THE RESILIENT HOMELAND: HOW DHS INTELLIGENCE SHOULD EMPOWER AMERICA TO PREPARE FOR, PREVENT, AND WITHSTAND TERRORIST ATTACKS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MAY 15, 2008

Serial No. 110–115

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

43–940 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey
PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*
DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

CONTENTS

THE RESILIENT HOMELAND: HOW DHS INTELLIGENCE SHOULD EMPOWER AMERICA TO PREPARE FOR, PREVENT, AND WITHSTAND TERRORIST ATTACKS

Thursday, May 15, 2008

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,
AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 10:08 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chair of the subcommittee] presiding.

Present: Representatives Harman, Dicks, Perlmutter, Reichert, Shays, and Dent.

Ms. HARMAN. The subcommittee will come to order.

We meet today to receive testimony on "The Resilient Homeland: How DHS Intelligence Should Empower America to Prepare for, Prevent and Withstand Terrorist Attacks."

For more than 6 years, the Bush administration has been relentlessly sounding the alarm about apocalyptic terrorist groups, but meaningful guidance to first responders about what to look for and what to do about these apocalyptic terrorist groups has been in short supply.

One of today's witnesses, a valued friend and counselor, Dr. Stephen Flynn, labels this a "toxic mix of fear and helplessness" in his recently published article, "America the Resilient." He sees it increasing the risk that the U.S. Government will overreact to another terrorist attack. I agree.

What Dr. Flynn says about resiliency and information-sharing is also on the mark. He says, "After decades of combating Soviet espionage during the Cold War, the Federal security establishment instinctively resists disclosing information for fear that it might end up in the wrong hands. Straight talk about the country's vulnerabilities and how to cope in emergencies is presumed to be too frightening for public consumption."

Well, in my view, the American people deserve honesty about what threatens us and deserve an open discussion about what we need to do to protect ourselves and our families from the terrorists who want to kill us. Make no mistake: There are terrorists out there who want to kill us.

This subcommittee has spent the last year-and-a-half working to get intelligence right for State, local and tribal law enforcement of-

ficers, the people who will most likely see something out of place and act to prevent the next attack. Starting with the information needs of State and locals is the way to go. I think we are unanimous, on a bipartisan basis, about that, and so is Matt Bettenhausen of California, Juliet Kayyem of Massachusetts, Frank Cilluffo at GW, who testified at last month's hearing.

There is good news here. Let me be clear, there is good news here. Police and sheriff's officers increasingly see themselves as our Nation's first preventers. That is a term we use here too, but they use it. Obviously, it makes much more sense to prevent or disrupt an attack than to respond to one.

At the same time, they have started to understand the full impact of what "prevention" means, that the critical infrastructure in their communities—power plants, mass transit, public health, chemical facilities, roadways, bridges and telecom—are all part of their protective responsibility.

We are finally making progress, a point I stressed at a major conference in San Francisco in March. The Department of Homeland Security's intelligence products are better. They include some local input, and put first preventers in the private sector on notice about a number of things: which terror plots most threaten the homeland; what State, local and tribal private-sector leaders should be doing to prepare for them so we can bounce back quickly; and how best to put those preparations into action, by running drills and exercises and testing the resiliency of the systems we are establishing.

By honestly assessing our vulnerabilities and preparing all levels of government, the private sector and the public to protect against them, we will become more and more secure in our ability to withstand attacks from our enemies.

After all, what is terrorism? Terrorism is the ability to terrify. If we are prepared, or as prepared as we can be, we will surely be less terrified and surely have more capability to prevent attacks.

I look forward to the testimony this morning. This is an excellent panel. I welcome all our witnesses.

I now yield to the Ranking Member, Sheriff Reichert, for his opening remarks.

Mr. REICHERT. Thank you, Madam Chair.

Good morning and thank all of you for being here this morning with us. We look forward to your testimony and your responses to our questions.

While the Department of Homeland Security's Office of Intelligence and Analysis should be primarily focused on preventing terrorist attacks, they do have a role in resiliency and in ensuring that they have a full continuity of operational plans in place in case of a terrorist attack.

As a part of these efforts, the Department of Homeland Security is working to ensure that they can provide the services that State and local governments need to prevent future attacks and recover from any attacks that may take place.

In order to help with these resiliency efforts, the Department has worked hard to create an information-sharing system that is multilayered and fairly resilient. In addition to off-site facilities that can

house analysts and intel components, DHS has several information-sharing councils that they can use to share information.

These councils and information-sharing mechanisms, however, are only as good as the resiliency of the communications backbone. DHS has worked to create an unclassified Homeland Security Information Network, called HSIN, that is available from any computer terminal, making HSIN available even when other Government facilities are not.

For secure communications, DHS has also built communications resiliency through the Homeland Secure Data Network and secure voice communications. Additionally, intelligence and analysis communications will benefit immensely from the legacy systems deployed to the fusion centers across the country. Many fusion centers have Department of Defense networks and communication through FBI, ICE, CBP and the Coast Guard. Ironically, one of the many things that we hear complaints about multiple networks and information systems may actually be helpful in making sure that States and locals have effective communication channels in the wake of an attack. Finally, while threat information can help prevent terrorism, specific information on the composition of the threat when available can help manage the consequences of an attack.

I look forward to hearing from our witnesses today on what else I&A has done to aid resiliency and what they may be able to better do before the next attack.

I yield.

Ms. HARMAN. I thank the Ranking Member.

Other members of the subcommittee are reminded that, under the committee rules, opening statements may be submitted for the record.

It is now time to welcome our witness.

Our first witness, Dr. Stephen Flynn, is the Jeane J. Kirkpatrick senior fellow for national security studies at the Council on Foreign Relations, where we he directs an ongoing private-sector working group on homeland security. Dr. Flynn is a consulting professor at the Center of International Security and Cooperation at Stanford and a senior fellow at the Wharton School of Risk Management and Decision Processes Center at the University of Pennsylvania.

From August 2000 to February 2001, Dr. Flynn served as the lead consultant to the U.S. Commission on National Security. He served in the White House Military Office during the George H. W. Bush administration and as director for the global issues on the National Security Council staff during the Clinton administration. He is the author of many books and someone I call when I want to understand this issue better.

Our second witness, Amos Guiora, is professor of law at the S.J. Quinney College of Law at the University of Utah. Professor Guiora teaches criminal law, global perspectives on counterterrorism, religion and terrorism, and national security law. His publications include the published case book, "Global Perspectives on Counterterrorism," as well as the forthcoming titles, "Constitutional Limits on Coercive Interrogation" and "Terrorism Primer."

Professor Guiora writes and lectures extensively on issues such as legal aspects of counterterrorism, global perspectives of counterterrorism, terror financing, international law, and morality in armed conflict. He served for 19 years in the Israel Defense Forces Judge Advocate General Corps, where he held a number of major senior command positions.

Our third witness, R.P. Eddy, is a senior fellow for counterterrorism at the Manhattan Institute and the executive director for the Center for Policing Terrorism, CPT. He is also CEO of Ergo Advisors. Mr. Eddy has worked with the NYPD, LAPD, the Greek Government, the United Nations, and various multinational corporations on terrorism and security issues. He is founding member of the International Counterterrorism Academic Community.

Previously, Mr. Eddy was senior policy officer to the U.N. Secretary General, as director the counterterrorism at the White House National Security Council, chief of staff to the U.S. Ambassador to the United Nations, Richard Holbrooke; senior advisor for intelligence and counterterrorism to the Secretary of Energy; and a U.S. representative to international negotiations, including the creation of the International Criminal Court.

Obviously, we have people who know this subject inside and out.

The subcommittee welcomes you.

Without objection, your full statements will be inserted in the record, and I urge you to summarize your statements, each of you, to summarize your statements for 5 minutes. There is a little clock that will start beeping close to 5 minutes. In order to allow time for questions, I will try to cut you off.

Finally, let my say in advance, we are expecting procedural votes on the floor this morning, so this hearing may have to be recessed a couple of times. Hopefully, if we are very efficient, we will be able to do this and then leave for votes.

Dr. Flynn, you are the first witness.

STATEMENT OF STEPHEN E. FLYNN, PH.D., JEANE J. KIRKPATRICK SENIOR FELLOW FOR NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS

Mr. FLYNN. Thank you very much. It is an honor to be before you today and the distinguished members of this subcommittee on this hearing, which I really commend your leadership for hosting.

To some extent, I increasingly describe myself as a bit like a reformed, recovering alcoholic, as a reformed national security guy. Reformed in two ways: first, in having to come to grips with the inherent limits of the professional tools often available to national security professionals to deal with the threat that we must as a Nation deal with in this post-9/11 world; and, second, for underestimating the capacity of the American people to play an essential role in supporting that.

I would argue that I, like many of the generation of folks who are now at the front lines in our national security apparatus, are creatures of a Cold War where essentially the security was in the hands of a few while we, as everyday citizens, went about our lives. Problems were managed beyond our shores, and they were managed with the tools that we have available and dominate in, in terms of what other nations have around the world.

But I make the case in my written testimony, and it is one that I feel increasingly more passionate about, that really, with the benefit of hindsight, we missed one of the most important and, I would argue, critical lessons of September 11. Nine-eleven taught us not only that we have a determined adversary who is intent on exploiting vulnerabilities here at home to cause mass destruction and disruption, but also that the greatest asset we have as our Nation is the "we, the people" part.

That story is really captured in, not the first three airplanes, but the fourth, United 93. United 93 was, of course, the plane that got off the ground late, and it was the one plane where the passengers on board got information that was critical for them to do something extremely important in time enough for them to act. They got that information not because it was shared with them via the U.S. Government, but they got it in the course of frenzied phone calls made to friends and loved ones in the heart of the emergency, where they found out something that, again, parts of our U.S. Government knew but the general public did not know, which is that we had an adversary out there intent on taking an airplane and turning it into a missile.

Armed with that information, those passengers did something that was critical for this body, as well as for the other branch of Government just down the other end of Pennsylvania Avenue. Armed that with information, they charged the cockpit and kept that target—foiled al Qaeda from reaching its likely intended target, which was here in Washington.

There is an enormous irony and, in a larger sense, I would argue, a quintessentially heroic part of the American narrative captured in what those passengers did. The people who are gathered in this town with the sworn obligation, as our Constitution requires, of providing for the common defense were, themselves, on September 11 defended by one thing alone: an alerted, brave, everyday citizenry.

The Air Force did not know the plane had been taken hostage and was heading this way. There were no Federal air marshals aboard the plane. The only thing that kept it from reaching its intended target was the alerted, courageous, everyday Americans who were gathered in that plane.

That should have been something we in Washington took as a very sober lesson with a healthy element of humility: that, in the end, managing a threat that increasingly will be in the civil and economic space cannot possibly be achieved without including as many of the people who occupy it as possible. Those will turn out to be everyday citizens, State and local officials, and private-sector leaders.

We should have been working overtime in the immediate aftermath of September 11, empowering and informing and inspiring those very same players to be a part of the solution of managing the terrorist hazard.

Unfortunately, we had a Cold War reflex, which was essentially to say the national security apparatus of this country must do whatever it takes, further empowered with new authorities and resources, to prevent and protect the American people from this ever happening again.

Now, that is a potent tool, and I want to continue to use it. But the nature of this threat, again, as 9/11 should have taught us, is in a place which is more likely to be occupied by civilians than it is by our active-duty military, our spies or Federal law enforcement apparatus.

What this screams to is the imperative that this hearing is holding, is a need to get information out to the people who are most likely to be the first preventers and the first responders, and engaging them in meaningful ways to deal with this hazard.

What we have is enormous structural barriers, a culture that grew up in the Cold War that treats the American people as either potential victims or possibly, because they haven't been vetted, as part of the problem, but also the classification schemes and so forth that we have in place that make it difficult to get that information out to them.

So I would be happy, of course, to address a lot of these issues and some of the recommendations I have here in my testimony during the questions. But I think what is fundamental here—and I hope this hearing can help to develop, and it is clearly something we will probably have to look toward in the next administration regardless of party—but is a change in course that really empowers and enables and inspires the American people to be a part of the solution and make sure that the Department of Homeland Security is able to provide them those tools.

[The statement of Mr. Flynn follows:]

PREPARED STATEMENT OF STEPHEN E. FLYNN

MAY 15, 2008

Chairwoman Harman, Ranking Member Reichert, and distinguished members of the House Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, thank you for inviting me to provide an assessment of the current U.S. Government efforts to share intelligence and homeland security information with the American public. This issue has for too long received only cursory attention, and I commend your leadership for holding this important hearing today.

As a stepping off point, it is my strongly held view that the single greatest lapse in leadership in response to the attacks of September 11, 2001 was the failure of the White House and Congress to look beyond the U.S. military and the national and homeland security agencies in formulating its response to the terrorist threat. As a result, it has neglected the Nation's greatest asset: the legacy of American grit, volunteerism, and ingenuity in the face of adversity. Instead, the Bush administration has sent a mixed message, declaring terrorism to be a clear and present danger while, at the same time, telling Americans to just go about their lives. Unlike during World War II when everyday people, industry leaders, and local and State officials were mobilized in a national effort, since 9/11, national security and homeland security officials have too often treated citizens as potential security risks to be held at arm's length or like helpless children in need of protection.

Overwhelmingly, the national defense and Federal law enforcement community have chosen secrecy over openness when it comes to providing the general public with details about the nature of the terrorist threat and the actions required to mitigate and respond to that risk. Officials reflexively assert that candor would only "provide ideas to the terrorist and spook the public." Not only is this instinct shortsighted and counterproductive, I would argue it ignores what should have been one of the central lessons from the 9/11 attacks.

In retrospect, it is remarkable that Washington has done so little to enlist citizens and the private sector in addressing the vulnerability of the Nation to catastrophic terrorism. September 11 made clear two things. First, the targets of choice for current and future terrorists will be civilians and infrastructure. Second, safeguarding those targets can only be accomplished with an informed, inspired and mobilized public. The first preventers and the first responders are far more likely to be civilians and local officials, not soldiers or Federal law enforcement officers.

The prevailing interpretation of September 11 focuses almost entirely on the three airliners that struck the World Trade Center towers and the Pentagon. President Bush concluded from those attacks that the U.S. Government needs to do whatever it takes to hunt down its enemies before they kill innocent civilians again. He has essentially said that this is a job that must be left to more fully empowered and resourced national security professionals. However, as I recently outlined in an article published in the March/April 2008 issue of *Foreign Affairs,* it is the story of United Airlines flight 93, the thwarted fourth plane which crashed 140 miles from its likely destination—the U.S. Capitol or the White House—that ought to have been the dominant 9/11 narrative.

United 93 passengers foiled al Qaeda without any help from the U.S. Government. The North American Aerospace Defense Command (NORAD) could not intercept the flight. Officials did not even know that the plane had been hijacked. There were no Federal air marshals aboard. The passengers of United 93 mobilized to thwart their terrorist hijackers because they knew the hijackers' intention. United 93 was the last of the hijacked planes to get off the ground. Once the terrorists took control, they did not prevent passengers from making urgent calls to family and friends. These passengers found out something that their counterparts on the three earlier flights discovered only after it was too late to act: that the terrorists were on a suicide mission, intent on using the commandeered jet airline as a deadly missile. Armed with that information, the everyday Americans aboard United 93 did something very important: they charged the cockpit and prevented the plane from reaching its intended target.

In the aftermath of September 11, Washington should have soberly embraced the implications of what was both an ironic and quintessentially American testament of national strength: that the legislative and executive centers of the U.S. Federal Government, whose constitutional duty is "to provide for the common defense," were themselves defended that day by one thing alone: an alert and heroic citizenry. With regret, government officials should have acknowledged that the brave passengers aboard United 93 accomplished what they did without an advance warning of the threat, despite the fact that intelligence had been collected by the U.S. Government that terrorists were intent on using planes as missiles. That information had to be learned by way of frantic calls to family and friends during the height of the emergency.

We will never know what might have happened aboard American Flight 11 or United Flight 175—the two planes flown into the World Trade Center towers in New York—if those passengers knew what their counterparts on United 93 were able to learn. But we do know that complying with the terrorist demand to remain quietly in their seat would have been an appropriate response for people who were relying for guidance on the pre-9/11 incidents of air hijackings. The pre-9/11 protocol was for passengers to do what they were told and leave it to professional negotiators or SWAT teams to deal with the captors after the plane landed. Had the U.S. Government been open about this risk, would the other plane passengers been more alert to the possibility that they were not involved in a conventional hijacking? Would they have decided to marshal a counterattack? Sadly, it never occurred to senior officials to share this critical information with the general public. Despite otherwise exemplary work, even the 9/11 Commission failed to discuss this issue in their final report. And, if anything, when it comes to developing responses to plausible threat scenarios, the instinct within the U.S. Department of Homeland Security and across the U.S. Government has been for officials embrace secrecy instead of openness.

The discounting of the public can be traced to a culture of secrecy and paternalism that now pervades the national defense and Federal law enforcement communities. Though, in historical terms, this culture has relatively recent roots. From the founding of the American republic through World War II, everyday citizens were presumed to be willing and able to contribute to the Nation's security in times of war. It was only during the cold war that the general public was increasingly relegated to the sidelines. The immediacy, complexity, and lethality of the threat of nuclear weapons placed the fate of millions in the hands of a few. Combating Soviet espionage during this high-stake conflict resulted in an extensive classification system premised on sharing information only with well-vetted individuals who were assigned specific duties that provided them with "a need to know." Despite the passage of nearly two decades since the fall of the Berlin Wall, this secretive system remains almost entirely intact. The sanctions for not protecting classified information from unlawful disclosure include arrest and imprisonment.

Today we live in an era in which the most likely battlegrounds will lie outside the conventional military realm. Terrorists will increasingly target civilians and critical infrastructure which places a premium on creating open and inclusive proc-

esses that provide meaningful information about threats and vulnerabilities to the citizens and private sector leaders. These groups are the Nation's best positioned resources for devising and implementing plans for safeguarding likely targets, responding to attacks—as the United 93 story highlights—and recovering from them should prevention efforts fail.

There is another vital imperative for placing greatest emphasis on information sharing: it is the key ingredient for building the kind of societal resilience that is essential to depriving al Qaeda and other terrorists of the fear dividend they hope to reap by attempting to carry out catastrophic attacks. In military terms, the United States is too large—and al Qaeda's capacity too limited—for an attack to cause damage that could weaken U.S. power in any meaningful way. What they can hope for is to spawn enough fear to spur Washington into overreacting in costly and self-destructive ways.

Fear arises from the awareness of a threat coupled with a feeling powerless to deal with it. Although it is impossible to eliminate every threat that causes fear, Americans do have the power to manage fear as well as their reactions to it. However, for nearly 7 years, Washington has been sounding the alarm about weapons of mass destruction and radical jihadists while providing the American people with no meaningful guidance on how to deal with these threats or the consequences of a successful attack. This toxic mix of fear and helplessness jeopardizes U.S. security by increasing the risk that the U.S. Government will overreact in the event of another terrorist attack.

What the Department of Homeland Security should be doing is arming Americans with greater confidence in their ability to prepare for and recover from terrorist strikes and disasters of all types. Bolstering confidence in our resilience will cap fear and in turn undermine much of the incentive our current and future adversaries have for incurring the costs and risks of targeting the U.S. homeland.

The United States should be striving to develop the kind of resilience that the British displayed during World War II when V–1 bombs were raining down on London. Volunteers put the fires out, rescued the wounded from the rubble, and then went on with their lives until air-raid warnings were sounded again. More than a half century later, the United Kingdom showed its resilience once more after suicide bombers attacked the London Underground with the intent of crippling the city's public transportation system. That objective was foiled when resolute commuters showed up to board the trains the next morning.

The approach the Department of Homeland Security should be pursuing is to gather and share as much threat, response, and recovery information as possible with private industry and State and local emergency responders. At the same time, it must place far greater emphasis on informing and engaging the American public. The key is to target the relevant audience with threat information that is matched with specific guidance on how to respond to the threat. To sounds alarms about the threat without providing people with details on what they should do only needlessly stokes anxiety. This is the fundamental problem with the color-coded national alert system.

Undertaking this approach will require far more interaction with the private sector and civil society than the Department of Homeland Security can currently support. For instance, the private sector liaison office at DHS that has been capably led since its inception by Assistant Secretary Al Martinez-Fonts has only 15 civil service positions supported by seven contractors. The office responsible for Ready.Gov and the Citizen Corps is less than half that size. Citizen Corps has been funded at only $15 million per year, roughly what the United States is spending each and every hour in Iraq. The vast majority of contact the public has with the Department of Homeland Security arises from its interactions with its operational agencies like TSA, CBP, ICE, the U.S. Coast Guard, and the Secret Service. The law enforcement and security missions of these organizations have frequently translated into strained and even adversarial relationships with private industry and the general public.

This is a formula that guarantees failure. When it comes to protecting the critical foundations that support our way of life and quality of life there are few law enforcement or security officials in government who have an intimate understanding of the design and operation of the complex infrastructure or who are capable of recognizing the real versus the perceived issues. Since Federal, State, and local agencies rarely work well together, if they are left to their own devices, the result is bound to be a mix of unacknowledged gaps and misguided or redundant requirements.

The problem boils down to this: the design, ownership, and day-to-day operational knowledge of many of America's most essential systems rest almost exclusively with the private sector, both domestic and foreign. But the security of these systems

throughout and following the cold war era has been handled almost exclusively by military, national security, and Federal law enforcement professionals. Government officials are unable to protect things about which they have only a peripheral understanding and over which they have limited jurisdiction, and the market, left on its own, is unlikely to provide the socially desired level of security and dependability.

What is required is a truly collaborative approach which engages civil society and taps extensive private-sector capabilities and ingenuity for managing risk and coping with disasters. A critical barrier to advancing collaboration is excessive secrecy throughout the Federal Government reinforced by a reflexive tendency to classify material or to designate it as "For Official Use Only" or "Treat as Classified." This instinct is enormously counterproductive since it holds the process of information system hostage to a completely overwhelmed and increasingly dysfunctional security clearance process. In order to successfully accomplish its core mission, the Department of Homeland Security should be taking the lead within the Federal Government in instituting controls to prevent the inappropriate classification of information and to work aggressively to declassify material so that vital information reaches the people who are best positioned to act on it.

The Department of Homeland Security should be provided with a clear mandate for public outreach and 750 new positions to be deployed to major cities around the country and at its headquarters. Each morning these individuals should arrive at their office and respond to this question: "Who needs homeland security-related information and how can I work to get it to them?" DHS should be the chief Federal conduit for sharing intelligence and threat, response, and recovery information with the Nation. They should lead the charge of moving the intelligence community away from its cold war "need-to-know" paradigm and toward the essential "need-to-share" paradigm that today's threat imperative requires.

Three tactical changes should be made immediately to help signal the overdue change in direction on information sharing. First, DHS should abandon the color-coded national alert system. Its fatal flaw is that it provides no meaningful guidance to the general public on what they should do. An alert system will never work at the national level. It must be tailored to regions, communities, and sectors where there is a known audience. Second, DHS should embrace the notion of "resilience" as a core strategic objective. Resilience is a concept that has the advantage of being an adult-like acknowledgment that disasters cannot always been prevented, but pragmatic measures can be taken to minimize the risk of occurrence and the consequences that can flow from them. In addition, resilience can only be achieved by an open and inclusive process that serves as a check on the secretive instincts of security professionals. Third, DHS must commit itself to making information sharing with local officials, the private sector, and the general public a two-way street with robust capabilities in place to support this. Only if DHS is committed to leading a team-effort will it achieve its mission.

In the end, it is essential that the next administration revisit the excessive reliance President Bush has placed on the U.S. military and intelligence community for dealing with the dangers associated with terrorism. These capabilities were developed for a different adversary, in a different time during which a closed and secretive culture was justifiable. However, America's greatest asset has always been and remains the industry, inventiveness, and patriotism of its people. Actively engaging the public in the work of managing the hazards of our post-9/11 world must be the top priority for the next President and the U.S. Congress.

Thank you and I look forward to responding to your questions.

Ms. HARMAN. Thank you, Dr. Flynn. I think this subcommittee has been channeling your thoughts for quite a while.

Mr. Guiora.

STATEMENT OF AMOS N. GUIORA, PROFESSOR OF LAW, UNIVERSITY OF UTAH

Mr. GUIORA. Thank you very much. It is a pleasure and an honor to be here this morning.

When I examined the issue that I have been asked to address this morning, I think that, in order to frame the issue, I think what we need to do is to establish the paradigm. To do so required defining terms, because I think without defining terms it is going to be very difficult for this subcommittee to go forward.

So the question is, what is effectiveness? What is accountability? What is terrorism? What is counterterrorism? What is homeland security? What is this threat assessment that we are all talking about? Because without doing that, we can't really begin the process of discussing a private-public partnership in information-sharing.

So I begin with what is terrorism. I think terrorism is obviously an attack against innocent civilians for the purpose of advancing a cause. There are a variety of causes out there. But when we talk, then, about counterterrorism, we need to understand that there are inherent limits on what counterterrorism is and what counterterrorism can do, meaning that when we talk about effectiveness in counterterrorism, the inherent understanding is that there are limits on power.

How, then, does that play into what we are talking about here, information-sharing? Information-sharing must play itself out on two different levels simultaneously, not in a linear fashion. First, as you referred to in your opening statement, there must be information-sharing between local, State and Federal Government. Without that up and down, bottom-up and top-down, without that, it is going to be absolutely impossible for the first preventers to be involved and to understand what is happening.

In addition to that, there must also be information-sharing between the public sector and the private sector. That obviously raises important constitutional legal questions in terms of how we are going to have a partnership between the two. But if we don't begin the process of having online, active information-sharing between the public and the private sector, I suggest that it will be all but impossible to truly develop a homeland security strategy.

If we don't have a homeland security strategy, then all we are really doing is having a tactical response to an attack, rather than having a strategic preventive policy in place beforehand.

I would suggest, then, Madam Chairwoman, there are three things that we need to talk about. No. 1 is clearly defined roles between the Government and the private sector. No. 2, in order to establish this coordinated preventive and response plan, we are going to have to articulate and institutionalize the information-sharing. No. 3, in order to most effectively implement that, I think it is going to be incumbent upon the Congress, maybe starting with this subcommittee, to develop simulation exercises that are scenario-based in which both the private sector and public sector can work together for the following purposes: No. 1, to develop a plan in advance of; and, No. 2, to develop a plan that would enable a response in the aftermath of.

If we are going to talk about resilience, we also have to then define what is resilience and what are our reasonable expectations. Given the fact that I think it is going to be impossible to prevent all acts of terrorism, the question is, what are we going to try to do? What we are going to try to do, Madam Chairwoman, is to have a plan that enables us to minimize the loss, minimize the cost in the aftermath of the attack. Which also means that we have to be very honest with the American people, in terms of what are the reasonable expectations.

Resilience, then, is a plan that must be implemented with reasonable expectations, also given the fact that there are limited resources. Ultimately, then, I would say, with respect to my opening statement, that it is going to require cooperation and coordination in information-sharing between the internal sectors and external sectors.

I would just say, in conclusion, that the work that I have done with my students at the University of Utah, what we have really tried to do is to articulate the limits of power and how that then plays into the development of an effective resilience plan.

Thank you.

[The statement of Mr. Guiora follows:]

PREPARED STATEMENT OF AMOS N. GUIORA*

MAY 15, 2008

I. INTRODUCTION

To ensure a resilient homeland in a post-9/11 society, the United States must have a homeland security strategy that (1) understands the threat, (2) effectively counters the threat while preserving American values, (3) establishes a system of accountability, and (4) creates public-private and Federal-State partnerships facilitating intelligence sharing and the continuity of society in the aftermath of an attack.

It is necessary to work with clear definitions of the terms and concepts that frame this strategy. As I have previously articulated, "one of the greatest hindrances to a cogent discussion of terrorism and counterterrorism has been that the terms lack clear, universal definitions."[1] For this reason, I will provide clear, concrete definitions of all key terms relevant to articulating strategy necessary for a resilient homeland.

II. UNDERSTANDING THE THREAT

A. Terrorism: Recommended Definition[2]

I define terrorism as: "Terrorism: Acts of politically based violence aimed at innocent civilians[3] with the intent to cause physical harm, including death, and/or conducting psychological warfare against a population aimed at intimidating it from conducting its daily life in a normal fashion."

I have chosen the definition above because it captures the core elements of terrorism in clear and concise language. In reviewing scholarship and terrorists' writings, the overwhelming impression is that causing harm (physical or psychological) to the innocent civilian population is the central characteristic of terrorist action. The available literature articulates that harming civilians is the most effective manner—from the terrorist mindset—to effectuate their goals.

While causing death or injury to the innocent civilian population is the "means to the end," I also suggest that intimidation of the population is of equal importance from the terrorist perspective. The emphasis—whether resulting in death, injury, property damage, or intimidation—is the attack, in whichever form, on the innocent civilian population. Accordingly, government must develop counterterrorism policies that protect the innocent civilian population.

In addition, the importance of impacting "daily life" cannot—and should not—be underestimated. Terrorism is a daily grind; it must be understood in the context of daily attacks rather than one-time, dramatic-effect attacks (such as 9/11). Smaller, more frequent attacks, while perhaps less "dramatic," have a much greater long-

---

*Professor of Law, S.J. Quinney College of Law, University of Utah. Publications include *Global Perspectives on Counter-terrorism,* casebook (Aspen); *Constitutional Limits on Coercive Interrogation* (OUP); *Understanding Counterterrorism* (Aspen, Fall 2008); and, general editor, *Annual Review—Top Ten Global Security Law Review Articles, Vol. I* (Oxford University Press, 2008). I would like to thank Tara Harrison, Pete Lattin, Rachel Otto, Rich Roberts, Evan Tea, Artemis Vamianakis, and Tasha Williams.

[1] Amos N. Guiora, *Global Perspectives on Counterterrorism* (Aspen Publishers 2007) [hereinafter Guiora, *Global Perspectives*].

[2] Id. at 5.

[3] *[Sic].*

term effect on an innocent civilian population than does a one-time major event whose undeniable short-term effect may not linger.

III. EFFECTIVELY COUNTERING THE THREAT WHILE PRESERVING AMERICAN VALUES

A. Counterterrorism: Recommended Definition

I define counterterrorism as: "Counterterrorism: The term must be viewed with two prongs (separate, yet of equal importance): the actions of a state, proactive or reactive, intended to kill or injure terrorists and/or to cause serious significant damage to the terrorist's infrastructure[4] and re-financing (financing) of socio-economic depressed regions of the world and educating communities regarding democracy and its values".

Counterterrorism "is a never-ending war of attrition conducted in baby steps comprised of some victories [and] some defeats." Defining counterterrorism is inextricably linked to the definitions and limits of terrorism. Counterterrorism must also be considered in the context of domestic balancing, international law, judicial activism, intelligence gathering, and interrogation of detainees.

Furthermore, any useful definition of counterterrorism requires a recognition of critical attributes of operational counterterrorism—"actionable intelligence, operational capability, and an understanding that swift victory is, at best, a fiction."[5] Counterterrorism in civil democratic societies must also be "conducted according to the rule of law and morality in armed conflict."[6]

I propose that "operational counterterrorism is effective if the terrorist infrastructure suffers serious damage, thereby preventing a particular, planned attack from going forth and postponing or impacting plans for future attacks."[7] It is important to note, that "the damage is not permanent; terrorism cannot be defeated. However, the tactical impact of the measures above should not be minimized . . . [B]y attacking the terrorist—rather than the state sponsor—the effectiveness model described above is not strategic and therefore inherently limited."[8]

B. Homeland Security: Recommended Definition

I define Homeland Security as: "Homeland Security: A group of preventative measures undertaken by a state in an attempt to reduce the probability that a terrorist attack will occur. This strategy will be fluid, constantly reassessing the balance between rights of the individual and rights of the state. A realistic strategy must prioritize threats according to their probability and imminence."

Priorities must be established according to the limits, both ideologically and fiscally, that the American people will support. In examining government policy in the aftermath of 9/11 the lack of a concentrated and realistic focus is dramatically apparent. In seeking to address "all" possible threats, the policy was, in actuality, not a policy.

Numerous State, Federal and municipal agencies must work together to ensure public safety in the United States. These include law enforcement agencies, the military and intelligence gathering and analysis realms, public health, and emergency response sectors, which coordinate activities with the community's utilities, infrastructure, transportation, police and fire personnel. Job security, education, and community values in the aftermath of an attack are critical components of homeland security.

Executive branch documents name two particular areas the United States must be protected against in the context of homeland security: first, al-Qaeda, its affiliates (international and domestic), and those inspired by them; and catastrophic events, including natural disasters and man-made accidents.[9] Scholars have suggested three priorities with respect to homeland security: border security, critical infrastructure protection, and intelligence analysis.[10]

C. Effectiveness: Recommended Definition

I define effectiveness as: "Effective counterterrorism causes the terrorist infrastructure to suffer serious damage—including damage to finances, intelligence, resources, or personnel—thereby preventing a particular, planned attack from going

---

[4] Guiora, *Global Perspectives*, *supra* note 1, at 139.
[5] Id.
[6] Id. at 140.
[7] Id.
[8] Id.
[9] Id. at 21.
[10] Paul Light & James Lindsay, Council on Foreign Relations, Views of Homeland Security (2002); *http://www.cfr.org/publication/6395/views__of__homeland__security.html.*

forth and/or postponing or impacting plans for future attacks while minimizing collateral damage, exercising fiscal responsibility, and preserving civil liberties."

This definition incorporates the following premises: (1) terrorism is not "100 percent preventable"; (2) counterterrorism must have a short-term (tactical) as well as a long-term (strategic) component; and (3) counterterrorism must be conducted while balancing competing interests of human life, financial cost, and civil liberty.

1. Terrorism Is Not 100 Percent Preventable.

Security analysts are wont to frame recommended counterterrorism measures in an effectiveness paradigm that demands "fool proof" safeguards. However, it must be clearly stated that terrorism is not 100 percent preventable. A successful terrorist attack does not mean existing counterterrorism measures are ineffective. The inverse is also true: the absence of terrorist attacks does not necessarily indicate existing counterterrorism measures are effective.

2. Counterterrorism Must Have a Short-Term as Well as a Long-Term Perspective.

If a counterterrorism strategy only targets short-term threats, it will likely overlook other (long-term) real threats. It is important to note that terrorist organizations define effectiveness through the prism of "long-term" strategic considerations.[11] To understand the terrorist mind-set, it is necessary to appreciate the determination, resilience, and single-mindedness with which terrorists work. Terrorists are willing to engage in a "war of attrition" with enormous personal hardship for the individual and his immediate family to achieve specific goals. Counterterrorism, both strategically and tactically, must be premised on this reality. Engaging in a never-ending cycle of violence is one means by which terrorist organizations signal to various audiences (the general public, followers, and the relevant government) their commitment to the cause.

3. Counterterrorism Must Be Conducted in Balance With Competing Interests of Human Life, Financial Cost, and Civil Liberty.

"Finding a balance between national security and the rights of individuals is the most significant issue faced by liberal democratic nations developing a counterterrorism strategy. Without a balance between these two tensions, democratic societies lose the very ethos for which they fight. As Benjamin Franklin once said, 'those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety.'[12] Indeed, it is imperative for democracies to avoid infringing on political freedoms and civil liberties. Yet, a government's ultimate responsibility is protecting its citizens. This struggle to balance competing interests may be the most fundamental dilemma confronting democracies today."[13]

IV. ACCOUNTABILITY

A. Recommended Definition

I define accountability as: "Accountability: Articulating in a transparent manner the effectiveness or ineffectiveness of a particular counterterrorism measure or strategy to one's superiors who have the power to rectify or discontinue measures."

The 9/11 Commission Report emphasizes in detail the need for standards of accountability in developing and implementing counterterrorism measures. The 9/11 Commission correctly stated that "effective public policies . . . need concrete objectives."[14] That is, in the struggle against terrorism, "agencies need to be able to measure success."[15]

Without standards for accountability, Congress unwittingly creates an unfettered executive. "An unfettered executive, unrestrained by courts and legislatures, is detrimental to liberal democracies attempting to balance national security and individual rights."[16] Furthermore, when neither the legislature nor the judiciary rein the executive in, the former is bound to make mistakes whereby more-effective alternative means are often overlooked. Particularly in the murkiness and uncertainty of drawn-out amorphous operational counterterrorism, the executive must know there are clear guidelines determining accountability. Counterterrorism requires both strict separation of powers and checks and balances.

---

[11] Guiora, *Global Perspectives*, *supra* note 1, at 14.

[12] Benjamin Franklin, Pennsylvania Assembly: Reply to the Governor, Nov. 11, 1755. The Papers of Benjamin Franklin, Leonard W. Labaree ed., vol. 6, p. 242 (1963).

[13] Guiora, *Global Perspectives*, *supra* note 1, at 19.

[14] "What to Do? A Global Strategy?", The 9/11 Commission Report (364).

[15] Id.

[16] Guiora, *Global Perspectives*, *supra* note 1, at 75.

V. RESILIENCY

A. Recommended Definition

I define resiliency as: "Resiliency: the capacity to prepare for, withstand, and endure terrorist attacks in order to assure continuity."

B. Establishing Partnerships

Post-9/11 and in the wake of Hurricane Katrina, one of the most important lessons learned by the United States was the dire consequences of the break-down in communications between governmental agencies amongst themselves and with the private sector. Ineffective communication directly led to hesitation, confusion, lost time, and ultimately lost property and lives. Effective cooperation and coordination between governmental agencies within, and among, the Federal, State, and local governments is essential to achieving a successful homeland security strategy. However, in order to realize resiliency, it is paramount that there is clear cooperation and coordination between the public sector and the private sector.

The importance of the public-private initiative is outlined in the Department of Homeland Security's recent National Response Framework ("NRF"), which defines the roles and responsibilities of the government (Federal, State, local, and tribal) and the private sector (private business and/or NGO). As articulated in the NRF, "Government agencies are responsible for protecting the lives and property of their citizens and promoting their well-being. However, the government does not, and cannot, work alone. In many facets of an incident, the government works with the private-sector groups as partners in emergency management."[17]

The NRF outlines five critical roles played by the private sector during both disasters and terror attacks. First, privately owned critical infrastructures such as transportation, private utilities, financial institutions, and hospitals play a significant role in economic recovery from disaster and terror incidents.[18] Second, "owners and operators of certain regulated facilities or hazardous operation may be legally responsible for preparing for and preventing incidents from occurring and responding to an incident once it occurs."[19] Third, private business "provide response resources during an incident—including specialized teams, essential service providers, equipment, and advanced technologies."[20] Fourth, private entities "may serve as partners in local and State emergency preparedness and response organizations and activities."[21] Fifth, private entities play an important role "as the key element of the national economy, private-sector resilience and continuity of operations planning, as well as recovery and restoration from an actual incident, represent essential homeland security activities."[22]

A necessary component to establishing a resilient homeland, therefore, is a viable public-private sector partnership that is based on: (1) Defined roles and responsibilities; (2) articulating a coordinated prevention-response plan; and, (3) repeated training or simulation exercises using the prevention-response plan against realistic disaster/terror scenarios.

1. Defined Roles and Responsibilities

In forging lasting partnerships between the public and private sectors, the private sector (private business and/or NGO) must define its role and responsibilities relative to the public sector on all government levels (local, State, and Federal). Agencies such as the New York Red Cross must work alongside FEMA and the NYPD in an effort to respond to a disaster or another terrorist attack. These partnerships must be created using individual liaisons to private and public entities predicated on clearly defined roles and responsibilities and open and frequent communication.

2. Articulating a Plan

The private sector must work closely with the public sector to articulate, develop and implement a disaster/terror prevention prevention/response plan. Such a plan must implement the clearly defined roles and responsibilities outlined above. Additionally, a proposed plan need take into account multiple scenarios addressing prevention and response thereby ensuring that different entities are seeking to achieve

---

[17] National Response Framework (hereinafter "NRF"), Department of Homeland Security, (January 2008) at 18, available at *http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf*.

[18] Id.

[19] Id. at 19 (this legal responsibility is exemplified by the owners and operators of nuclear power plants obligated under Federal regulations to maintain emergency plans and conduct training for a response to such an incident).

[20] Id.

[21] Id.

[22] Id.

similar goals. The plan will ensure that different organizations see the "big picture" and know their particular responsibilities within the larger framework.

3. Training and Simulation

Fundamental to creating and maintaining the public-private sector initiative is consistent training and simulation exercises. Members of the private and public sector should conduct scenario-based, simulation exercises (together and separately) with respect to the proposed plan. These exercises must include realistic disaster scenarios subject to real-life time constraints testing the effectiveness with which both the private and public sectors respond to complicated and complex attacks and disasters. Such training and simulation will ensure that the public and private sectors understand—both theoretically and practically—the vital necessity of cooperation and coordination. Such scenario-based simulation exercises—in highlighting existing institutionalized and systemic weaknesses—most effectively facilitate the development of an effective homeland security strategy.

C. Goals for Partnerships

Public-private partnerships, if properly developed and implemented, are the key to economic recovery. Such a partnership—in the aftermath of a disaster or attack—facilitates the resilience of critical infrastructure including transportation, utilities, financial institutions, and hospital care. By strategically strengthening security, sharing intelligence, and creating plans for post-attack procedures (including evacuation plans, transportation plans, identifying places of refuge, and providing basic supplies to aid first-responders) such partnerships become the key to a secure and resilient homeland.

1. Prevention & Resiliency Through Intelligence Sharing

The Department of Homeland Security (DHS) has provided excellent guidance regarding how to frame intelligence sharing between the public and private sectors. The importance of information before, during and after a disaster or attack is vital to resilience. Information sharing is, perhaps, the single most important aspect of successful resilience. Information sharing requires government agencies (Federal, State and local) to share information both amongst themselves and with the private sector. Furthermore, it requires that the private sector—subject to existing legal and constitutional limits—share information with the public sector. Successful information sharing requires cooperation and coordination both internally (within sectors) and cross sectors (between public-private entities).

The process must be institutionalized, requiring a fundamental re-articulation of homeland security strategy. While various public sector agencies are historically hesitant (predicated on policy, culture and legal restraints) to share information with other agencies—much less the private sector—the lessons of 9/11 and Katrina speak for themselves. Resilience in the aftermath of either disaster or attack requires Federal, State and local government agencies to understand that information sharing is vital to the Nation's homeland security. That information sharing process must include the private sector. Otherwise, the mistakes of yesterday will inevitably re-occur.

To that end, DHS recommends that public and private agencies:[23]

- Prepare memorandums of understanding and formal coordination agreements describing mechanisms for exchanging information regarding vulnerabilities and risks;
- Use community policing initiatives, strategies, and tactics to identify suspicious activities related to terrorism;
- Establish a regional prevention information command center; and
- Coordinate the flow of information regarding infrastructure.

In addition, the National Infrastructure Advisory Council published a report on private and public sector intelligence coordination and made the following recommendations:[24]

- *1. Senior Executive Information Sharing*.—Develop a voluntary executive-level information sharing process between critical infrastructure CEOs and senior intelligence officers. Begin with a pilot program of volunteer chief executives of one sector, with the goal of expanding to all sectors.

---

[23] *Engaging the Private Sector to Promote Homeland Security:* Law Enforcement-Private Security Partnerships: New Realities Law Enforcement in the Post–9/11 Era, U.S. Department of Justice Bureau of Justice Assistance, September 2005, at vi, available at *http://www.ncjrs.gov/pdffiles1/bja/210678.pdf*.

[24] National Infrastructure Advisory Council Public Private Sector Intelligence Coordination Final Report and Recommendations by the Council, July 11, 2006, available at *http://www.dhs.gov/xlibrary/assets/niac/niac_icwgreport_july06.pdf*.

- *2. Best Practices for the Private Sector*.—The U.S. Attorney General should publish a best practices guide for private sector employers to avoid being in conflict with the law. This guide should clarify legal issues surrounding the apparent conflict between privacy laws and counter terrorism laws involving employees. Moreover, it should clarify the limits of private sector cooperation with the IC.
- *3. Existing Mechanisms*.—Leverage existing information-sharing mechanisms as clearinghouses for information to and from critical infrastructure owners and operators. This takes advantage of the realities that exist sector by sector.
- *4. National-Level Fusion Capability*.—Establish or modify existing government entities to enable national- and State-level intelligence and information fusion capability focused on Critical Infrastructure Protection (CIP).
- *5. Staffing*.—Create additional—Sector Specialist positions at the executive and operational levels as applicable in the IC. These specialists should be civil servants who have the ability to develop a deep understanding of their private sector partners.
- *6. Training*.—Develop an ongoing training and career development program for sector specialists within intelligence agencies.
- *7. RFI Process*.—Develop a formal, and objectively manageable, homeland security intelligence and information requirements process, including requests for information (RFIs). This should include specific, bi-directional processes tailored sector by sector.
- *8. Standardize SBU Markings and Restrictions*.—The Federal Government should rationalize and standardize the use of SBU markings, especially "For Official Use Only."

2. Providing Critical Infrastructure—Continuity Planning

In order to play their essential role of re-establishing critical infrastructure after an attack, private entities must have continuity plans. These plans must take into account the known threats,[25] which are only "known" through intelligence sharing between the public and private sectors, as discussed above. These plans must also take into account the components essential to re-establishing the service that the particular entity provides. These plans must provide details regarding how the particular entity will promptly resume service, which may differ depending on the form of attack. In addition, the plan must articulate how the entity will communicate with the public sector after an attack and what, if any, assistance the entity will surely or likely need from the public sector in order to promptly re-establish service.

The United Kingdom has enacted legislation requiring contingency plans. That legislation, the Civil Contingencies Act, requires certain private entities to "maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable."[26] Specifically, entities are required to makes arrangements to warn and inform the public, handle emergencies, and make provisions to ensure that the entity's ordinary functions can be continued to the extent necessary.[27] To ensure effectiveness, the legislation also requires entities enact training programs for those directly involved in the execution of the continuity plan.[28] To assist the entities, the legislation requires local authorities to provide advice and assistance to businesses and voluntary organizations in relation to business continuity.[29]

New York City has taken a first step at creating similar legislation. New York City's Local Law 26 (2004) amended the existing administrative code in relation to building safety in the city.[30] In particular, this new law requires owners of big buildings, in coordination with the FDNY, to prepare detailed plans, train staff members and conduct full evacuation drills of the entire building every 3 years.[31] While evacuation plans are an essential first component of a contingency plan, they are not enough to establish even the hope for a resilient homeland.

The following is a list of suggested measures that would most effectively facilitate resilience in the aftermath of a disaster or attack:

- Educate the private sector regarding the importance of continuity plans;

---

[25] See Appendix A for a classification of "known" risks. For this discussion, all risks, including the imminent, foreseeable, long-range, and uncertain are considered "known" threats.

[26] UK Resilience: Business Continuity, May 7, 2008, available at *http://www.ukresilience.info/preparedness/businesscontinuity.aspx* (last visited May 10, 2008).

[27] Id.

[28] Id.

[29] Id.

[30] See Jim Dwyer. Evacuation Plans Due for High Rises in New York City, New York Times (August 5, 2004), available at *http://query.nytimes.com/gst/fullpage.html?res=9B03E2DA153CF936A3575BC0A9629C8B63* (last visited April 11, 2008).

[31] Id.

- Educate the public about the importance of continuity plans for the private sector;
- Offer expertise in the form of training to enable private entities to create continuity plans;
  - Require oversight in exchange for the expertise;
- Pass legislation that puts the private sector on notice regarding the importance of continuity plans;
- Encourage States to pass legislation mandating continuity plans, to the extent a State has such power;
- Offer financial incentives, possibly tax incentives, to entities that establish continuity plans and continue updating those plans.

VI. CONCLUSION

Not only the public sector, but also the private must contemplate resiliency must before a terrorist attack occurs. Sophisticated planning—based on scenario-based simulation exercises—will significantly contribute to creating a resilient homeland. The first step to making the homeland resilient to a terrorist attack requires defining terrorism, counterterrorism, effective counterterrorism and accountability.

Terrorism poses a threat that cannot be eliminated. Nor can the government truthfully claim that it will prevent all terrorist attacks. While measures can be implemented to prevent attacks civil, democratic societies must recognize that at some terrorist attacks will succeed. In an effort to minimize both the chances of a particular attack and the consequences of a successful attack it is necessary to create public-private sector partnerships. Such partnerships must be based upon communication, mutual (subject to legal and constitutional limits) information sharing and defined roles. Such partnerships will facilitate the development of continuity plans seeking to ensure the restoration of infrastructure vital to the Nation. Resilience depends on such cooperation; information sharing between and among the public and private sectors is the essence of that relationship.

Ms. HARMAN. Thank you very much, Mr. Guiora.

Mr. Eddy.

STATEMENT OF R.P. EDDY, EXECUTIVE DIRECTOR, CENTER FOR POLICING TERRORISM, THE MANHATTAN INSTITUTE FOR POLICY RESEARCH

Mr. EDDY. Madam Chair, members of the committee, thank you very much for the opportunity to be speaking here.

I fully agree with some of the statements made by the Chair that we learned many of the wrong lessons after 9/11. That morning, we all looked to the skies for the Air Force F–16s; we looked to Washington to protect us. The main thrust of Federal efforts since then certainly has been deployed overseas, funding the Intelligence Community and working with the FBI. But State and local police, when considered, were considered as first responders. They were funded to be, in effect, the clean-up crew to help remediate our communities after the terrorists launched a successful attack.

This focus in funding on Federal forces and not local police, on international intelligence and not internal awareness, is wise only if our enemies are outside our borders and we can stop them before they get in. But the reality is much more complicated and much more dangerous, as this committee is well aware. Our next 9/11 is as likely to be from terrorists inside our borders as it is from terrorists outside our borders.

Terrorism everywhere is increasingly homegrown. This committee has done much good work on that. Nearly every major attack since 9/11 around the world had a very strong homegrown component. There have been, as you know, well over 12 U.S. locales in which terrorist activities have been disrupted in the last 5 years.

In each of these incidents, the perpetrators were not infiltrators. They were residents, they were citizens, they were the neighbors next door. They had all the necessary IDs and all the excuses. They didn't have to blend in; they already were in.

Soon after 9/11, the NYPD realized they had to tackle prevention on their own. They asked me and the Manhattan Institute to build them a think tank to support them as they ramped up their counterterrorism operations. NYPD wasn't getting the Federal support necessary to detect and defeat terrorism then, and most police forces are not getting the information now.

Since our start with the NYPD, the CPT, the Center for Policing Terrorism, Manhattan Institute, has expanded to become involved with other agencies, such as the LAPD and the New Jersey State Police. Our focus is to advocate to and enable core police departments to become first preventers and to adapt the practice of intelligence-led policing.

I humbly suggest three categories of solution to the topic of today's hearing, in which you can build resiliency and improve our overall counterterrorism posture, while also strengthening capacity of State and local police against all hazards, the entire range of challenges that they face.

First, support national counterterrorism academies. The CPT is proud to have partnered with LAPD, LA Sheriff's Department and others to launch the National Counterterrorism Academy just a few months ago. We already have more than 60 students from over 27 public agencies and private-sector companies throughout California and Nevada.

The topics of instruction include precisely what I have described before—homegrown radicalization, method of interdicting terrorist finance, case studies of significant attacks—all of these taught by world-class instructors. Over the next year, the academy will expand its offerings, will seek additional funding to grow a bricks-and-mortar location, a virtual online academy, a digital library, and mobile training teams. Under LAPD's guidance and Chief Bratton's leadership, a small staff of professionals will develop the curricula, manage operations, and outsource the instruction to the best and the brightest.

To fully fund 3 years of this academy, teaching hundreds of police and private leaders in the "train the trainers" model, injecting intelligence-led policing and first preventers practices into hundreds of departments will cost less than $4 million. DHS should fund NCTA and its East Coast counterpart in 2009.

I skipped that part; I am sorry. We are building a sister academy in New Jersey, and we are going to build a regional structure in between.

No. 2 suggestion is to support intelligence-led policing in the Foreign Liaison Officer Program. Looking at the intelligence picture throughout the homegrown threat, we need to shift our paradigm from believing that we have to simply solve for how to get intelligence and training from DHS or from the Federal family to State and locals, and instead we have to recognize that most of the intelligence relevant to State and locals is simply not being collected federally. There are not huge buckets of magic information and in-

telligence sitting in Federal SCIFs that will solve all the problems of big cities.

In fact, there are three things we have to understand about this: First, a vast array of useful intelligence for counterterrorism and other crimes is already in our communities. Generally, homegrown terrorists live in the communities where they plot and are in the communities in which they are going to launch their attacks. Even most foreign-born plots have a very strong local dimension. Recall that two of the 9/11 hijackers were pulled over and released before the hijackings for speeding.

No. 2, police are simply the best entity suited to collect this intelligence. Our hugely decentralized police force, over 17,000 police departments, ensures that police come from the communities, they have community access, and generally the community trusts them. Local entities also have broader legal allowances to investigate crimes and assess the risks in their communities. Then, of course, there are the numbers. We know there are 730,000 police in this Nation but perhaps less than 2,500 FBI agents focusing on domestic counterterrorism. No Federal entity has the exposure, the tools and the breadth to collect local information.

Third, while police are best suited to collect this critical intelligence to prevent terrorism, they simply are not collecting it. That is to say, much of what we tend to think about intelligence-sharing, which is that we have to grease the skids downhill from the Federal Government to locals, isn't entirely correct. We also have to figure out how to enable the locals to collect on their own and how that information can work laterally.

Intelligence-led policing is exactly that. At the strategic level, DHS should teach intelligence-led policing and push that out at the user level. They can do that through the fusion centers.

Just as James Q. Wilson and George——

Ms. HARMAN. Could you summarize, please, Mr. Eddy?

Mr. EDDY. I will.

My final summary, I guess, based on resiliency—a resilient homeland is based on numerous layers of prevention and response, but it is important to realize we cannot begin to consider true resiliency until we know that the 730,000 local police are recruited to the cause.

I also suggest that the Federal Government consider implementing the LA Police Department's Archangel program across the Nation to allow to you have a much more comprehensive and clear ability to assess vulnerabilities across the country in a clear fashion.

Thank you very much.

[The statement of Mr. Eddy follows:]

PREPARED STATEMENT OF R.P. EDDY

MAY 15, 2008

Chairman, members of the committee, my sincere thanks for inviting me to speak with you today.

Our Federal Government learned some of the wrong lessons from 9/11.

That morning we all looked to the skies for the Air Force F–16's and we looked to Washington to protect us. The main thrust of Federal effort since then answered that call: troops were deployed overseas, funding for the CIA and NSA was greatly increased, and the FBI has begun to focus more on counterterrorism. But State and

local police, when considered, were considered only as the "first responders" of terrorism. They were funded to be—in effect—the clean-up crew to remediate our communities after the terrorists launched a successful attack.

This focus and funding—on Federal forces and not local police, on international intelligence and not internal awareness—is wise only if our enemies are outside our borders and we can stop them before they get in. But our reality is much more complicated, and much more dangerous. Our next 9/11 is as likely to be from terrorists already within our borders as is it to be from terrorists overseas who plot to penetrate our Nation.

Terrorism everywhere is increasingly homegrown. The trend line is unmistakable: it runs from the 2002 Bali nightclub bombings, to the 2003 attacks in Casablanca and Istanbul, through the 2005 subway bombings in London and to the foiled plans to bomb jumbo-jets flying from London to the United States in 2006. But we need not look only overseas for examples of the local threat. Consider this partial list of U.S. locales in which terrorist activities have been disrupted in the last 5 years: Lackawanna, NY; Bly, OR; Lodi, CA; Torrance, CA; Iredell County, NC; Miami, FL; Toledo, OH; and Syracuse, NY. In each of these incidents, and in dozens of other smaller ones, the perpetrators were not infiltrators. They were residents, citizens, neighbors-next-door. They had all the necessary IDs and excuses. They didn't have to blend in; they were in.

Of course we do still face a threat from international terrorists seeking to hit us at home, a la 9/11. In these instances as well, State and local law enforcement are the critical line of defense. Recall that two of the 9/11 hijackers were pulled over by local police on routine traffic stops and released. These terrorists lived in our towns, ate at our restaurants, and studied at our schools for many months. It is much more likely that the Nation's 730,000 local police officers—with years on the beat and connections with all aspects of the community—and not the perhaps 2,500 FBI agents dedicated to domestic counterterrorism, or other Federal forces, will have the situational awareness to identify and locate terrorists already in our midst.

Soon after 9/11, the NYPD realized they had to tackle prevention on their own. They asked me and the Manhattan Institute to build them a small think-tank to support them as they ramped up their counterterrorism capabilities. NYPD wasn't getting the Federal support necessary to detect and defeat terrorists then, and most police forces still aren't now.

Since our start with NYPD, The Center for Policing Terrorism at the Manhattan Institute for Policy Research (CPT) has expanded to become involved with other agencies such as the Los Angeles Police Department and the New Jersey State Police. CPT's focus is to advocate to and enable core police departments to become "first preventers" and to adopt the practice of "intelligence led policing."

CPT is supported entirely by private philanthropy. Our donors, who span the political spectrum, have enabled CPT to fill gaps in public funding, gaps that I believe should not exist.

I hope to bring to you today an invested understanding of what needs to be done to prevent terrorism in our Nation. By invested I mean: my donors, my colleagues, and I have put our money where our collective mouth is. I am not an academic promoting theories or a contractor looking for support. I have the honor of representing a small group of dedicated citizens who have sought Federal leadership and Federal funding, and when we found both lacking we went and created the solutions on our own, with our own dollars.

I humbly suggest three categories of solution—all with minimal budget impact—in which Congress can build resiliency and improve our overall counterterrorism posture, while also strengthening the capacity of our State and local police against the entire range of hazards.

1. SUPPORT NATIONAL COUNTERTERRORISM ACADEMIES

CPT is proud to have partnered with LAPD to begin building the National Counter-Terrorism Academy (NCTA), funded by the Ahmanson Foundation and the State of California. NCTA already has 60 students from more than 27 public agencies and private sector companies throughout the States of California and Nevada. Topics of instruction include homegrown radicalization, methods for interdicting terrorism finance and case studies of significant terrorism plots presented by the investigators themselves.[1]

Over the next year, the Academy will expand its course offerings, seek additional funding and grow to eventually include four components: a bricks-and-mortar loca-

[1] Manhattan Institute, *Manhattan Institute and LAPD Unveil Counter-Terrorism Academy for State and Local Cops,* Press Release, March 10, 2008.

tion in Los Angeles; a virtual, or online, academy; a digital library; and mobile academic teams. Under the LAPD's guidance and Chief Bratton's leadership, a small staff of professionals will develop curricula, manage operations and outsource the instruction to the best and brightest.

The Academy will augment and serve as a focal point for existing Federal training programs and strengthen the intellectual body of homeland security knowledge by adding the critical perspective of local agencies. The training will be tailored to the needs of the up-and-coming leaders in State and local agencies and their counterparts in the public safety and private security fields.

NCTA does not compete with existing institutions like FLETC. Rather it offers a first-rate, dedicated option for police leaders to become evangelists and trainers of first prevention and intelligence-led policing doctrine.

In just a few months of operation, NCTA has already proven to be such a success that we are eager to expand the model across the Nation. CPT is already underway in discussions to partner with the New Jersey State Police to build a sister academy on the East Coast. We are happy to note that the Bureau of Justice Assistance was heavily represented in these discussions. This academy will scale from the LA academy and draw on the same virtual library, training teams, and other key assets of the NCTA.

Though the NCTA academy is teaching nearly 30 public agencies the skills they need to prevent and respond to terrorism, as well as many other hazards, proposals for modest levels of Federal funding have not been accepted. To fully fund 3 full years of NCTA operation, teaching hundreds of police and private leaders in a train-the-trainers model, injecting intelligence-led policing and first preventers practices into hundreds of departments, and establishing the premier online library of written materials and videotaped lectures available to police across the nations will cost less than $4,000,000.

DHS should fund NCTA and its East Coast counterpart in 2009.

2. SUPPORT INTELLIGENCE-LED POLICING AND FOREIGN LIAISON OFFICERS

Looking at the intelligence picture through the reality of the homegrown threat, we need to shift our paradigm from believing we have to solve for simply how to get intel and training from DHS (or other Federal entities) to State and locals, and instead recognize most of the intelligence relevant to State and locals simply is not being collected federally. There are not huge buckets full of magic intelligence sitting in Federal SCIFS that will solve all the puzzles of big city police.

It has become a well-worn criticism that there is very little tasking in Federal collection toward things useful to State and locals, and that the sharing of what does exist is pitiful. While Federal organization, tasking and sharing certainly needs to be fixed, we also must learn three simple things:

- *1. A vast array of useful intelligence for CT and many other crimes is in our communities.* Generally homegrown threats will only be detected in the communities where they are plotted and to be launched, but even most foreign-borne plots will demand that terrorists spend real time attempting to integrate into the fabric of our communities. This is intelligence that will come from close connections with the communities and the establishment of situational awareness in the way only our hometown police can do.
- *2. Police are simply the best entity suited to collect this intelligence.* Our hugely decentralize police system (the United States has over 17,000 police departments) ensures police come from the communities, they have the community access and generally the community trust to find this information. Local entities also generally have broader legal allowances to investigate crimes and assess risk in their communities. Then there are the numbers: there are, of course, 730,000 police in this nation but perhaps less than 2,500 FBI agents focusing on domestic counterterrorism.[2] No Federal entity has the exposure, the insight, the tools, let alone the breadth to collect local threat information.
- *3. But, while Police are best suited to collect this critical intelligence, most simply are not collecting.*

That is to say, we miss much of the need (versus the homegrown terror threat at least) when we think we simply need to grease the skids of information downhill. It is as critical for DHS to help police collect the intelligence that exists in their communities as it is for DHS to share intelligence with police.

---

[2] Federal Law Enforcement Statistics, U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics. Available at *http://www.ojp.usdoj.gov/bjs/lawenf.htm* [accessed 5/9/2008].

After the success of community-led policing and COMPSTAT, the next major innovation in policing is upon us. Intelligence-led policing is the ultimate addition of strategy to counterterrorism and fighting crime. It is conceptually simple: police departments should create intelligence opportunities and use the outcomes to direct their limited resources. A tiny number of U.S. police departments have intelligence capacities; the vast majority does not. Though we need to be mindful of the past abuses by some police departments in the 1960's, today's police departments are vastly different organizations, and intelligence gathering must be integrated into police work, and not just for counterterrorism.

ILP can be applied to virtually every public safety challenge police face. Having a firm understanding of a challenge, in real time, improves decisionmaking and produces better results. Resiliency begins with the way we think about problems and deal with mental adversity. Enhancing local intelligence capabilities will allow us to achieve exactly that.

Fusion centers hold tremendous promise. Though they exist in every State, many lack real strategy on how to share intelligence across, up and down. Fusion centers also offer a perfect vessel to push the necessity and tactics of Intelligence-led policing to their client police departments, but again many are not resourced to do so.

At the strategic level DHS should begin to preach the value of intelligence-led policing, and at the user level, institute a pilot plan via the fusion centers to teach intelligence-led policing to local police departments.

Intelligence-led policing and First Preventers doctrine transforms police departments into proactive counterterrorism agencies. Not only will they continue to thwart dozens of terrorist incidents, this posture will deter untold potential homegrown terrorists as it will create a hostile environment for violent extremists. Much as the Broken Windows theory created by George Kelling and James Q. Wilson and implemented by Chief Bratton revolutionized crime fighting, so too will these tools revolutionize the Nation's fight against terrorists.

Although controversial for the FBI and State, police should take intelligence collection to the international level. NYPD's international liaison program is a well-known success. The NYPD officers stationed with foreign counterparts in major overseas metropolitan police departments have built NYPD's knowledge networks and best practices[3] immensely. These relationships inform NYPD's thinking not only on counterterrorism, but also on fighting crime and other hazards.

We were very pleased to see this committee propose the concept of a Foreign Liaison Officers Against Terrorism (FLOAT) Program as part of the LEAPS legislation. Since 2003, we have proposed a program much like FLOAT, in which 5–10 major city police departments would each assign one officer overseas to liaison relationships with foreign police departments. Ideally each city would send an experienced officer to an area they know well. LA could send an officer of Indonesian heritage to Jakarta, Miami could send a Colombian-American to Bogota, Detroit could send an Arab-American to Cairo, etc. These officers would embed with the local police to collect information on counterterrorism.

The regular reporting from the liaison officers would then be pooled to the intelligence apparatus of all participating police departments, and others.

I won't get into a detailed defense here of why police need their own international liaison relationships, but suffice it to say, the current reporting back from FBI and State generally does not make it to police. When it does, it is obvious these departments are curious about very different lessons and learnings than the locals. Instead of being seen as adversarial, Federal agencies should see the police liaison presence as a complement to Federal activities which can also provide real-time threat reporting to their local agencies.[4]

As this initiative has not made progress at the Federal level, CPT leadership is endeavoring to launch a FLOAT program funded by the local police and donor dollars. Presuming the police departments will continue to pay the salary and benefits of the officers, we estimate the cost for housing and travel and other incidentals to be less than $100,000 per year per officer. We will also arrange to create and house the fusion hub that will task, collect and distribute the liaison reports. NCTA, discussed above, is an obvious home to serve as the hub to disseminate FLOAT reports throughout the police community.

Again, there is an obvious Federal role here and we urge the committee to fund international police liaisons.

---

[3] Kelling, George L., and Bratton, William J. *Policing Terrorism.* Civic Bulletin, No. 43, September 2006, page 6.

[4] LEAP Proposal, page 10.

3. SUPPORT STRATEGIC RESOURCE ALLOCATION

Local police agencies are the most knowledgeable resource when it comes to their own critical assets. While many States and localities have done impressive work understanding and cataloguing critical assets and key resources in their jurisdictions, there is a stark lack of uniformity in terms, methodologies and fundamental approaches. We believe that this ultimately hinders the ability of national level decisionmakers to make risk-based resource allocation decisions, since there is not a baseline for comparing assets across jurisdictions.

We believe that a common approach for evaluating critical infrastructure should be mandated on State and local agencies. There is good news here. The LAPD, in partnership with DHS has developed Operation Archangel, a robust methodology and information technology system for evaluating and protecting critical infrastructure. Archangel was created to utilize cooperation and coordination across departments as well as public and private sectors to facilitate the strategic application and management of information and resources to prevent, deter, mitigate, and respond to an attack.[5] It is well thought-out and vetted and could be easily and cheaply incorporated around the country.

Resiliency Comes From First Preventers and Intelligence-led Policing

The focus of your hearing today, a resilient homeland—cities and towns that can return to stability after a disaster—relies on numerous layers of prevention and response preparation. But it is important to realize that we cannot begin to consider true resiliency until we know the 730,000 local police are recruited to the cause.

When CPT goes to police leadership across the nations to help them build prevention capacities, we find many police departments to be nearly tabula rasa when it comes to counterterrorism. This is not to say they are not eager to be involved with CT, rather most police departments—particularly in major cities—are already very overburdened and under-resourced. If they don't see a clear and present terrorism danger to their city, it is hard to convince elected officials or their staff to shift their limited resources from fighting crime to counterterrorism.

But we have had success and can be successful elsewhere for two reasons:

1. Police leaders quickly realize that the "First Preventers" curricula and intelligence-led policing helps police and their local partners not just with CT, but against "all hazards," and
2. These concepts resonate with the highly successful proactive policing models such as COMPSTAT of the 1990's.

Most agree the Londoners were resilient to the 7/7 subway bombings because of the long English history with terrorism and even cultural memories of WWII. We should not presume to think we can change American mindsets, but a process of empowerment and knowledge-sharing is, of course, key to reducing panic in the event of an attack.

Local police departments are not just the crux of public safety in over 17,000 communities, but they are also the public servants most integrated with the populace. By offering police insights and the ability to proactively understand and pre-empt terrorism, we are in fact injecting this confidence into our communities.

I would counsel that while we work hard to adopt the goals of resiliency into nearly everything related to counterterrorism, we also realize that sometimes resiliency will not be an option. Some attack scenarios, including some we judge as highly likely in the medium term, are so horrific that the only real strategic alternative is prevention.

I close by noting that I propose these initiatives not as a theoretician, but as a representative of a group of citizens that have since soon after 9/11 found aspects of Federal leadership in domestic counterterrorism lacking so have been funding and enacting, on our own, solutions to support our best hope for a secure homeland: our local police.

APPENDIX.—LOS ANGELES POLICE DEPARTMENT NEWS RELEASE

LAPD STARTS ITS NATIONAL COUNTER-TERRORISM ACADEMY

March 10, 2008, Los Angeles, California.

Mayor Antonio Villaraigosa and Police Chief William Bratton jointly announced the model for what is expected become a National Counter-Terrorism Academy (NCTA) for State and local law enforcement—the first of its kind in the country created by local law enforcement and its private partners.

[5] Los Angeles Police Department, *Operation Archangel*. *http://www.lapdonline.org/emergency_services_division/content_basic_view/33044* [accessed 4/7/2008].

"Police officers are out in the communities every day, gathering critical information and fighting crime. With the proper training, we can apply the skills we already have to the fight against terrorism as well," said Chief Bratton. "This academy will offer standardized, counter-terrorism training that teaches us how to apply the crime-fighting and information-gathering strengths we already have to the issue of terrorism."

The pilot program for the Academy, which starts today and runs through July 30, will bring world-class counter-terrorism training to nearly 70 students from more than 27 public agencies and private sector companies throughout the State of California and Nevada. Topics of instruction include homegrown radicalization, methods for interdicting terrorism finance and case studies of significant terrorism plots presented by the investigators themselves.

The pilot program is a public-private partnership between the LAPD and the Center for Policing Terrorism at the Manhattan Institute, a think tank with a long history of confronting the most challenging public policy issues.

"The Manhattan Institute welcomes the opportunity to contribute to a curriculum that will expose law enforcement and other public safety professionals to imaginative thinking about the links between common crime and political violence, and to do so without losing sight of constitutional rights and civil liberties," said Howard Husock, the institute's vice president for policy research.

The pilot program was funded primarily by the Ahmanson Foundation. The State of California has provided additional funding for the further development of the academy.

Over the next year, the Academy will expand its course offerings, seek additional funding and grow to eventually include four components: a bricks-and-mortar location in Los Angeles; a virtual, or online, academy; a digital library; and mobile academic teams. Under the LAPD's guidance and Chief Bratton's leadership, a small staff of professionals will develop curricula, manage operations and outsource the instruction to the best and brightest.

The Academy will augment and serve as a focal point for existing Federal training programs and strengthen the intellectual body of homeland security knowledge by adding the critical perspective of local agencies. The training will be tailored to the needs of the up and coming leaders in State and local agencies and their counterparts in the public safety and private security fields.

Background

In the wake of 9/11, America's roughly 700,000 State, local and tribal law enforcers stand to play a critical role in homeland security as "First Preventers" of terrorism and other crimes. Despite this potential, there is no training academy where officers can receive basic homeland security education based on a standardized curriculum specifically tailored to their needs.

The Los Angeles Police Department, under the leadership of Chief Bratton, proposes the creation of a national academy in Los Angeles that will fill that void while serving as a vehicle to promote and teach the philosophy of Intelligence-Led Policing—a policing model in which operations are guided by intelligence gathering and analysis rather than the other way around.

If you have any questions, please contact Media Relations Section.

Ms. HARMAN. Thank you very much.

I think all of the testimony was right on point and excellent.

We have a large member turnout, so I am going to be sure that my own questions are limited strictly, including the answers, to 5 minutes.

I have two questions. I will ask them both at once and ask you all to comment, or whoever would like to.

First, Mr. Guiora was trying to define the term "resilience," and he included things, at least the way I wrote them down, like preparation, participation, managing expectations.

I want to ask—because, in your case specifically, you spent many years at the IDF in Israel—whether there isn't also a cultural or experiential dimension to this. Israelis have been the test bed for terrorism for 60 years or maybe, depending on which bible you read, 60 millennia.

But, at any rate, after terrorist attacks, within a matter of hours, the attack site is cleaned up, the yellow police tape is gone, and people go back to business. That is a hugely impressive act. It doesn't happen in America. So I just want to ask if there is another dimension to this.

My second question is to pick up on what Dr. Flynn said about overclassification. I wonder—and the reason I am asking this is because our subcommittee is readying legislation on this subject. But I wonder if overclassification is one of the main stumbling blocks to sharing information?

So let me ask you to respond in any order, and I am watching the clock.

Mr. GUIORA. I will begin with the question about the Israeli response to acts of terrorism.

You are absolutely right. We have been, in a sense, if you will, conditioned on how to respond. The Israeli version of the Department of Homeland Security, the Home Front Command, there is a response, there is a prepared, institutionalized response, which the public is a critical aspect of that. That is correct.

That being said, I think in terms of the subcommittee and the Homeland Security Committee, there is no reason that this process of institutionalizing a response can't begin here in the United States.

I would say that 9/11 is a very unusual kind of terror attack. It is not the daily fabric of terrorism. I think that in order to have a more effective public response, what we have to do is to begin, maybe through you, to educate the people on how to respond in the case of an act of terrorism, which goes exactly what to resiliency is.

I think the most important aspect of all this is to institutionalize both the preparation and the response, rather than to have it at a tactical level and thereby to develop a more strategic response. That, I think, in terms of, God forbid, there be another terrorist attack in the United States, that would lead to more effective prevention, and maybe more importantly, a more effective response too.

But it is all about institutionalizing and educating the public.

Ms. HARMAN. Thank you.

Dr. Flynn.

Mr. FLYNN. Well, one key component of resilience you captured very well, Chairwoman Harman, in your opening statement, which was about making terror less terrifying. Really, at its heart, fear, which is of course the main ingredient of terror, is really two things. It is, first, an awareness of threat of vulnerability. So what a terrorist does, if they take us by surprise, is they take things we would think are benign and we didn't pay much attention to and suddenly see them as vulnerable or see them as they pose a threat.

The second component, the most critical one, is a sense of powerlessness with dealing with that threat of vulnerability. I would argue, therefore, the Nation is more at risk today than we were on September 11 for being terrified, because we get a lot from Washington about our sense of threat and vulnerability, and because we have failed to give the American people and the people they turn to first, the first responders and first preventers, the tools they need to manage and respond and recover from these.

Now, we say a child is fearless when they don't know putting a hand on the stove is going to hurt. But what we do is we give them information, and ultimately that vulnerability is there, but we work our way through it.

In the same way, while getting information is so important to the American people, is it bounds the fear and it gives us confidence to bounce back, which is very much a part of the American tradition. It is in our DNA to be resilient as a people.

Specifically, on the classification issue, there is just no question that the system is broken, fundamentally broken. The clearance process is completely overwhelmed. Because things get routinely overclassified, they can't get to the people who need it. There are horror stories of locals who present information to the Federal Government, who classifies it, and then they are told they can't share it with their own chiefs, never mind anybody else, because those locals don't have the clearances to share it. As soon as you are in the process, you are in a morass that makes information-sharing impossible.

We are not dealing with Soviet espionage here. We are dealing in a case where, as the DNI has said, we need to be more geared toward the need-to-share than the need-to-know. The rules, the entire structure, is still built on the need-to-know. Until that changes, which is just the work that this subcommittee needs to do and the administration should have done, we are basically digging ourselves into a deeper hole.

Ms. HARMAN. Thank you.

Mr. Eddy, I couldn't get to you under my strict rules, but I am sure you will have an opportunity to address these questions and others as others ask you questions.

The ranking member is now recognized for 5 minutes.

Let me add that I will recognize people who came before the gavel in the order that you would expect. Those who came afterwards will be recognized in the order that they arrived.

Mr. Reichert.

Mr. REICHERT. I thank you, Madam Chair.

I want to first, again, thank you for being here. Remembering that this week is National Police Week, and today we are watching thousands of our local police officers visiting Washington, DC, to remember their brothers and sisters who have fallen in defending freedom here in the United States of America.

I spent 33 years in law enforcement before I came here. I liken your description of cultural change to a change from the 1970s patrol mentality that we had when I was in a patrol car—with dark brown hair, by the way, a long time ago—where today we have community policing. A philosophical cultural change had to take place to include the community. It was a very difficult thing to do.

So I want to touch on the cultural issues that the Chair has touched on, more in the way of how you overcome those. I think there are two ways. No. 1 certainly is the personal relationship, and then, No. 2, there has to be a commitment. Sometimes a commitment is attached to money.

So I hear a lot from my sheriff's friends, my police chief friends across the Nation regarding recent efforts to cut some of the monies going to local law enforcement in their efforts to be a part of

the fusion center. FTEs, for example, are a very important asset to any police department, but the smaller you get, the more important that asset becomes. But it doesn't mean that you are not involved in the homeland security effort, one way or another.

I have heard the horror stories, too. I am aware of the barriers and those things that prevent us from sharing information. I am excited to hear that you have all recognized the barriers.

What do we do about the cultural change at a national level? Then, also, your opinions on, if we are to spend more money, which I believe we must, in aiding our local officials, what do you spend it on?

Mr. EDDY. I appreciate that very thoughtful question. Let me give you my brief thoughts on it and see if there is some time for my fellow panelists here.

I would suggest that, first of all, the police are the most present and woven aspect of government in our local communities, so they can be the beginning of resiliency. Having them be trained and aware will allow to you have a more resilient and robust community. Community policing obviously helps with that.

The next evolution since community policing, of course, has been COMPSTAT and, we think, intelligence-led policing. That is where the Federal Government can be of huge asset to the local police. The need for FTEs, the need for analysts, the need for folks who learn intelligence and that can inject that into policing not only will make police better for counterterrorism, it will make them better against all hazards. The proof is irrefutable, and the cost is minimal.

So it is a way to increase highly leveraged dollars, increased police efficiency, by getting in and helping them with intelligence programs. These fusion centers are a great way to get there, is a quick answer.

Mr. GUIORA. I think that what is going to be very critical, in terms of responding to your question, is to institutionalize changing the emphasis of how the police are going about their work, I think from a law enforcement paradigm to a counterterrorism paradigm. Particularly, if we think about homegrown terrorism, that raises, obviously, again, important constitutional legal questions.

But I think that in my meetings with police around the country, it is clear that this change in focus is going to be critical, which ties in directly, going back to your question, Madam Chairwoman, about how we go about educating the public. Because I think the police and the public are going to have to work very closely together in changing a cultural focus and institutionalizing that. That will, I think, also require reallocation of resources.

I think in terms of how we go forward, we are going to have to be very honest with the public that terrorism is out there; it is a constant threat. No, we cannot prevent every act of terrorism. It is impossible to do that. What are the limits in terms of how we go about preventing acts of terrorism, protecting ourselves? But it really is going to require also institutionalizing the educational process with respect to the public.

Mr. FLYNN. The only thing I would add, perhaps, just reinforce, in the experience as a retired Coast Guard officer, cops talk to cops; they don't talk to bureaucracies.

So the things that are most important are finding ways in which we enhance those relationships by creating the kind of training academy that R.P. Eddy was talking about, broaden those out, and finding mechanisms, fusion centers and so forth, where people do come together. But the education can really be the multiplier in creating those settings.

I just had the opportunity to go to the National Fire Academy. They had their 20th anniversary. Every year they have a reunion of all the graduates of that institution, over 200 fire chiefs were there. That relationship, you could tell, is as thick as blood. It is across the country, and they come voluntarily on their own dime to those reunions.

So those things are not hugely expensive, but facilitating it—but, most important, I think, is a sense of it is not a caste system, where the Feds and the national security apparatus, that is real place where we put our money and resources, and the locals, well, get to this when you get to it. We are structured, basically, where most locals are sending one or two officers, perhaps, off to a joint terrorism task force, checking that box, and going about the daily policing. We are not figuring out how we integrate the counterterrorism mission into the course of normal police work, and recognizing that is where ultimately we are going to get our biggest bang for the buck.

Ms. HARMAN. Thank you very much.

Mr. Dicks is recognized for 5 minutes.

Mr. DICKS. Let me follow up on that. What is the best way to do that? How do we work with the local police in order to do that?

I mean, I remember the story we had out in Los Angeles where there was a group people that had come out of the prison system, and they got arrested on I think it was a crime, a robbery of some sort. Then they found out, when they went to their homes to arrest them, they found out that—they had been sensitized to look for this other kind of information. They found this stuff that looked like, you know, something that a terrorist might by doing, and, therefore, they discovered that this was, in fact, a terrorist ring.

So, I mean, who should do this? Should the Department of Homeland Security work with the police departments or through the fusion centers? How do you start the educational process?

I like your academy idea. I think that is a good one.

Mr. EDDY. I will answer that briefly, Congressman Dicks.

Right now, as far as I can tell, working with a number of police departments, they are entirely puzzled as to the answer to that question. They don't know to whom they should turn to try and get information. Whereas 2, 3, 4 years ago, the Federal Government apparently couldn't really care less about working with the police, now it appears there is some sort of rush to be the one who does this.

So what is clear and necessary is that this Congress figure out what those lines of authority are. I think the President recently waived something so that DHS lost part of their role to the DCI to be an intelligence fusion capacity for State and locals. I could certainly be confused about that. But I think that——

Mr. DICKS. Say that again. What happened?

Mr. EDDY. My understanding is that, via presidential waiver, the DCI, within the DCI, I think within the NCTC, they are now taking on part of the role to share information with State and locals, a role that presumably could have been better filled at some point by DHS or by FBI. Although, I would say that whoever will share that information and whoever will take the initiative should be the ones to do it.

Most critical to realize, though, is it is not just about getting the information pushed down to the State and locals. It is about enabling the State and locals to collect it on their own, in a constitutional manner. Right now they don't have the capacity to do so, because they don't have the time or the skills or the money to do it.

So I would suggest the NCTCA academy that we proposed and we have already launched in L.A. become a Federal model. It is a fantastic, high-leverage way to teach police how to get involved with intelligence and intelligence-led policing. I would suggest the foreign liaison——

Mr. DICKS. So they go to the academy and they come back and then they educate the rest of the police force.

Mr. EDDY. Exactly. They go once every 2 weeks for 2 hours to get trained by world-class professionals to begin thinking about first preventers.

That only works if you have an intelligence capacity bringing analysis in. So you have to have analysts in the Department or in the fusion center looking at international attacks, looking at domestic threats, and bringing that intelligence in and saying, listen—the Lodi case, to which you referred, is a perfect example of what I am describing. Those police were sensitized via our program and the work by John Miller and Chief Bratton to look for things that are suspicious and ask the next question, and that ended what could have been a horrific series of attacks. We need more success stories like that.

Mr. FLYNN. If I might add just one very brief illustration of doing this right but the barriers that you run into—the NYPD, shortly after the 7/7 attack in London in 2005, that they had a foreign liaison law enforcement official there, but they came back with photos of the Leeds apartment, which was a long ways from London, where the suicide packs were made up. They took two trailers, and they recreated that apartment with everything basically as it was in that apartment. They ran virtually every NYPD patrolman through those trailers and said, "If you see this when you are out in the domestic, if you see this when you are dealing with a burglary, it is not a meth lab or kitchen chemistry. This is what is going on here."

Now, that could be made available to folks at Newark, which is just across the river, or elsewhere, but there are no training resources or other things for that occur. NYPD doesn't have a budget to train the rest of the law enforcement.

So there are a lot of self-help ways where this can happen as a cross-fertilization, but this has not been seen as a priority to support at the national level, at the Federal level.

Mr. GUIORA. If I could just add one comment to that, I think, Congressman Dicks, to answer your question, it is going to require articulating, not rearticulating, but articulating the

counterterrorism paradigm in terms of homegrown terrorism. I don't think we have really begun doing that. It makes people very uncomfortable. I think it is going to require doing that.

I think in terms of the police, State and then moving up to the Federal Government, up and down in terms of this interaction, it is going to require, for instance, as I said earlier, having scenario-based simulation exercises where the local police are working with State government and Federal Government, in trying to get to the essence of your question——

Mr. DICKS. Well, I have 14 seconds left. To me, that is the way to do this, is to bring the Federal people and the State people together and do case studies or scenarios and move from that. I would hope these fusion centers that we have created would also play a role in this.

Mr. GUIORA. I have 2 seconds. I think it is also going to require thinking long and hard about various constitutional questions, in terms of the limits of various jurisdictional issues. But I think the time, clearly, is now to address those issues and not to wait until tomorrow.

Mr. EDDY. It is easier to do those with State and locals than with Federals.

Ms. HARMAN. Thank you very much.

Mr. Dent is now recognized for 5 minutes.

Mr. DENT. Thank you, Madam Chair.

Good morning.

Mr. Eddy, you mentioned in your testimony, and then I guess Dr. Flynn touched on it just a few moments ago, but you mentioned it, the concept of a foreign liaison program for State and local law enforcement, and partially because foreign reporting is apparently not getting to the State and local levels.

Should the Federal Government, in your view, be footing the bill for State and local officials to bypass Federal intelligence agencies, or should there just be more of an effort to make sure that this information is shared better?

I would like to hear what you have to say, as well as Dr. Flynn, on that point.

Mr. EDDY. I appreciate that question, Congressman.

I helped build the NYPD foreign liaison program, which has been massively successful. Dr. Flynn was describing earlier the 7/7 trailers. Those were only buildable because we had police officers in London looking at this site and learning about it.

The thing that we have to understand is different bosses, different agendas mean you ask different questions and you look for different answers. So if you have an FBI legal attache overseas and he arrives at the site of an attack, versus an NYPD police officer at the site of an attack, they are looking for very different things, and they are doing different things, and they are probably doing them well. The FBI officer is looking for issues that are necessary for his line of authority. The NYPD officer is looking for issues about subway security; he is looking at issues about the way the security was set up, how far the garbage cans were from their front door. The list goes on and on and on.

The ability to have overseas intelligence—I mean, you know, it is so axiomatic to say we live in a global world, the terrorist threat

is everywhere and anywhere at the same time. You have to be aware of what is going on around us. If you don't have that intelligence collected from a police point of view, it doesn't matter if you share or don't.

So, right now, I don't believe that it is even collected the way that it needs to be collected for State and locals. So the idea of bypassing the FBI or bypassing State is not the way I look at it. I look at it as complementing the collection and bringing more resources into the United States. That is something that the foreign liaisons can do.

The proposal in the LEAB legislation, to me, seems very smart. So my center, my leadership and donors, we are going to take this on on our own, because the Federal Government hasn't put money into it. I helped build it for NYPD. We are going to build it for a number of other police departments. LAPD is interested; Miami and Chicago also are.

So we are going to have these departments each assign one police officer that they will pay for their salary, and then local donors will pay for their travel and their housing. We will send them overseas, and they will do this collection and this integration with the local police. Then, of course, that will be pooled amongst all the Police Executive Research Forum communities to bring that intelligence in. So it is not a bypassing; it is critical piece of intelligence that needs to be collected.

Mr. DENT. Dr. Flynn.

Mr. FLYNN. I really would reinforce that. What we are really talking about is building essentially different lines of capabilities, using different assets we have as a Nation, which is extraordinary professional local police who can interact with their counterparts oversees.

I recently, just a few months ago, had a chance to give a talk to New Jersey's law enforcement community. I was getting a ride by one of the State police detectives, and I was asking him about the relationship with the FBI, which historically is a bit of a challenge in most communities. He said, "Yeah, everything is fine. In fact, we have a new guy here in Newark. And I was kind of interested, I went with him to a meeting we had to go to. And we were running a bit late, and he kept circling around the building we had to go to. And I said, 'Look, there is a parking space right here; why don't you park there?' And it turned out the agent didn't know how to parallel park."

That just highlights one issue, which is that locals don't tend to stand out when they do their local policing in a way that somebody from outside coming in does. It is a culture, it is a whole—so we have that strength that we want to take advantage of. That has counterparts overseas. How people talk and interact is different at that level.

The bottom line is this, the new battlespace is the civil economic space. Who is going to be there? Then how do we get information to those players? We should be working overtime as a Nation finding the resources to basically capitalize on relationships that exist and being able to build up that expertise.

Mr. DENT. I guess, to follow up—I appreciate your answers. They are well thought-out. But do you think we should be assigning

more State and local police officials then to help Federal intelligence officials prepare product, intelligence product? Is that what we need to be doing more of?

Mr. FLYNN. Absolutely. There is little question that they see, often, things that the Federal law enforcement people don't. Particularly when we talk about things like critical infrastructure and so forth where there is often not a lot of resident expertise at the Federal law enforcement level, where you go to a community where someone has been in port for a long time—you have L.A. police, marine police forces who have been operating in the port for 30 years. They are going to know a heck of a lot more than a new FBI mission that brings them into the port.

So capitalizing on that is so important. They help to tell you what is real and what is not, and finding a liaison and making sure we have that capability. Again, we are not trying to replace things. We are really trying to make sure that we get better collaboration than we have had before.

Mr. GUIORA. Can I just add one comment on that, Congressman Dent?

Mr. DENT. Sure.

Mr. GUIORA. I think what really needs to happen is we need to articulate what is it we are trying to do. So if you move the policeman and you have them working closer with Federal officials, the question is, for what purpose? Is there, again, a large, overriding, strategic thought behind it, or are you just responding or thinking tactically rather than strategically?

Because, without thinking about the strategic question, all you are going to be doing is moving people from here to here without some sophisticated thought process behind it.

Ms. HARMAN. Thank you very much.

I would just point out for the record that this subcommittee has worked for almost 2 years to force, and now by force of law, the inclusion of State and local law enforcement in the preparation of intelligence products by the NCTC. They are now, as an organization, called the ITAG.

We have had a number of hearings about this. I think all of us continue to believe not only that they are valuable, but that they should be doing more and more so that these products are much more useful by the people who are actually going to find and prevent the next terror attack.

Mr. Perlmutter is recognized for 5 minutes.

Mr. PERLMUTTER. Thanks, Madam Chair.

First of all, I got here late, but just in the discussion I have learned a lot. One of the things I hadn't really summarized it, in the need-to-know versus need-to-share. The need-to-share is preventative, you know, prevention kind of approach, as opposed to need-to-know, where you want to capture somebody. So that helped me, kind of, you know, understand this whole categorization, classification a lot better.

My question comes more of a constitutional question. On bouncing back, which several of you talked about the resilience, one of the reasons that I think we don't bounce back as quickly as we might is because there are circumstances, the attack, whatever, is played and played and played and played again, to the point that—

and I will just take one of my kids. Sort of, 9/11 traumatized the heck out of her, and lots of other people obviously. Here I am in Denver, Colorado, watching it again and again and again. I think the first amendment, you know, clearly limits the ability—allows the media to play it as many times as they want.

But, you know, you guys looking at this issue of bouncing back and the public bouncing back, what do we do about that?

Mr. GUIORA. I think, in terms of the first amendment, obviously, freedom of speech amendment, the media rights are clearly articulated. I would take that to a different paradigm, though, Congressman Perlmutter. What needs to be made clear to the public is that terrorism is going to occur and it is a reality.

Going back to your original question, in Israel my 11-year-old will tell you it is a matter of time until there is another terrorist bombing, just like there was yesterday. That is the reality.

I think once the public understands and once leadership articulates to the public that this is our new reality, this post-9/11 world, it is what it is, it will help us in a much more effective manner to create and articulate a new paradigm in terms of going forward.

The media is going to play the role of watchdog; that is inevitable. TV will have the pictures over and over again. Your child, hopefully, won't have to be traumatized again. But in the context of articulating up and down to the public that this is the new reality, it will make it much more feasible or realistic to respond to acts of terrorism. If we think that we are going to defeat terrorism, if we think that we are going to prevent acts of terrorism, then when it happens, we are going to say, "Oh, it can't be." But it is the reality, and it really does require rearticulating how we educate the public.

Mr. FLYNN. I would just reinforce this notion about the education of the public, that it is not just, "Here is a threat, here is a threat, here is a threat and vulnerability," but, "Here are tangible things that you can do to make yourself safer and better prepared."

It is important, also, though, to understand resilience as a concept, which is drawn heavily from the folks who did earthquake issues, is built in up front. We are seeing this tragedy in China right now, and of course virtually all the buildings that have come down were ones that weren't resilient enough to withstand a foreseeable event and the result is massive loss of life and destruction of property. You build resilience up front by, in that case, designing buildings well enough to withstand the expected level of forces.

I think the real point here is that terrorism is a fact of life, as natural disasters are. We need to acknowledge that, but not just say that is out there in the ether. You give people things to do. You give them information which will make them better prepared and able to ride these things. When they do, inevitably they are less terrified.

It is difficult for me as a retired Coast Guard officer; I came in at age 17. We have an unofficial motto in the Coast Guard: You have to go out, but you don't have to come back. The whole notion is you do whatever it takes to rescue somebody by going into harm's way. But when you develop the skills for doing that here, I found my crew always were empowered. They grew up in the process of giving them the skills to deal with the terror that Moth-

er Nature could put on us here. So part of it is just dealing with that reality, and we need to do it.

On the media issue very specifically, it has just got to cut both ways. We know, in the Second World War, the media both entertained and informed. But we have to find ways to create incentives and engagement with the media as an industry, just like other private-sector entities with critical infrastructure, to address this issue. There are messages that hurt, messages that cause fear, and there are messages that can be quite helpful.

I have made just very basic recommendations to the media about making sure you have a ready list of people who really know what they are talking about, so when things go on, you can get their faces in front of the cameras instead of a talking head or the guy who wrote a spy thriller last week who is coming in now because the producer knows him.

There are mechanical things that we can ask the industry to do, but we haven't engaged them in a constructive way. I found media executives, when I had a chance to talk with them, they are responsive to this. But, again, the Government has never made the outreach, largely by saying, "We are holding our cards close to the chest. We are taking care of terrorism. You go about your lives. You go to the mall." All this is really heightening anxiety, almost guaranteeing more trauma than we need to have from what our eventuality is.

Mr. PERLMUTTER. Thank you.

Ms. HARMAN. Thank you.

Mr. Shays is now recognized for 5 minutes.

Mr. SHAYS. Thank you, Madam Chairman, for holding this hearing. I would like to get into two areas.

One, I would like your comment on whether you think the media, the so-called "terrorist experts" on TV, are contributing to helping people understand the threat and dealing with the threat, or are they insignificant, or are they moving the public in the wrong direction.

I would like all three of you to answer.

Mr. EDDY. If I can take a shot at that, and that builds nicely on the previous question.

I think a lesson that we learned in New York and that we are trying to teach in Los Angeles is that the media exposure after an attack or before attack can largely be shaped by the engagement you had beforehand, just as Dr. Flynn was saying.

So part of what we encouraged NYPD to do, for example, is bring the media in early, before anything happens, and give them a tour. You end up getting a positive press story out of that, about, "Look how strong and resilient the police department is," and that is positive——

Mr. SHAYS. Well, you guys are the experts. I am talking about the talking-head types that show up on the talking-head programs.

Mr. EDDY. Sure. Well, I think we were, kind of, talking about this earlier amongst ourselves. It is, sort of—they are very—well, most of——

Mr. SHAYS. I need a short answer.

Mr. EDDY. Not positive, don't have a very positive impact, and tend to play to the producers, who want you to stoke fear, because that sells TV minutes and commercials.

Mr. SHAYS. Thank you.

Mr. GUIORA. I think a true expert can be very effective in terms of explaining what the threat is and what is going to be the appropriate response and what is the realistic response. A non-expert talking head who is going to be playing to various audiences I think, Congressman Shays, is going to be very ineffective. A real expert who can speak clearly, concisely and precisely is going to be very effective in terms of explaining to the public how do we go forward and what is next.

Mr. FLYNN. Fundamentally, it is usually how the interviews are structured, classically "what happened" instead of "what do we do about it." So to the extent of what do people know and what should people be doing.

So the fact that, basically, the media stories often stop with just reporting what happened and the terrorist experts are explaining that without giving information, that can just sort of feed the sense that this is an omnipotent threat which is unbounded and which there is nothing we can do. People feel powerless as a result.

Mr. SHAYS. Well, it strikes me that, therefore, what you are telling me is that the experts in law enforcement and so on should not give up the time to leave this large void to be filled by people who aren't going to make a contribution.

Let me talk about overclassification. I chaired the National Security Subcommittee of the Oversight Committee, of Government Reform, and am now its ranking member. We had a number of hearings. The defense witness said that 50 percent was overclassified, and the nongovernment folks said up to 90 percent was overclassified.

That strikes me as perhaps accurate, somewhere in between those two, but has, I think, horrific implications. I would be interested to know your reactions. You touched on it a little bit. But give me an example of where overclassification can hurt and what you think about the issue in general.

I will start with you, Dr. Flynn.

Mr. FLYNN. Probably the place where it hurts the most is dealing with the private sector in safeguarding critical infrastructure. What you have, of course, are the people who design and operate that infrastructure, know its real vulnerabilities and know its real strengths. Most of the people who are actually assessing it are in a classified world and making best guesses, and most of those educated, best guesses are usually very uneducated.

So you can't have this conversation. If you think about what happened in 2003 in the Northeast when the grid went down, as a result, as we found out quickly, not by acts of terror but trees overgrowing and triggering a series of events that shut that grid down, it was easy for us to learn how to mitigate that in the future and respond better because we had everybody in the room—Canadians, State hearings and so forth.

I can imagine the scenario where the information started that we had pulled out maps or charts from Afghanistan that somebody was targeting towers, and then that was shared only with chief se-

curity officers, well, what would the industry do about that? The problem wasn't the towers. The problem was how the grid was integrated.

So that is really the key, is where it is going to get fixed.

Mr. SHAYS. Thank you.

Mr. GUIORA. To your question, last week I met with some agents from the FBI, and I told them that the only way we can begin discussing resilience is by having public-private information-sharing. They turned more white than the color of your shirt and more red than the color of the University of Utah.

I said the only way that we can begin addressing the issue is by information-sharing, which goes exactly to the issue of minimizing classification, because otherwise——

Mr. SHAYS. Why did they turn white or red or whatever color?

Mr. GUIORA. Because I think they found the idea of having to share information with the private sector to be problematic on a practical level, on a policy level and on a constitutional level, which goes back to the issue of we can't go forward without information-sharing.

Mr. SHAYS. Mr. Eddy, you have 10 seconds.

Mr. EDDY. I think one of the quick solutions would be to try and figure out who the U.S. military reservists are within police departments and see if you can access a clearance that way, so you have one channel then, at least, where someone is cleared.

I don't find overclassification to be as much of a threat as most people do, because I think the ultimate threat information can move its way down to the police department if it needs to. I think intelligence, actually, is more important lateral and local. That is real the intel is going to come from, and at that point doesn't need to be classified.

Mr. SHAYS. Thank you.

Ms. HARMAN. Thank you, Mr. Shays.

Thank you to our members and to our witnesses for a really extraordinarily good hour-plus of conversation about these issues.

Let me just say to Mr. Eddy, in closing remarks, that we think—and we are, again, readying this bill—that protecting sources and methods is the right justification for classifying information. Protecting turf and protecting oneself from political embarrassment are not good reasons. So our focus is going to be on how to make the system work as it should work.

I do think, consistent with what Dr. Flynn has said, that that will enable us to move more information more quickly to people who need it. But you are also right that a lot of what has to change is that police departments and sheriff's departments have to be educated to do what they can do better than anyone else.

So I think this hearing confirms something this subcommittee believes on a bipartisan basis, which is that we need to be advocates at that level, and we need to be sure that the people at that level get what they need from this level, not the other way around. Because they are the people who will be the true first preventers and who will connect the dots, as Mr. Dicks was talking about, and figure out that a series of gas station robberies wasn't a series of gas station robberies, it was an effort to collect money to fund a terror

cell that was going to attack Jewish sites and military recruiting centers in the Los Angeles area, as an example.

So I thank you for your testimony. This is what we work on in this subcommittee, and hopefully we are adding value. For sure, you are.

The hearing stands adjourned.

[Whereupon, at 11:10 a.m., the subcommittee was adjourned.]