understood by the American public as buckling a car seatbelt before driving. These types of risk-reducing steps need to be incorporated in the mindsets of Americans. So, Washington needs to do a much better job of empowering Americans with practical, lifesaving information.

My third and last educational challenge is aimed inside the Beltway. If Americans cannot save themselves during a disaster, then front-line responders will come to their rescue. Over the last few years, a disturbingly small percentage of the federal dollars being spent on terrorism preparedness have made it into the hands of frontline personnel. Yes, that is unfortunately still the case. This point can be illustrated with a visit to the front lines of response, courtesy of Paul Maniscalco, who is a paramedic, a member of the Gilmore Commission, and the government affairs director of the National Association of Emergency Medical Technicians. He was kind enough to share with me an advance copy of the data

that he is releasing at the association's annual conference in Las Vegas this week. Paul conducted an electronic survey of paramedics and EMTs from the middle of June to August of this year. The geographic distribution of the 13,203 respondents was quite even across the country. Of those responding, 24 percent were in career service, 23 percent were volunteers, and 53 percent were both volunteer and career. Forty-two percent of the survey respondents were working in urban areas, 41 percent in the suburbs, and the remaining 15 percent were serving rural communities.

Their survey responses provide a really quick reality check as to whether federal terrorism preparedness dollars are hitting the mark. Remember, these are the people that are going to save your tail if disaster strikes. When asked if they believed themselves to be prepared to respond safely and effectively to a terrorist attack, 12,096 of the more than 13,200 respondents said "no." Asked to grade their preparedness from A to F, F being the worst grade, 48 percent gave their EMS system a D, another 43 percent gave their EMS system a grade of F. Only 18 A's were handed out. Asked whether their EMS system had received any federal funding specific to terrorism preparedness, 98 percent reported receiving zero federal dollars for planning, training, and equipment. A whopping 89 percent of the respondents said their EMS system had not been issued any personal protective gear. Translation, in a chemical attack, 12,582 of these EMS paramedics would go to the scene in their regular work clothes. Only 941 of the respondents reported having any cyanide kits, Mark One kits, antibiotics, or full HAZMAT medical kits on their rigs. If these survey results are not a sobering reality check on how well current preparedness policies and programs are doing, I do not know what is.

Washington needs to do a radically better job of getting the money where the response is. Two speakers today, Representative Shays and Governor Gilmore, said that this cannot be just about spending. They observed that we are bouncing from threat to threat in the absence of a threat assessment, and we are still in need of that and a national strategy.

If U.S. policymakers do not first address such fundamentals, we may not ever get the healthcare surge capacities that Jerry Hauer just asked for and so rightly pointed out that we need, or the plans, capabilities, and resources necessary to implement a quarantine in a pandemic as our last speaker also rightly said were needed. The extent to which dollars get to the right places—to the frontline personnel—will make a lifesaving difference not only when terrorists strike again, but also in the everyday emergency situations that Americans are far more likely to confront.

With that, you have the pieces of the puzzle that I assembled from today's excellent talks. Thank you for your attention.

Conference Agenda

September 25, 2003

9:00–9:20	
Introduction:	*Dr. Kurt Campbell*, Senior Vice President and Director, International Security Program, CSIS
Opening Remarks:	*Rep. Jim Turner* (D-Texas), Ranking Member, House Select Committee on Homeland Security and Committee on Armed Services
9:20–10:30	ASSESSING RISK: THREATS, VULNERABILITIES, AND SETTING PRIORITIES
Moderator:	*Arnaud de Borchgrave*, Senior Adviser and Director, Transnational Threats Initiative, CSIS
Panelists:	*Hon. William Parrish*, Acting Assistant Secretary for Information Analysis *Dr. Philip Anderson*, Vice President for Government Strategies and Homeland Security, Lucent Technology *John MacGaffin*, President, MacGaffin and Associates *David Heyman*, Director, Homeland Security Program, CSIS
10:30–10:40	Break
10:40–11:50	BALANCING SECURITY, PRIVACY, AND CIVIL LIBERTIES
Moderator:	*Anne Witkowsky*, Senior Fellow, Technology and Public Policy Program, CSIS
Speaker:	*Rep. Jane Harman* (D-Calif.), Select Committee on Homeland Security, Subcommittee on Intelligence and Terrorism and Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security
Panelists:	*Nuala O'Connor Kelly*, Chief Privacy Officer, Department of Homeland Security *Joseph Onek*, Senior Counsel and Director, Liberty and Security Initiative, The Constitution Project, Georgetown University *Stewart Baker*, Partner, Steptoe and Johnson

11:50–12:00	Break
12:00–1:15	THE AMERICAN PUBLIC AND TERRORISM
Introduction:	*Dr. John Hamre*, President and CEO, CSIS
Keynote Speaker:	*Governor James S. Gilmore III*, Kelley, Drye & Warren; Chairman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction
1:15–2:25	COMMUNICATING WITH THE PUBLIC BEFORE AND THROUGHOUT A CRISIS
Moderator:	*Jay Farrar*, Vice President for External Affairs, CSIS
Panelists:	*Tasia Scolinos*, Deputy Assistant Secretary for Public Affairs, Department of Homeland Security *James Lee Witt*, President, James Lee Witt Associates *Ed Staffa*, Vice President, Pharmacy Practice and Communications, National Association of Chain Drug Stores *Jim Pebley*, Chair, Public Emergency Communications Task Group, Arlington Citizen Corps Council
2:25–2:35	Break
2:35–3:45	PROTECTIVE ACTION RESPONSES: SHELTER, EVACUATION, QUARANTINE, AND MEDICAL COUNTERMEASURES
Moderator:	*Amanda Dory*, International Affairs Fellow, CSIS
Speaker:	*Representative Christopher Shays* (R-Conn.), Select Committee on Homeland Security, Subcommittee on Emergency Preparedness and Response
Panelists:	*Jerry Hauer*, Assistant Secretary for Public Health Emergency Preparedness, Health and Human Services *Dr. Lynn Davis*, Senior Fellow, RAND *Jason Sapsin*, Center for Law and the Public's Health, Johns Hopkins School of Public Health
3:45–4:00	
Conclusion:	*Dr. Amy Smithson*, Senior Fellow, International Security Program, CSIS

About the Participants

Philip Anderson is vice president for government strategies and homeland security at Lucent Technology. Until mid-2003, he was a senior fellow in the CSIS International Security Program, specializing in homeland security issues. Previously, he was the director of defense and aerospace content for Intellibridge Corporation, a provider of customized, Internet-based intelligence and advisory solutions. Anderson served as a Marine Corps officer for 23 years, and his military experience includes leadership of operational organizations from platoon through battalion with deployments worldwide. Anderson served as principle operations adviser to the commander U.S. Marine Corps Forces, Atlantic, where he conducted research and on-site analyses resulting in an antiterrorism/force-protection plan for U.S. forces assigned to Haiti. He also conducted analyses and developed an operational scheme and cost estimates for potential maritime pre-positioned force and amphibious operations in Bosnia, and chaired a planning group conducting research with the Center for Naval Analysis for a revised predeployment training plan for operational naval forces. Anderson earned a bachelor's degree in sociology from Suffolk University, a master's degree and doctorate in education from George Mason University, and a master's in international relations from the Bundeswehr University.

Stewart A. Baker is a partner with Steptoe and Johnson. His practice includes issues relating to national security, computer security, electronic surveillance, privacy, encryption, digital commerce, and export controls. He has advised hardware and software companies on U.S. export controls and on foreign import controls on encryption. In October 2000, he was named to the Washington "Power 100" by *Regardie's* magazine for his work in this field. He also represents major telecommunications equipment manufacturers and carriers in connection with the Communications Assistance for Law Enforcement Act and law enforcement intercept requirements. In the area of authentication and digital signatures, his clients include major banks, mortgage companies, and credit card associations, as well as technology companies. Mr. Baker is the former general counsel of the National Security Agency (1992–1994) and author of the book, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce* (1998), as well as various other publications and articles on electronic commerce and international trade. Earlier in his career, Mr. Baker served as law clerk to John Paul Stevens, U.S. Supreme Court (1977–1978), Frank M. Coffin, U.S. Court of Appeals, First Circuit (1976–1977), and Shirley M. Hufstedler, U.S. Court of Appeals, Ninth Circuit (1975). Mr. Baker has been named to numerous bodies dealing with electronic commerce and related topics, including most recently:

President's Export Council Subcommittee on Export Administration (2003), Markle Foundation's Task Force on National Security in the Information Age (2002-present), and the Defense Science Board's Task Force on Information Warfare (1995–1996 and 1999–2001).

Kurt Campbell is senior vice president and director of the International Security Program at CSIS, where he also holds the Henry A. Kissinger Chair in National Security. In addition, he is the director of the Aspen Strategy Group and a contributing writer for the *New York Times.* Previously, Campbell served in several capacities in government, including as deputy assistant secretary of defense for Asia and the Pacific at the Pentagon, director on the National Security Council staff and deputy special counselor to the president for NAFTA in the White House, and as a White House fellow at the Department of the Treasury. Campbell was also associate professor of public policy and international relations at the John F. Kennedy School of Government at Harvard University and an officer in the U.S. Navy serving on the Joint Chiefs of Staff. He is the author or editor of several books and has contributed pieces to numerous journals, magazines, and newspapers. Campbell received his bachelor's degree from the University of California at San Diego, a certificate in music and politics from the University of Erevan in the Soviet Union, and a doctorate in international relations from Oxford University.

Lynn E. Davis is a senior political scientist at RAND. Her current research focuses on terrorism, citizen preparedness, and homeland security. From 1993 to 1997, Dr. Davis served as under secretary for arms control and international security affairs at the State Department. She was a member of the Secretary of State's Accountability Review Board in 1998 that investigated the embassy bombings in East Africa and the senior study group adviser for the recent Commission on National Security/Twenty-first Century. Prior to joining the State Department, Dr. Davis was vice president and director of the Arroyo Center at RAND. She has also served on the staffs of the secretary of defense, the National Security Council, and the Senate Select Committee on Intelligence. She has taught at Georgetown University in the National Security Studies Program, the National War College, and Columbia University. Her recent RAND publications include *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks,* with Tom LaTourrette et al. (2003), *The U.S. Army and the New National Security Strategy,* edited with Jeremy Shapiro (2003), and *Globalization's Security Implications* (2003). She has a doctorate in political science from Columbia University.

Arnaud de Borchgrave is senior adviser and director of the Transnational Threats Initiative at CSIS. While at CSIS, he has coauthored *Cyber Threats and Information Security: Meeting the Twenty-first Century Challenge* (2001), *Russian Organized Crime & Corruption: Putin's Challenge* (2000), *Cybercrime, Cyberterrorism, Cyberwarfare* (1998), *Russian Organized Cr*ime (1997), and *Global Organized Crime: The New Empire of Evil* (1994). Previously, during a 30-year career at

Newsweek magazine, he covered most of the world's major news events. At 21, he was appointed Brussels bureau chief of United Press International, and three years later he was *Newsweek*'s bureau chief in Paris. At 27, he became senior editor of the magazine, a position he held for 25 years. He was appointed editor in chief of the *Washington Times* and *Insight* magazine in 1985. He currently serves as editor at large at the *Washington Times*. He served as president and CEO of United Press International from 1999 to January 2001. He is currently serving as editor in chief at UPI. His awards include Best Magazine Reporting from Abroad and Best Magazine Interpretation of Foreign Affairs. In 1981, Mr. de Borchgrave received the World Business Council's Medal of Honor, and in 1985 he was awarded the George Washington Medal of Honor for Excellence in Published Works.

Amanda J. Dory is a Council on Foreign Relations 2002–2003 International Affairs Fellow associated with CSIS. At CSIS, she established the Civil Security Working Group with participation from federal, state, local, academic, Congressional, NGO, and private sector communities to explore issues relating to the role of the individual American in homeland security. A final report from the working group series entitled *Civil Security: Americans and the Challenge of Homeland Security* was published in September 2003. She has also participated in the CSIS "Beyond Goldwater-Nichols" project to study areas for future defense reform. Amanda's permanent affiliation is with the policy component of the Office of the Secretary of Defense where she has served for nine years as a career civil servant, first as a presidential management intern, and subsequently in the Strategy Office and the Office of African Affairs.

Jay Farrar is vice president for external relations at CSIS, where he is responsible for interactions with Congress, the executive branch, foreign embassies, and the media. Prior to joining CSIS, he served as deputy assistant secretary for legislative affairs at the Department of Defense, director of legislative affairs for the National Security Council, and legislative assistant to the chairman of the Joint Chiefs of Staff. Mr. Farrar served over 22 years in the U.S. Marine Corps, where he specialized in public affairs and political-military affairs. During his Marine Corps tenure he also taught military history, business management, and military-media relations at the University of California at Los Angeles. He is a member of the Council on Foreign Relations and a recipient of the Department of Defense Award for Exceptional Public Service. He is a graduate of Marquette University in Milwaukee, Wisconsin, and has a master's degree from Central Michigan University in Mt. Pleasant, Michigan.

James S. Gilmore III is a partner at the law firm of Kelley, Drye and Warren where he chairs the Homeland Security Practice Group, and president of USA Secure. He is the former governor of Virginia (1998–2002) and was in office when the Pentagon was attacked on September 11, 2001. Since 1999, former governor Gilmore has been chairman of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the "Gilmore Commission." The panel was established

by Congress to assess federal, state, and local governments' capability to respond to the consequences of a terrorist attack. The panel submitted its findings to the president and Congress each of the past four years and is extended until December 15, 2003. He holds a bachelor's degree in foreign affairs from the University of Virginia and graduated from the University of Virginia Law School in 1977. He was elected commonwealth's attorney in his home county of Henrico in 1987 and 1991 and Virginia attorney general in 1993.

John Hamre was elected CSIS president and CEO in January 2000. Before joining CSIS, he served as U.S. deputy secretary of defense (1997–1999) and under secretary of defense (comptroller) (1993–1997). As comptroller, Dr. Hamre was the principal assistant to the secretary of defense for the preparation, presentation, and execution of the defense budget and management improvement programs. Before serving in the Department of Defense, Dr. Hamre worked for 10 years as a professional staff member of the Senate Armed Services Committee. During that time he was primarily responsible for the oversight and evaluation of procurement, research, and development programs, defense budget issues, and relations with the Senate Appropriations Committee. From 1978 to 1984, Dr. Hamre served in the Congressional Budget Office, where he became its deputy assistant director for national security and international affairs. In that position, he oversaw analysis and other support for committees in both the House of Representatives and the Senate. Dr. Hamre received his doctorate in 1978 from the School of Advanced International Studies, Johns Hopkins University. He received a bachelor's from Augustana College in Sioux Falls, South Dakota, in 1972, emphasizing political science and economics. He also studied as a Rockefeller Fellow at the Harvard Divinity School.

Representative Jane Harman (D-Calif.) is a leading Congressional expert on terrorism and homeland security issues, a strong advocate of fiscal responsibility and of opportunity for working families, Representative Harman serves California's dynamic South Bay region. Elected to a fifth term in 2002, Harman was appointed by the House Democratic leadership to serve as ranking member on the Intelligence Committee for the 108th Congress. At the request of the house speaker and minority leader, she previously helped spearhead all House actions in response to the September 11 attacks as ranking member on the panel's Subcommittee on Terrorism and Homeland Security. Harman was also appointed to the new House Select Committee on Homeland Security. In 1999, Harman was named regents' professor at the University of California, Los Angeles, where she taught public policy and international relations. Earlier in her career, she served as special counsel to the Defense Department, deputy cabinet secretary for President Carter, and chief counsel and staff director of the U.S. Senate Judiciary Subcommittee on Constitutional Rights.

Jerry Hauer is assistant secretary for public health emergency preparedness at the Department of Health and Human Services. In this role, Mr. Hauer is responsible for coordinating U.S. medical and public health preparedness and response to

emergencies, including acts of biological, chemical, and nuclear terrorism. He has more than 20 years experience in emergency management. Most recently, he was the first director of the mayor's Office of Emergency Management for New York City. During his tenure there, he was charged with coordinating the city's on-scene response to multi-agency emergencies and drafting the city's emergency response plans to natural and man-made events. Mr. Hauer has also served as the executive director of the state of Indiana's Emergency Management Agency, as well as its Department of Fire and Building Services. Mr. Hauer has served on the National Academy of Science's Institute of Medicine's Committee to Evaluate R&D Needs for Improved Civilian Medical Response to Chemical or Biological Terrorism Incidents, and was an adviser to the U. S. Marine Corps' Chemical-Biological Incident Response Force. He is an adviser to the Columbia University's School of Public Health and the University of Southern California's School of Medicine. He is also a member of the Johns Hopkins Working Group on Civilian Biodefense. Mr. Hauer has served as a volunteer firefighter, a member of the Fairfield County Hazardous Materials Response Team, and in the U.S. Army Reserve attached to the Walter Reed Army Institute of Research. Mr. Hauer has a master's degree from the Johns Hopkins Bloomberg School of Public Health.

David Heyman is a senior fellow and director of the Homeland Security Program at CSIS. Prior to joining CSIS, he served as a senior adviser to the secretary of energy from 1998 to 2001. From 1995 to 1998, he worked in the Office of Science and Technology Policy, National Security and International Affairs Division, coordinating U.S. policies, programs, and budgets related to international cooperation in science and technology. Before entering government, Mr. Heyman briefly worked as a consultant with Ernst & Young in their International Privatization and Economics Group in London and was the director of international operations for a New York–based software company developing supply-chain management systems for Fortune 100 firms. He has worked in Europe, Russia, and the Middle East. His recent publications include *Public Domain Information: Legal Pressures in National Security Restrictions* (2003), *Lessons from the Anthrax Attacks: Implications for U.S. Bioterrorism Preparedness* (2002), as well as contributions to *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories* (2002). Mr. Heyman received a bachelor's degree from Brandeis University and a master's degree in technology policy and international economics from Johns Hopkins University School of Advanced International Studies.

Nuala O'Connor Kelly is the chief privacy officer at the Department of Homeland Security. In this capacity, she is responsible for privacy compliance across the organization, including assuring that technologies sustain privacy protections relating to the use, collection, and disclosure of personal information. Prior to her service at the Department of Homeland Security, Ms. O'Connor Kelly served as chief privacy officer at the U.S. Department of Commerce. While at Commerce, she also served as chief counsel for technology, and as deputy director of the Office of Policy and Strategic Planning. Prior to her service in the Bush

administration, Ms. O'Connor Kelly was vice president for data protection and chief privacy officer for emerging technologies of the online media services company, DoubleClick. She also served as the company's first deputy general counsel for privacy. She practiced law with the firms of Sidley & Austin, Hudson Cook, and Venable, Baetjer, Howard & Civiletti in Washington, D.C. Ms. O'Connor Kelly is a member of the bar in Washington, D.C., and Maryland. She received her bachelor's degree from Princeton University, a master's of education degree from Harvard University, and a J.D. from the Georgetown University Law Center.

Jody Lanard M.D. is a psychiatrist who writes and consults on psychological aspects of risk communication. With her husband and colleague, Peter Sandman, she has been consulting with the World Health Organization on SARS communication since March, and has written in the Asian press about Singapore's extraordinary SARS risk communication. Dr. Lanard recently consulted with FEMA's Northern Virginia Community Resilience Project on addressing the terrorism worries of different target audiences (e.g., the fearful and dependent, the counterphobic brave and bold, people in denial, and others). Several of Dr. Lanard's articles can be found on the Peter Sandman Risk Communication Web site at www.psandman.com. Dr. Lanard attended the University of Pennsylvania Medical School and did her psychiatric residency at Harvard University.

John MacGaffin III is the president of MacGaffin and Associates. He has been involved in matters of intelligence collection, law enforcement, counterterrorism, counterintelligence, and security for almost 40 years. Mr. MacGaffin served with the Central Intelligence Agency for 31 years, including 5 assignments overseas as chief of station, primarily in the Middle East. After leaving the CIA, he became senior adviser to the director and deputy director of the FBI, with responsibility for long-range enhancement of CIA/FBI relationships and for development of the FBI's Five-year Strategic Plan. Beginning in 1998, he chaired a commission to restructure the national counterintelligence system. Since the conclusion of the commission, Mr. MacGaffin has served as a consultant to various government departments and corporations providing advice and assistance in a range of areas including counterterrorism, counterintelligence, and security. Mr. MacGaffin currently serves on the Defense Science Board Taskforce on Homeland Security and is a member of the CSIS Project on Transnational Threats. He also participates in a working group on the potential impact of terrorism on the agriculture and public health communities sponsored by ANSER. He was a member of the CSIS Global Organized Crime Project and in 2002 was a member of the Defense Science Board Taskforce on Intelligence in Support of the War on Terrorism.

Joseph Onek is senior counsel and director of the Liberty and Security Initiative, The Constitution Project, Georgetown University. A graduate of Yale Law School, he has practiced in both public interest and private law firms in the areas of constitutional law and health law. He first served in government as a law clerk to

Chief Judge David L. Bazelon of the District of Columbia Circuit and Supreme Court Justice William J. Brennan and as a Senate staffer. In the Carter administration, he served as a member of the White House Domestic Policy staff and then as deputy counsel to the president. In the Clinton administration, he served as principal deputy associate attorney general and as senior coordinator for rule of law in the State Department.

William H. Parrish is acting assistant secretary for information analysis at the Department of Homeland Security. Prior to assuming this position, Mr. Parrish served as senior adviser to the secretary of homeland security for combating terrorism and as the senior homeland security representative to the Terrorist Threat Integration Center. He was also the lead planner and coordinated the implementation of Operation Liberty Shield in the United States and territories while Operation Iraqi Freedom was under way. Previously, he served in U.S. Customs where he established the first Office of Antiterrorism in 2001. During his Marine Corps career, Mr. Parrish served as commanding officer of the U.S. Marine Corps Security Forces, where he was responsible for expanding the capabilities of Fleet Antiterrorism Security Teams (FAST) in support of antiterrorism operations worldwide. As commander of FAST, Colonel Parrish led a specialized antiterrorism unit in response to the Khobar Towers bombing, and developed an extensive force protection and antiterrorism security plan for U.S. installations in Bahrain. Mr. Parrish received his bachelor's degree in criminal justice from Central Missouri State University. He earned a master's degree in international strategic studies from the Naval War College, as well as a master's degree in management from Salve Regina University.

Jim Pebley is a retired naval officer and pilot, currently employed as a project manager by the Northrop Grumman Corporation in the field of systems engineering. He served 22 years in the U.S. Navy, including tours as a patrol plane commander, on the staff of the Seventh Fleet and on the Joint Staff under General Colin Powell. He also served as a nuclear weapons system development and acquisition manager with the Department of Energy (seconded from the Navy) before retiring to Arlington, Virginia. He became a participant in Arlington's active civic affairs scene, first as a civic association president and later for two terms as the president of the Arlington County Civic Federation, the umbrella organization for 84 civic organizations. He served five years on the County's Fiscal Affairs Advisory Commission. Mr. Pebley was an early advocate of public emergency preparedness (before September 11) and a catalyst for the formation of the county's Citizen Corps Council (CCC). He currently serves as chair of the CCC's Public Emergency Communications Task Group. He holds a bachelor's degree in physical sciences and dual master's degrees in national security studies and general management. In 2002 he was the recipient of the Journal Newspapers "Journal Cup" for outstanding civic service and has published articles in the *Washington Post*, the Journal Newspapers, and trade publications.

Jason Sapsin joined the faculty of the Department of Health Policy and Management at the Johns Hopkins Bloomberg School of Public Health in October 2001. He is a member of the Center for Law and the Public's Health at Johns Hopkins and Georgetown Universities. With other center faculty he is a coauthor of the Model State Emergency Health Powers Act. Currently, he focuses on public health preparedness and bioterrorism, developing a legal training module for emergency public health response for the Centers for Disease Control and Prevention. Mr. Sapsin is an author of publications dealing with the Model State Emergency Health Powers Act, public health law and emergency response, and litigation as a public health tool. His interests include public health strategies for epidemic control, administrative regulation, and trade and health. He is affiliated with the Johns Hopkins Centers of Excellence in Environmental Public Health Tracking and Environmental Public Health Practice. Mr. Sapsin is a graduate of Williams College, the University of Michigan Law School, and Johns Hopkins University. Prior to joining Hopkins, he practiced international litigation and health legislative policy at a Washington, D.C., law firm, served as a corporate vice president and general counsel, and engaged in trial, appellate, and administrative practice. His community activities have focused primarily on child education and welfare.

Tasia M. Scolinos is the Department of Homeland Security's senior director for communications. She oversees more than two hundred public affairs employees who are part of the new department. Ms. Scolinos joined the homeland security transition planning office as the director of internal communications. In that capacity she was also instrumental in structuring all facets of the department's Public Affairs Office. Previously, she served as the Treasury Department's lead spokeswoman for all law enforcement and terrorist financing issues. A native of Arcadia, California, Ms. Scolinos has practiced law in the private sector and has appeared on television shows as a legal and political commentator. She received her bachelor's degree from Claremont McKenna College and earned a J.D. from the Georgetown University Law Center.

Representative Christopher Shays (R-Conn.) serves as vice chairman of the House Government Reform Committee and as chairman of its Subcommittee on National Security, Emerging Threats and International Relations. In this role and as cochairman of the Congressional Nonproliferation Task Force, Shays helped lead the effort to reduce the threat of weapons of mass destruction and prepare emergency response teams to handle potential terrorist attacks. Representative Shays held 22 hearings assessing the terrorist threat prior to September 2001 and has convened more than 40 hearings in all documenting the need for American citizens, the media, and our government to take this threat more seriously, develop a strategy to combat it, and reorganize our government to more effectively respond to this threat. As a result of his work, he was appointed by Speaker Hastert to serve on the new Select Committee on Homeland Security at the beginning of the 108th Congress. He also serves as vice chairman of the House

Budget Committee and is a member of the Financial Services Committee. Shays was first elected to the Connecticut House of Representatives in 1974.

Amy E. Smithson was recently named a senior fellow in the CSIS International Security Program where she will concentrate on nonproliferation issues, particularly focusing on chemical and biological weapons. Previously, she was a senior associate at the Henry L. Stimson Center where she directed the Chemical and Biological Weapons Nonproliferation Project, which she launched in January 1993 to serve as an information clearinghouse, watchdog, and problem solver on chemical and biological weapons issues. Dr. Smithson has conducted in-depth, first-source research on such topics as the lackluster implementation of the Chemical Weapons Convention, the difficulties associated with destroying U.S. and Russian poison gas arsenals, the threat of unconventional terrorism and the U.S. response to it, the mechanisms needed to strengthen bioweapons nonproliferation, and the efforts to prevent the leakage of weapons knowledge and materials from the former USSR's chemical and biological weapons complexes. She has testified before Congress and is frequently consulted by the media on chemical and biological weapons issues. Before joining the Stimson Center in 1990, Dr. Smithson worked at Pacific-Sierra Research Corp. and the Center for Naval Analyses. She received her doctorate in political science from George Washington University, her master's degree in international relations from Georgetown University, and two bachelor's degrees in political science and Russian from the University of North Carolina, Chapel Hill.

Edward J. Staffa is currently vice president, pharmacy practice & communications, at the National Association of Chain Drug Stores Foundation (NACDS). In this capacity, he has responsibility for pharmacy practice issues, such as patient safety and also oversees a variety of association communications. Mr. Staffa writes the weekly *NACDS Update*, distributed to pharmacy and government executives, and is also the editor of the NACDS Foundation's *Chain Pharmacist Practice Memo*, a monthly newsletter distributed to front-line practicing pharmacists. Prior to joining NACDS, Mr. Staffa was a practicing community pharmacist for 16 years, most recently as a pharmacist and pharmacy manager for 11 years with Giant Food of Landover, Maryland. Mr. Staffa is a graduate of the University of Rhode Island's College of Pharmacy and is a licensed pharmacist in the state of Maryland.

Representative Jim Turner (D-Texas) is serving his fourth term in Congress representing the Second Congressional District of Texas. As the ranking member of the House Select Committee on Homeland Security, Representative Turner is working to protect the safety and security of the American people in the war on terrorism. As a member of the Armed Services Committee, he has served as the ranking member of the Terrorism Subcommittee. Before his election to Congress, Representative Turner served 10 years in the Texas Senate and the Texas House. His lifetime interest in public service has given him the opportunity to serve under four former governors of Texas in positions ranging from mail room clerk to chief

of staff. In the Texas Senate, he was recognized as an outstanding legislator by a number of statewide organizations for his leadership in health care, criminal justice, education, and on behalf of Texas children. Representative Turner earned his bachelor's and master's degrees in business and his law degree from the University of Texas at Austin. He served in the U.S. Army, attaining the rank of captain.

Anne Witkowsky is a senior fellow in the Technology and Public Policy Program at CSIS. At CSIS, she directed the Commission on Science and Security, mandated by the secretary of energy. Prior to joining CSIS in September 2000, Ms. Witkowsky was a director for defense policy and arms control at the National Security Council (NSC). At the NSC, she was responsible for conventional arms control and European defense issues. Her work included negotiation and implementation of conventional arms limitation agreements (the adapted CFE Treaty), European confidence- and security-building measures, humanitarian law agreements, and policy related to antipersonnel land mines. She also covered a wide range of NATO defense matters. From 1988 until joining the NSC staff in 1993, she served in the Office of the Secretary of Defense, including the Office of Russian, Ukrainian, and Eurasian Affairs, and the Office of European Security Negotiations. She is a recipient of the Defense Distinguished Service Award. Ms. Witkowsky holds a bachelor's degree in Russian and East European Studies from Yale University and an M.P.A. with a concentration in international security from Harvard University's Kennedy School of Government.