S. Hrg. 112–612

THE FUTURE OF HOMELAND SECURITY

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

EVOLVING AND EMERGING THREATS—JULY 11, 2012

THE EVOLUTION OF THE HOMELAND SECURITY DEPARTMENT'S ROLES AND MISSIONS—JULY 12, 2012

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
76–059 PDF WASHINGTON : 2012

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 AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE MCCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*
CHRISTIAN J. BECKNER, *Associate Staff Director for Homeland Security Prevention and Protection*
NICHOLAS A. ROSSI, *Minority Staff Director*
BRENDAN P. SHIELDS, *Minority Director of Homeland Security Policy*
ERIC B. HEIGHBERGER, *Minority Professional Staff Member*
MARK K. HARRIS, *Minority U.S. Coast Guard Detailee*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk*
LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

Opening statements: Page
Senator Lieberman 1, 39
Senator Collins 3, 41
Senator Carper 21, 58
Senator McCain 24
Senator Johnson 28, 62
Senator Akaka 66
Prepared statements:
Senator Lieberman 79, 148
Senator Collins 81, 151
Senator Carper 153

WITNESSES

WEDNESDAY, JULY 11, 2012

Hon. Michael V. Hayden, Principal, Chertoff Group 5
Brian Michael Jenkins, Senior Adviser to the President, RAND Corporation ... 7
Frank J. Cilluffo, Director, Homeland Seurity Policy Institute, George Washington University 9
Stephen E. Flynn, Ph.D., Founding Co-Director, George J. Kostas Research Institute for Homeland Security, Northeastern University 12

THURSDAY, JULY 12, 2012

Hon. Jane Harman, Director, President, and Chief Executive Officer, Woodrow Wilson International Center for Scholars 44
Admiral Thad W. Allen, U.S. Coast Guard (Retired), Former Commandant of the U.S. Coast Guard 48
Hon. Richard L. Skinner, Chief Executive Officer, Richard Skinner Consulting 51

ALPHABETICAL LIST OF WITNESSES

Allen, Admiral Thad W.:
Testimony 48
Prepared statement with an attachment 157
Cilluffo, Frank J.:
Testimony 9
Prepared statement 102
Flynn, Ph.D., Stephen E.:
Testimony 12
Prepared statement 114
Harman, Hon. Jane:
Testimony 44
Prepared statement 154
Hayden, Hon. Michael V.:
Testimony 5
Prepared statement 83
Jenkins, Brian Michael:
Testimony 7
Prepared statement 86
Skinner, Hon. Richard L.:
Testimony 51
Prepared statement 168

Page

APPENDIX

Response to post-hearing questions for the Record of July 11, 2012:
Mr. Hayden 125
Mr. Jenkins 127
Mr. Cilluffo 135
Mr. Flynn 142
Response to post-hearing questions for the Record of July 12, 2012:
Ms. Harman 179
Admiral Allen with an attachment 183
Mr. Skinner 200

THE FUTURE OF HOMELAND SECURITY: EVOLVING AND EMERGING THREATS

WEDNESDAY, JULY 11, 2012

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:09 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, Pryor, Collins, Coburn, Brown, McCain, and Johnson.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. I apologize to my colleagues for being late. I got a call about a pending legislative matter that I had to attend to. And I thank Senator Collins for resisting the urge to grab the gavel. [Laughter.]

Although a twist of fate may take somebody at this table to the gavel in January.

This is the first of two hearings that this Committee will hold this week, today and tomorrow, and other hearings will probably follow in a series that is aimed at looking backward and forward to both the terrorist threat to our country, particularly to our homeland, and how the Department of Homeland Security (DHS) has done in responding to that threat and what it should do to respond to the threat, be ready to meet the evolving threat in the decade ahead.

This review is engendered first and most significantly in anticipation of the 10th anniversary of the Homeland Security Act being passed, in November 2002, that created the Department of Homeland Security legislation, which this Committee sponsored and originated.

I suppose in a different sense more directly related to the Committee, as I said a moment or two ago, there will be a change in leadership of this Committee in the next session since I am leaving the Senate at the end of this term. I personally thought that it would be responsible for me in the last 6 months of my chairmanship to try to build a record, particularly from outside experts such as those we have here today, but also from the Department and others in government in later hearings, to help guide the new leadership of the Committee as it continues its work in the next session of Congress.

This first hearing is going to examine the mid- to long-term evolution of the terrorist threat and other threats to our homeland security. It will focus less on current or near-term terrorism threats.

In September, the Committee will hold once again our annual threat hearing with Secretary Janet Napolitano, Federal Bureau of Investigations (FBI) Director Robert Mueller, and National Counterterrorism Center (NCTC) Director Matthew Olsen that will focus more on the current threat picture, and then tomorrow with another set of witnesses, we will take a look at how the Department of Homeland Security has evolved over the last 10 years, how it has done, and what it will need to do in the decade ahead.

Within the longer-term time frame that we are going to discuss today, I hope we will answer questions such as this: To what extent will the terrorist threat to the homeland 5 to 10 years from now resemble the current threat picture? What is the mid- to long-term significance of Osama bin Laden's death and the death of other al-Qaeda operatives for core al-Qaeda external operations? Will the historic developments in the Arab world politically—the Arab Spring or Arab Awakening—affect the terrorist threat to our homeland in any way? And then, more broadly, what societal or technological factors are likely to have an impact on the future threat within the time frame that we have talked about?

For example, how will the continued expansion of online social networking impact the way terrorist groups recruit and radicalize individuals? And in a different way, what will be the impact of current demographic trends in different parts of the world—the Middle East, Africa, and Europe?

So those are some of the kinds of questions that I hope we will deal with today. We have a really extraordinary panel of witnesses, and I am grateful to the four of you for being here.

Very briefly, General Michael Hayden, one of our Nation's leading intelligence and security experts, served within the last decade as Director of the Central Intelligence Agency (CIA), Deputy Director of National Intelligence, and Director of the National Security Agency (NSA). A retired four-star general from the Air Force, General Hayden is now currently a principal at the Chertoff Group, which is a strategic consultancy led by former DHS Secretary Michael Chertoff.

Brian Jenkins is a senior analyst at RAND and has been a greatly respected expert on terrorism and related issues since the 1970s. He was very young at the time he first appeared as an expert in this regard. He has authored dozens of reports on homeland security and terrorism issues in the last decade.

Frank Cilluffo is Director of the Homeland Security Policy Institute at the George Washington University (GW), one of the leading think tanks for homeland security issues in our country. Before working at GW, he served from 2001 to 2003 as Special Assistant to President Bush for Homeland Security, working in the White House Office of Homeland Security as a Principal Adviser to Governor Tom Ridge.

And Steve Flynn, Founding Co-Director of the Kostas Research Institute for Homeland Security at Northeastern University. Prior to this, he was President of the Center for National Policy and a senior fellow at the Council on Foreign Relations. He has testified

dozens of times before Congress on homeland security issues and is the author of two books, "America the Vulnerable," and "The Edge of Disaster: Rebuilding a Resilient Nation."

I could not ask for four better people to help us look back, look forward, and build the kind of record that we want to build. I appreciate your presence here.

With that, I will yield to Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

The terrorist threats facing our country have evolved since the horrific attacks on September 11, 2001 (9/11). That awful day steeled our national resolve and drove us to rethink how our intelligence agencies were organized and how our instruments of national power ought to be used.

Since then, we have taken significant actions to better counter the terrorist threat, but the terrorists have constantly modified their tactics in an effort to defeat the security measures we have put in place. An example is the October 2010 air cargo plot originating in Yemen in which al-Qaeda apparently sought to avoid improvements in passenger and baggage screening by exploiting vulnerabilities in cargo security.

Let me emphasize that it is extremely troubling that terrorists have been aided in their efforts to circumvent our security by the all-too-frequent leaks regarding our counterterrorism activities and capabilities. As we consider the challenges posed by emerging threats, we simply cannot tolerate giving our adversaries information that they can turn against us.

When Chairman Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), our goal was to create a coordinated effort among the Department of Homeland Security, the Director of National Intelligence (DNI), and the National Counterterrorism Center as well as other Federal partners and stakeholders.

One instrument used in these collaborative efforts has been the network of 77 State and local fusion centers that help manage the vital flow of information and intelligence across all levels of government. These centers are recipients of national intelligence products, but they must also become robust aggregators and analyzers of information from their own areas that can be shared so that trends can be identified and the understanding of threats to our homeland can be strengthened.

An example of the effectiveness of fusion centers occurred on June 25 of last year when officers from the Colorado State Patrol attempted to pull over a man who was driving erratically, fled authorities, and eventually crashed. As the police processed the driver and information about his pick-up truck, they learned from the Colorado Fusion Center that he was linked to an attempted bombing of a book store. That driver is now in custody facing Federal charges.

This type of grassroots teamwork is essential to combat a deceptive and often elusive enemy. As discussed in a recent report by the Homeland Security Policy Institute at George Washington University, however, fusion centers have yet to achieve their full poten-

VerDate Nov 24 2008 13:06 Dec 04, 2012 Jkt 76059 PO 00000 Frm 000007 Fmt 06633 Sfmt 06633 P:\DOCS\76059.TXT SAFFAIRS PsN: PAT

tial. Questions have been raised about their analytic capabilities and about whether they are duplicative of the work of the Joint Terrorism Task Forces.

The reforms enacted in response to the 9/11 attacks have helped to ensure that there have been no other large-scale attacks in the United States. The absence of such attacks and our success in thwarting terrorist plots at home and abroad should not lull us into a false sense of security, for this is no time to rest as gaps in our security net remain.

We continue, for example, to witness the growing threat of violent Islamist extremists within our own borders. Sometimes these terrorists have been trained overseas. Others have taken inspiration from charismatic terrorists via the Internet, plotting the attacks as lone wolves.

Last year, as Members of this Committee well know, two alleged al-Qaeda terrorists were arrested in Bowling Green, Kentucky. This highlighted a gap where elements of our security establishment had critical fingerprint information that was not shared with those granting access to these three men to our country.

Another growing and pervasive threat is that of cyber attacks. Earlier this year, the FBI Director warned that cyber threats will soon equal or surpass the threat from terrorism, and just last month, several former national security officials warned that the cyber threat is imminent and represents one of the most serious challenges to our national security since the onset of the Nuclear Age 60 years ago. They further wrote that protection of our critical infrastructure is essential in order to effectively protect our national and economic security from the growing cyber threat, and that is exactly what Chairman Lieberman and I have been working with our colleagues on legislation that would accomplish the goal of helping to secure our Nation's most critical infrastructure, such as the power grid, nuclear facilities, water treatment plants, pipelines, and transportation systems. I can think of no other area where the threat is greater and we have done less to counter it.

There is also a growing threat from transnational organized crime. The Director of National Intelligence has testified that these criminal organizations, particularly those from Latin America, are an abiding threat to U.S. economic and national security interests. Our intelligence community needs to focus on their evolution and their potential to develop ties with terrorist groups and rogue states.

The 9/11 Commission devoted substantial attention to the challenge of institutionalizing imagination. In an understatement, the Commission's report observed that imagination is not a gift usually associated with bureaucracies. Yet imagination is precisely what is needed to address emerging and future threats. We must persistently ask: What are the future threats? What technology could be used? Do we have the intelligence that we need? How can we stop these leaks that compromise our security? Are we prepared to thwart novel plans of attack? What will our enemy even look like in 2, 5, or even 10 years?

Surely we are safer than we were a decade ago, but we must be relentless in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden has proved,

America's resolve and creativity are our most powerful weapons against those who seek to destroy our way of life.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, for that excellent opening statement.

General Hayden, let us go right to you, and thanks again for being here.

TESTIMONY OF HON. MICHAEL V. HAYDEN,[1] PRINCIPAL, CHERTOFF GROUP

General HAYDEN. Well, thank you, Mr. Chairman, Senator Collins, and other Senators. Thank you for the invitation to be here.

Mr. Chairman, as you pointed out, I am with Secretary Chertoff and the Chertoff Group, and we actually deal with a lot of the issues that we are going to discuss today. But I am here, of course, in a personal capacity, and I am really delighted to be here with this team. And I know the other members of the panel are going to drill down into some specific issues in their own areas of expertise. So what I would like to do is maybe just step back a little bit and perhaps provide a broader context in which we can place some of this morning's discussion.

One of my old bosses, General Brent Scowcroft, wrote very recently for the Atlantic Council—and I am kind of paraphrasing what the General said here—that he had spent his professional career dealing with a universe that was dominated by nation-states in which the pieces on the board were by and large influenced by what all of us today would call "hard power."

And he writes that is no longer true. Because of globalization, the international structure that was actually created by the Treaty of Westphalia about five centuries ago is no longer dominant. General Scowcroft points out that during the age of industrialization practically everything tended to make the state stronger. In today's era of globalization, practically everything tends to make the state weaker and less relevant.

And in addition to eroding the traditional role of the nation-state, globalization has pushed on to the international stage actors that we have never seen before, and it has made immediate and direct threats that a few decades ago were, at best, distant and oblique.

And here we sit with institutions, built for that age General Scowcroft governed in, practiced to be methodical, thorough, and stable, which are attributes, Senator Collins, none of which you listed as to what we need to be in terms of this new age.

So that really demonstrates our challenge. How do we adapt to these new dangers, be they terrorism or cyber or transnational crime? Frankly, I would suggest they are all merely specific expressions of this new reality of what we have, an intensely interconnected world that empowers individuals and small groups beyond all previous experience.

Now, with that as a premise as to what we are facing, let me illustrate both the challenge we face, repeating some of the things already mentioned, and the difficulty we are having forming an appropriate response. My personal experience: Prior to 9/11, we all

[1] The prepared statement of General Hayden appears in the Appendix on page 83.

believed, wrongly, that we had little to fear personally from religious fanatics living in camps in Afghanistan. We were wrong.

Prior to that, we saw no need for a Department of Homeland Security, and we were well practiced and very comfortable protecting both our liberty and our security by creating barriers to separate things that were foreign from things that were domestic, dividing things that were intelligence related to those things that were law enforcement related, and, frankly, that model worked just fine for about two centuries. But they failed, and now we are still adapting, and as this Committee knows, we are adapting with a great deal of controversy.

Again, pulling out of my personal experience, the Terrorist Surveillance Program that we created at NSA, designed to close an obvious gap: Detecting the communications of foreign terrorists operating from within the homeland. A very controversial program. You embraced that controversy in 2008 when you debated changes to the Foreign Intelligence Surveillance Act (FISA). And it is still controversial as the Senate debates even now an extension of the FISA Amendments Act.

We all agreed, for example, in the 9/11 Commission report that we needed a domestic intelligence service and that it was probably best to put it in the FBI. And despite that agreement, look at the reaction even today when the Bureau tries to collect information on anything without a criminal predicate, in that area we would call "spaces between cases."

And heaven help us and save us from the Associated Press if the New York City Police Department tries to do anything like the same thing.

Now, over two administrations, we have had measurable success against al-Qaeda, against those who attacked us on September 11, 2001. Dangers remain, though. Al-Qaeda Central could still reconstitute if we ease up the pressure on it; al-Qaeda franchises continue to pose danger, and at least one of them, al-Qaeda in the Arabian Peninsula (AQAP), is intent on showing global reach. And finally, and, frankly, I think, Senator Collins, you suggested this, quite disturbingly, that homegrown radicalized threat, self-radicalized threat, still persists. Also persisting is the question about what constitutes an appropriate, lawful, and effective response from us.

We are seeing this same thing play out in the cyber domain where the threats are all too obvious but, frankly, where our response is very late to need. I know this Committee knows more than most what we are losing out there in terms of state secrets, private information, and intellectual property being stolen by foreign governments; how much of our wealth is being pilfered by criminal gangs; and how much of our infrastructure is now vulnerable to cyber-enabled malcontents and anarchists.

And here our response—and I know you know this—is even slower and more difficult to organize than we have seen in the fight against terror. There are some who fear regulation being too burdensome. Others fear a loss of civil liberties. And yet all of us should fear the loss of privacy, ideas, jobs, and wealth that is going on right now.

As we encountered 10 years ago in the fight against terror, the old forms do not fit. They do not fit the new cyber dangers. But here, absent that catastrophic stimulus of a 9/11, we are moving very slowly to adapt to new realities.

Now, as you suggested, Senator Collins, there are other dangers out there, and I know we are going to touch on transnational crime. But, again, I am trying to suggest the immediacy of all of these—terror, cyber, and transnational crime—and why it is so threatening today, is this new effect of globalization.

Our response has to be synchronized, and the challenge is we have optimized our institutions across all three branches of government for a different world, and now we have to undertake the same tasks our political ancestors undertook over two centuries ago. How do we best secure our safety and our liberty in our time?

This Committee has been relentless in its efforts to answer that question in a way consistent with our enduring values, and I congratulate you on that.

It is hearings like, frankly, what we are doing today that help push this necessary debate forward.

Thank you again for the opportunity to contribute my personal views, and I know we will have more detailed questions as we go forward. Thank you.

Chairman LIEBERMAN. Thanks, General. That was really a perfect way to begin the discussion. I appreciate it. You raise a lot of questions in my mind which I look forward to asking you.

Mr. Jenkins, thanks for being here.

TESTIMONY OF BRIAN MICHAEL JENKINS,[1] SENIOR ADVISER TO THE PRESIDENT, RAND CORPORATION

Mr. JENKINS. Mr. Chairman, Senator Collins, and Members of the Committee, thank you very much for inviting me to address these important matters. I have prepared some written testimony, which I suspect will provoke some questions, but let me just highlight some of the headlines.

Looking ahead, the United States confronts a more diverse terrorist threat. Al-Qaeda, still our principal concern, is exploiting the turmoil created by the Arab uprisings to make tactical advances and open new fronts. Several incidents in the past year suggest a resurgence of Iranian-sponsored terrorism. South of our borders, Mexico faces what some analysts are calling a "criminal insurgency," which could expose the United States eventually to the kind of savage violence we have seen in that country.

The global economic crisis has sparked mass protests, which are entirely legitimate. But these in turn attract violence-prone anarchists and other extremists seeking venues and constituents. Anti-Federal Government sentiments have become more virulent, fueled in part by economic dislocation that transcends the current economic crisis, by long-term demographic shifts, and by deep national divisions and rancorous partisanship. For now, the anti-government extremists seem content to talk about armed resistance, but the hostility runs deep, and the potential for violence, long-term violence, is there.

[1] The prepared statement of Mr. Jenkins appears in the Appendix on page 86.

Let me come back to al-Qaeda. Al-Qaeda today is more decentralized, more dependent on its affiliates and allied groups and on its ability to activate homegrown terrorists. It is exploiting opportunities created by the Arab uprisings in Yemen, in the Sinai, in the Sahara, and most recently in Syria, where it can attach itself to local insurgencies and resistance movements.

Now, al-Qaeda's presence in a particular part of the world where it has not been before does not always present an immediate threat to U.S. security. While local insurgents may welcome al-Qaeda's brand name and assistance, this does not necessarily mean that they embrace al-Qaeda's war on the "far enemy." That is us. The longer-term threat is that al-Qaeda will be able to deepen relationships that ultimately give it new operational bases and recruits for international terrorist operations.

Its own operational capabilities degraded, unable to directly attack the West, al-Qaeda has emphasized—embraced, really—a do-it-yourself strategy supported by an intensive online recruiting campaign. They have had modest success. In fact, the meager response suggests that thus far this marketing effort appears to be failing. It is still a danger, but they are not selling a lot of cars.

Since 9/11, there have been 96 cases of homegrown terrorism involving 192 persons who offered support to jihadist groups or plotted to carry out terrorist attacks in this country. Of 37 homegrown jihadist terrorist plots since 9/11, 34 were uncovered and thwarted by the authorities.

Our success in preventing further terrorist attacks is owed largely to our own intensive intelligence collection efforts worldwide and at home, plus unprecedented cooperation among the intelligence services and law enforcement organizations worldwide. That latter aspect is going to become more difficult to sustain in the future, in part because of fiscal constraints, in part because of a certain amount of complacency, but also in part because we are going to be dealing with governments in the Middle East that are being challenged by their own citizens whose efforts we support in principle, and also we are going to be dealing with governments for which counterterrorism is no longer their top priority. It is new political institutions, it is the creation of jobs. We are going to be dealing with some governments whose leaders may have very different ideas about terrorism—for example, the recent statements by the new president of Egypt. This places an increased burden on our domestic intelligence capabilities.

Now, Senator Collins, I certainly agree with you that our domestic intelligence collection, although not optimized, certainly has been a remarkable success. It is, however, under assault, in part motivated by concerns about civil liberties, but also by personal, ideological, and political agendas which in some cases are further fueled by organizational rivalries.

Now, intelligence collection is always a delicate business in a democracy, and review is always appropriate. But the dismantling of the intelligence effort, which seems to be the politically correct desire of some, I think would be extremely dangerous.

The recent string of terrorist plots by Iranian-trained operatives in Azerbaijan, Georgia, India, Thailand, Kenya, and the United States, itself, I think indicate a resurgence in Iranian-sponsored

terrorism. Its future trajectory will depend on Iran's perceptions of Western intentions and its own calculations of risk. And, of course, the uncovering of a plot in this country I think really raises some questions about our calibrations of their willingness to accept risk.

Let me make a couple comments briefly about the terrorist targets and tactics. Terrorists have contemplated a wide range of targets: Government buildings, public transportation, hotels, tourist sites, and religious institutions predominate, but they remain obsessed with attacking commercial aviation, currently with well-concealed explosive devices that are difficult to detect, hoping to kill hundreds. I think that protecting airliners will remain a matter of national security.

But while terrorists consider airlines gold medal targets, when it comes to slaughter, they do their work on surface transportation, which offers easier access and crowds of people in confined spaces.

Let me just follow on something that General Hayden has said here, and that is, it is really a long-term trend that we are struggling with. We have known for some years that power—and here I mean power defined crudely, simply as the capacity to kill, destroy, disrupt, compel us to divert vast resources to security—is coming into the hands of smaller and smaller groups, into the hands of gangs whose grievances, real or imaginary, it is not always going to be possible to satisfy. And how we deal with that within the context of a democracy and remain a democracy I think is one of the major challenges we face in this century. Thank you.

Chairman LIEBERMAN. Thank you. Right you are. I think you both pointed to the changes that are affecting the nature of the threat. I am going to wait until the question period to say more.

Mr. Cilluffo, thanks for being here again. Good to see you.

TESTIMONY OF FRANK J. CILLUFFO,[1] DIRECTOR, HOMELAND SECURITY POLICY INSTITUTE, GEORGE WASHINGTON UNIVERSITY

Mr. CILLUFFO. Thank you, Chairman Lieberman, and not to soften you up for the question period, but I do want to say we all owe you a debt of gratitude in terms of your oversight on homeland security. It is really sad that these are the last rounds of hearings, but really we are pleased you have contributed so much to all of our efforts here.

Let me also say thank you to Senator Collins, a good friend and a big champion on these issues, distinguished Members of the Committee, and even those from other committees, which I think is really important in terms of Senator McCain, which, when you look at cyber, you cannot look at the world through the boxes and organization charts that make up our governments and agencies because these threats require us to look at it holistically. So when you talk cyber in particular, it obviously transcends any particular department and agency, but also any particular committee, so thank you, Senator McCain, for being here as well.

All too often, hearings along these lines are after a crisis occurs, what we "coulda, shoulda, woulda." I think it is really important that we take the time in advance—I guess it was President Ken-

[1] The prepared statement of Mr. Cilluffo appears in the Appendix on page 102.

nedy who said that the time to fix your roof is when it is sunny, not when it is raining. And I think it is important to be able to reflect, it is important to be able to recalibrate, because ultimately that is the objective here, to be able to try to shape outcomes.

Before jumping into the particular issues, I almost think that, General Hayden, maybe the NSA does spy because you guys, I think, hacked my system. You said everything I wanted to be able to say. So I will try to pick up on a couple of very brief points here.

I think it was Yogi Berra who said this—"the future ain't what it used to be." I would add some time since the end of the Cold War, threat forecasting has tended to make astrology look respectable. That said, the best way to predict is to shape, and I think we do have an opportunity to shape and are doing so right now.

It was Mark Twain, or Samuel Clemens at the time, who said, "While history may not repeat itself, it does tend to rhyme." And let me say we have some rhyming that is warrant for concern.

Senator Collins, you mentioned complacency. I am very concerned that complacency is setting in. That is stymieing some of the initiatives that could be moving at a faster clip and ought to be moving at a faster clip.

General Hayden, one point I may disagree a teeny bit with you on is whereas technology, tactics, techniques, and procedures continue to change and advance based on new advancements, human nature never changes. So to think that we are out of the woods right now would be a big mistake. And I get the sense that we are not necessarily recognizing that.

Ding, dong, the witch is not dead. Good news that we have had some very successful strikes against Osama bin Laden and Anwar al-Awlaki, I would say most significantly underdiscussed is Ilyas Kashmiri. He was one of these guys that cut across all the jihadi organizations. And the threat today comes in various shapes, sizes, flavors, and forms, ranging from al-Qaeda senior leadership that has proven to be resurgent, able to pop up again, is resilient, so let us not take our eye off the ball there; but also to its affiliates that are growing by leaps and bounds. Whether it is AQAP, home to one of the world's most dangerous bomb makers, Ibrahim al-Asiri; al-Qaeda in the Islamic Maghreb spreading all throughout the Sahel; al-Shabaab in Somalia; or across Africa, you are seeing fall under an arc of Islamist extremism right now, from east to west. I mean, Timbuktu, who would have thought that would fall to Islamist extremists, but it has. So all the news is far from good.

One of the more concerning trends when you look at some of these organizations, historically they had very indigenous, regional, and local objectives. More and more they are ascribing to al-Qaeda's goals, to the broader global jihad, and who is in the crosshairs? Obviously, the United States, Israel, and India—the West generally. So that warrants additional concern.

Then let us look at the Federally Administered Tribal Areas. We have had major success here, but do not think it is happening in a vacuum. It is because we are applying pressure, continuing to apply pressure. If we take a foot off the gas pedal, you are going to see instantaneously our adversaries re-emerge. Think of it as suppressive fire. They are looking over their shoulder, spending less time plotting, less time training, and less time carrying out at-

tacks. So as much as we can—and I know drones are not the complete answer, but I think some of these approaches have been very successful in terms of some of our counterterrorism opportunities.

Pakistan, a big issue. You see a witch's brew of terrorist organizations there, from Tehrik-i-Taliban to Harkat-ul-Jihad al-Islami (HuJI) to the Haqqani Network, which I think should be designated a foreign terrorist organization (FTO)—if you guys are jumping into that—to a number of other organizations. So when you look at the threat, by no means gone.

Then, as Mr. Jenkins touched on, the homegrown threat. I take a little different perspective than perhaps Mr. Jenkins does. I think it is very significant. We have seen 58 plots, according to the Congressional Research Service (CRS), that have been disrupted, ranging from very sophisticated plots, such as Najibullah Zazi, down to less sophisticated. But at the end of the day, let us keep in mind terrorism is a small-numbers business. You do not need big numbers to cause real consequences. Nineteen hijackers—look at the impact they had. And to me, the missing dimension of our counterterrorism statecraft is, to paraphrase Bill Clinton, it is not the economy, stupid—or maybe it is—but it is the narrative, stupid. We have not done enough in combating violent Islamist extremism to go after the narrative, the underlying fuel or blood that makes the system fly.

So we need to expose the hypocrisy, unpack, dissect, and attack that narrative, expose it for what it is. It is ideologically bankrupt. And I would argue that part of that is also looking at—I see we have a good friend of mine here, Carie Lemack, and others—the role of victims. Why do we know all the martyrs, why do we know all the terrorists, why don't we know al-Qaeda's victims of terrorism? To me that has to be part of the equation. So defectors, disaggregate, deglobalize, and ultimately remember the victims.

Two words on cyber. I know I am over time. I have never had an unspoken thought. I think it is fair to say in terms of cyber we are where we were in the counterterrorism environment shortly after September 11, 2001. We do not need any more examples, anecdotes, and incidents to be able to wake us up. What we do lack is strategy, and I may disagree with everyone here, and am probably a minority position, but I do not feel we can firewall our way out of this problem. Yes, we need to get security high enough, we need to raise the bar, but to me we need to ultimately communicate a clear and articulated cyber deterrent strategy aimed to dissuade, deter, and compel our adversaries from turning to computer network exploit, espionage, or attack. We have now named names: China, Russia. We have all known this for a long time. But what are we doing to compel them to stop continuing what they are doing?

To me, it is about investing in some of our computer network attack capabilities. We need the cyber equivalent of nuclear tests that ultimately demonstrate a need to respond. And critical infrastructure. If anyone is doing the cyber equivalent of intelligence preparation of the battlefield, that is not for stealing secrets. That can only be as an advance equivalent of mapping our critical infrastructure that can be used in a time of crisis. Completely unaccept-

able. I hope we can act on legislation, and information sharing is critical, but we need to go the next step as well.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much. Cybersecurity legislation, as you know, is the No. 1 priority of this Committee, and hopefully the Senate will take up the bill soon, and we will have a good and open debate and get something done.

Mr. Flynn, great to see you again. Welcome back. Please proceed.

TESTIMONY OF STEPHEN E. FLYNN, PH.D.,[1] FOUNDING CO-DIRECTOR, GEORGE J. KOSTAS RESEARCH INSTITUTE FOR HOMELAND SECURITY, NORTHEASTERN UNIVERSITY

Mr. FLYNN. Thank you very much, Mr. Chairman, Senator Collins, and other Senators. It is an honor to be here. As I went back to prepare for this testimony, I reflected on my first time appearing before you, Mr. Chairman. It was when this was still the Governmental Affairs Committee, and it was literally a month after Sepember 11, 2001, on October 12, 2001. And at that point, I concluded my testimony essentially arguing that we need to fundamentally rethink and reorganize how we provide the security for this Nation in this new and dangerous world. And you, Mr. Chairman, have really taken up that mantle with Senator Collins, and I really want to express my gratitude for the enormous service you have done to this Nation over the last 10 years. I am honored to be here at this hearing.

I am now here in my new capacity as the founding co-director of the Kostas Research Institute for Homeland Security, made 10 years after 9/11 as a result of a very generous gift from a graduate and trustee from Northeastern University, and I was honored to take on this role at a university that has made security one of its three focal areas for research. That I think speaks to the greatest strength of this country that we have not yet really tapped, which is the everyday citizens who are out there, who are patriotic and willing to give, and also our universities that have largely been missing in action unless we have bribed them into it to play an effective role. In the Second World War, we harnessed the best talents we had across our Nation, from our civil society to universities that mobilized for the war. Today, to a large extent, civil society has been left on the sidelines.

When we come to today's hearing topic on the nature of the threat, I would certainly suggest that what we have heard so far and what I think we are going to continue to see in terms of evidence going forward is we really need to recalibrate, to have that engagement with civil society happen with a greater order of magnitude.

What do we know? We know essentially that there are limits to the war on offense. That was pretty much the approach we took in the immediate aftermath of 9/11. We even used the terms often of "we do it over there so we do not have to do it here," and "the only defense is offense." That effort, certainly a case can be made, has helped to protect this country from another 9/11 scale attack, but it does not and did not succeed at eliminating the threat.

[1] The prepared statement of Mr. Flynn appears in the Appendix on page 114.

The reality is now the threat has morphed into the more smaller-scale attacks that have one key attribute highlighted by the testimony we have heard so far that I think should give us a little pause, which is they are almost impossible to prevent. These smaller-scale attacks, particularly with homegrown dimensions, essentially do not hit enough tripwires. They are really not that sophisticated. They can be done relatively nimbly and quickly, so it means we are going to have them from time to time.

The second thing we know is that al-Qaeda is not the only threat that we need to be dealing with to the homeland. What we also have, with the example of 9/11, is the illustration of how warfare will be waged against the United States in the 21st Century. This is a country that is so dominant on the conventional military realm, it is just insane for an adversary to want to take on our second-to-none armed forces. The future battle space, therefore, is in our civil and economic space, with the critical infrastructure that underpins the great strength of this Nation. That genie came out of the bottle on 9/11, and we see it primarily in terms of the current threat environment in the cyber realm, where, through the use of cyber attacks on critical infrastructure, we are not only talking about disruption of service but sabotage of those key components with loss of life and huge economic losses.

Any current and future adversary of the United States will essentially gravitate to wanting to target the critical infrastructure that underpins the power of this country, and we have to think about defensive measures to deal with that.

The other key hazards that we definitely face that falls under the homeland security mission are always clear, always present, age-old; they are natural disasters. In the big scheme of things, one it is hard put in some cases to come up with a terrorist attack that can come close to causing the loss of life and disruption of property as what Mother Nature can throw our way. And in that regard, we have to be prepared to deal with natural disasters because we cannot prevent them.

Now, what is the implication arising from the fact that we have smaller attacks that are more difficult to prevent, a growing asymmetric threat largely through cyber that we have to defend against, and the ongoing risk of natural disasters? It is that we really have to take homeland security very seriously and not imagine, as General Hayden also pointed out, that all threats can be managed beyond our shores. We have to manage them here at home.

How do we go about doing that? I argue that three key ways are important. One is we have to reset some expectations with the American public. There are limits to what the Federal Government can do to prevent every possible hazard, and responding to them is all-hands evolution. We have to say frequently and often that bad stuff is going to happen from time to time, and the measure of an individual's character as well as our Nation's character is how you cope, not necessarily that you prevent every bad thing from happening. Overcoming adversity has always been part of our national DNA, and it is something that we are going to continue to need as we move forward.

The other is this real tension over secrecy—and, Senator Collins, you certainly highlighted it—about the leak issue. On the one

hand, you cannot engage civil society unless we are more forthcoming about threat, about vulnerability, and, very importantly, what it is we all have to do. So we really have to figure out how we not keep everything in a cone of silence, but we really push the envelope on pushing information out. These small attacks have almost always been broken up by locals or by citizens. We have to make them a part of the solution.

And the last thing I suggest is that an overarching focus going forward is this concept of resilience, of building a more resilient society. In a world where there are no risk-free zones—and I have yet to find one—it will be the communities, the companies, and the countries that are best able to manage risk, to withstand it, to promptly respond and recover from it, and to adapt to it that will be a competitive advantage over everybody else. People will not invest in and live in places that when they get knocked down, cannot get back up. They will live in places that can manage risk very well.

America historically has done that, and we need to harness that capability again, and the focus has to be around individual resilience, our self-sufficiency, self-reliance, character that was very much a part of our Nation's blood, our companies, our communities. It is, in other words, a bottom-up effort that we need to be engaged in versus a top-down one. And taking on this effort, I would argue, has a remarkably beneficial effect. It reminds us why we come together as communities in the first place, because there are some problems we cannot manage all by ourselves. And it turns out that we have to work together as a society in order to nail down these problems.

So a call to the American people is necessary because the threat and the ongoing hazard risk necessitates the engagement of the private sector and necessitates the engagement of everyday citizens and companies. We need to move away from essentially a largely offense-based and largely overreliance on Federal capability and not one that engages on the lowest levels.

I just want to finish with a final number to help us put this all in context on the away-versus-home sort of investment.

If we take the rough number of the cost of war operations since 9/11, the number that is used is roughly about $1.3 trillion. That is what we have invested in those war operations to make this country a bit safer. Well, that turns out to be a burn rate of $350 million a day every single day for a decade, $15 million an hour every hour, 24 hours a day for a decade. Fifteen million dollars is the highest we have spent as an annual investment in Citizen Corps, which is a program designed to get everyday citizens to play a voluntary role in supporting front-line first responders. That is one hour of our investment in war operations in a decade.

I think we need to put some resources where the need is, and that is in how we basically make our Nation a bit more secure in defense and preventing and prepare to dealing with the kinds of challenges that are facing us today.

Thank you so very much, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Mr. Flynn. Again, an excellent statement. And I agree with you. We have found in some ways, through the See Something, Say Something programs that

began in New York, a way to involve the citizenry, and it has been effective. But we have only begun to do that here.

We will do 7-minute rounds of questions.

General Hayden, I will start with your evocative beginning and ask a question that is either an overview of the philosophical or even strategic stakes. You said that ". . . most of the attributes of the age of industrialization made the state stronger and more relevant. Most of the effects of today's globalization make the state weaker and less relevant." I presume that within the term "globalization"—I know you are quoting General Scowcroft, or paraphrasing him—that he must have meant digitalization, information technology, and the whole array of modern technological development.

General HAYDEN. I think he did, Senator, and that actually might be the best poster child for the whole process.

Chairman LIEBERMAN. Yes.

General HAYDEN. But it is just not confined to that. Look at manufacturing.

Chairman LIEBERMAN. Right.

General HAYDEN. You pull the question of supply chain issues in a global economy. It is impossible to build even critical systems in an autarchic sort of way in which you have control over everything. Everything has just gotten so much more interconnected that it allows, again, actors that were very small, self-motivated, as Mr. Jenkins pointed out, and cannot be satisfied. A degree of destructive power that we have just never experienced.

Chairman LIEBERMAN. I agree. So let me make this statement and then ask you to respond. Certainly in terms of the threat to us, as you just cited Mr. Jenkins, small groups, non-state actors, like we saw on 9/11 and since, can do great damage to us. But I want to just mention this irony, and I think you are right that the developments of digitalization and globalization, "have made the state weaker and less relevant." And notwithstanding the exchange I just had with Mr. Flynn about the citizens' responsibility, it is the state ultimately that in our country still has the constitutional responsibility to provide for the common defense.

So really part of what I hear you saying, paraphrasing General Scowcroft, is that the state has to figure out how to get in the new game in a defensive way, how to protect the citizenry, which is our fundamental responsibility in the Federal Government.

General HAYDEN. Senator, that is exactly the message I was trying to lay out. The effects of the broader environment work against state power, make it more difficult for states to influence events for a variety of reasons. It does not change the moral, political, or legal responsibility of the state to protect its citizens, and that is precisely the dilemma we now have.

I will use an example. We are very sensitive in this country because of our political culture and—God bless us, I believe in it strongly—foreign and domestic intelligence and law enforcement that protected our liberties very well, and the threat to our security that created for two centuries, not so much. Now it does. And so we now need a new formula.

I am sure Senator McCain is very aware of this. Getting NSA involved in terms of defending something other than "dot-mil" Web

sites seems to be an obviously clear thing to do because of its capability. But our old structures work against that. It is very difficult for us to digest that institution assuming that new role.

Chairman LIEBERMAN. You are absolutely right, and, in fact, that is exactly what we are dealing with now in the cybersecurity legislation because you really want NSA, which has traditionally, and still does largely, had responsibility for protecting the country and operating overseas, protecting us from overseas attack, but then you have DHS with a set of responsibilities for homeland security, and now the FBI with law enforcement responsibilities. We have a challenge of how we break through the traditional stovepipes and get them all at the table together to protect our security against state actors and non-state actors in a cyber world is a challenge we have. I appreciate that exchange.

Let me ask one of those questions we tend to ask, which is I would ask you to be much more simplistic than I know you want to be, but I want to ask each of you. Tell me what you would say today are the two or three, your choice, most significant threats to our homeland security. And then give us a guess—and I agree with what Mr. Cilluffo said, that prophecy in this area is pretty close to astrology. But give us your guess about whether your ordering of the threats to our homeland security will be the same 5 years from now or 10 years from now.

Mr. FLYNN. Senator, I will begin with the one I have been testifying for a long time before this Committee about, which is I think the ongoing vulnerability of the intermodal transportation system profound disruption. I think the fact is while some measures have been put in place to improve the ability for it not to be used essentially as a weapons delivery device, that threat still exists. My concern is not so much the successful attack, which is certainly quite worrisome, but it is that the only tool in the tool bag likely is to throw a kill switch to sort it out afterwards and then try to figure out how to restart it. And what we will have, basically, is a meltdown of the global economy in the interim. So what we have there in short is a very critical system infrastructure that currently is quite fragile if we are spooked, and more work I think needs to be done there.

Chairman LIEBERMAN. So that would be by a terrorist bombing or by cyber attack.

Mr. FLYNN. Yes, there are two sides there, I guess. For that one, it is essentially the bomb in the box scenario that basically gets everybody looking at trains and worried.

Chairman LIEBERMAN. Right, a traditional terrorist attack.

Mr. FLYNN. Then my next would go to highlight the cyber threat, like a cyber attack on the grid, because everything requires electricity. We have some huge vulnerabilities with industrial control systems across all our critical infrastructure, and that one is, I think, a newer one that we need to really step out smartly on.

Chairman LIEBERMAN. Thanks. How about your guess about whether that ordering will be the same 5 years from now?

Mr. FLYNN. Well, I think on the current trajectory in terms of dealing with the cyber threat, our government response does not look like it is going to get any better. I worry unless we have a

large incident that motivates some change—both of these problems are solvable in the next 5 years.

Chairman LIEBERMAN. Right.

Mr. FLYNN. The question really is our actions, not necessarily those of the terrorists.

Chairman LIEBERMAN. That is up to us,

Because my time is up, I am not going to even ask you to be more simplistic. Just give me your two or three top ones and whether you think they will change in 5 years, Mr. Cilluffo.

Mr. CILLUFFO. I agree with Mr. Jenkins and General Hayden. Al-Qaeda senior leadership, and those that are in one way or another affiliated with al-Qaeda are still No. 1 right now.

Chairman LIEBERMAN. Right.

Mr. CILLUFFO. No. 2, and based on consequence, not necessarily likelihood, but if you were to break out the risk management, I would put the government of Iran and other countries that may look to asymmetric forms of attack that can have catastrophic implications. So I would not discount state sponsors of terrorism, looking to proxies and the convergence of crime and terrorism. I mean, this is scary stuff. Who knows who is exploiting Anonymous even?

Chairman LIEBERMAN. Right.

Mr. CILLUFFO. If it is foreign intelligence services or other organizations.

Chairman LIEBERMAN. Same 5 years from now?

Mr. CILLUFFO. I actually think on the terrorism threat, I am hoping our actions will mitigate that. I think cyber and nation-states and their capabilities———

Chairman LIEBERMAN. Will become a greater threat. Mr. Jenkins.

Mr. JENKINS. I am not nationally recognized in the field of prophecy, so I am going to be very cautious about——

Chairman LIEBERMAN. But we will convey that authority on you officially today. [Laughter.]

Mr. JENKINS. I am not going to try to identify the group or the event, but rather I'll talk about something really internally on our side, and that is our psychological resilience.

Look, terrorists cannot win by force of arms. They can hope only to create terror that will cause us to overreact or destroy our own economy or sap our will, and that makes our determination, our courage, our self-reliance, our sense of community part of the assessment, and these are really difficult to measure. But there are some vulnerabilities here in terms of our tendency to overreact and the divisions that we have in our own society.

So I really look internally and say, "What really can we do"—as Mr. Flynn and the others were saying—"about really strengthening our own capacity, not just our physical capacity but our psychological capacity?"

Chairman LIEBERMAN. Right.

Mr. JENKINS. And I think that is going to remain the same. I hope it does, because there are some trends that say some of these divisions in our society are going to get worse.

Chairman LIEBERMAN. Well said. I agree. General Hayden.

General HAYDEN. Senator, I would agree with all that, and let me just add one. If you look at dangers in the cyber domain, the actors, the sinners, you have criminals, anarchists—now often called hacktivists. States are generally stealing our stuff, and I know some states can be very dangerous, and they are very capable. But, in essence, a state has to judge whether or not they are making themselves vulnerable to retaliation.

Criminals are stealing our money. They are in a symbiotic relationship with their target. Parasites are generally not motivated to destroy their hosts so they do not bring about catastrophic damage. I am really worried about that third layer, the anarchists or the hacktivists. They are currently the least capable, but as time goes on, the water level for all these ships is rising in the harbor. So imagine a world in 2, 3, or 4 years in which the hacktivist groups, the ones that cannot be deterred, who cannot be satisfied——

Chairman LIEBERMAN. You are talking about cyber attacks?

General HAYDEN. Yes, sir. Those that cannot be deterred, cannot be satisfied, begin to acquire tools and skills we associate with nation-states today, and I think it gives you some sense of how dramatic that threat can be.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

General Hayden, I want to draw a distinction between what Mr. Flynn said about the need for more citizen involvement versus the leaks that I think have made it more difficult for our country to defend ourselves against both current and future threats. I certainly agree with Mr. Flynn that an alert citizenry in many ways is our best defense. We have seen that over and over again. The Times Square Bomber, for example, was caught by an alert street vendor. The Chairman and I are the authors of the See Something, Say Something law that applies to the transportation sector.

But it seems to me that is very different from leaks from within agencies, from within the Administration, perhaps from within the White House, that reveal highly classified information, may compromise sources that are working with us, and that, for example, identify the President's personal role in targeting terrorists.

Could you comment on the impact of these national security leaks, of which there have been a great many recently, on our ongoing counterterrorism efforts as well as our larger effort to stay ahead of those who would do us harm?

General HAYDEN. Senator, as I think Mr. Flynn pointed out, this is a hard question in a democracy, but let me take the negative side first and then maybe treat very briefly some of the dialogue that might be more appropriate and proper with regard to what espionage services do or do not do.

I think the single greatest toll on us by the unauthorized disclosure of information—for whatever purpose, even for policy reasons that may have some legitimacy or political reasons that are understandable, if not forgivable—is the confidence in potential partners in working with us and their belief that we can be discreet. And that works down to the guy on the street who is going to betray the organization of which he is a part, only if he has confidence that you can keep that relation secret, to the foreign intelligence service who might be willing to do something very edgy with you,

lawful, certainly, but politically very edgy in our government and in their government, they will only do it if they can count on your discretion

Let us use one that was authorized, one I am very familiar with. The Administration decided several summers ago to release the Department of Justice memos when it came to the CIA detention and intelligence program. A separate question, something fully within the ability of the President to do. That is not the issue. But that was over the objection of the then current CIA Director and six of his predecessors. I can imagine intelligence chiefs around the world saying, "When I meet with that person and he gives me assurances of secrecy and discretion, it is now clear to me that he does not have absolute control over that process inside the American political system." That is the dilemma we face.

Now, to echo something that Mr. Flynn said earlier, though, when I came to NSA in 2000, I actually tried to make some of what the Agency was doing more public, and the reason I did that was I did not think the American people would give us the authority and the resources to do that which I thought we had to do without having a greater comfort level with regard to what the Agency was, with whom it was populated, and how it deeply respected American privacy. So there is this need to have this dialogue.

Let me end with this, Senator. I had a panel of outside experts, a board of advisers at the CIA. I gave them tough problems. The toughest problem I gave them was this: Can America continue to conduct secret espionage in the future inside a society that every day demands more transparency and more accountability from every aspect of national life? And that is where we are. That is where the dilemma is.

Senator COLLINS. I would say that I think there is an easily drawn distinction between educating the American people about the threat generally, the role played by various Federal agencies, the need for certain authorities versus getting into the details of specific counterterrorism actions that may compromise the agent involved—I think of that poor physician in Pakistan, for example, who is now in jail; I think of other cases more recently that have occurred in Yemen—and also would jeopardize, as you said, the willingness of foreign intelligence services to work with us, to trust us not to reveal the details in a way that may compromise their government politically or may truly put in danger sources and methods.

General HAYDEN. I agree totally, Senator.

Senator COLLINS. Thank you. Mr. Cilluffo, I want to get back to an issue that you touched on which I think is so important, and in some ways it contradicts a little bit or takes a different view from Mr. Jenkins' testimony in which he talks about a failure of al-Qaeda, a marketing failure, to spread its ideology in a large-scale way.

You, on the other hand, were critical that there is a lack of a strategy to counter the narrative that inspires people, whether as larger groups or countries or as individual lone wolves. And this is an issue that the Chairman and I have brought up over and over again with the Administration, the failure to appoint a point per-

son to come up with a narrative, the failure to recognize the term of Islamist extremism within our country.

What do you think we should be doing to more effectively put out a counter-narrative to help dissuade young people in particular who may be drawn to the radical perversion of a great religion, Islam, that they are seeing on the Internet?

Mr. CILLUFFO. Thank you, Senator Collins. I do not want to suggest we are completely out of step in some of this thinking, but I do think our efforts to address the counter-narrative and counter-radicalization in countering violent extremism (CVE) is lacking at best. In fact, I think that is the missing dimension of our counter-terrorism statecraft right now. We are having major successes kinetically. We have to continue to do that, but it needs to be a full complementary approach, all instruments of statecraft. And let me also note that I very much supported the letter you and the Chairman sent to Mr. Brennan in terms of the release of what could very liberally be called the CVE strategy.

My view—this is personal, and I am not sure everyone else will see it this way. It is about going negative. It is not about what is great and this, that, and the other thing. Think of a negative political campaign, expose the hypocrisies, expose the lies, and illuminate the seamy connections to drug traffickers. It really is kind of frustrating that the country that invented the Internet, the country that is home to Madison Avenue, the country that is Silicon Valley is getting our butts kicked in this space.

So I would feel we need to be able to—rather than try to look at—just expose the negatives and then bring up the defectors. There have been so many defectors of al-Qaeda who are going to have much more resonance, they are going to have more balance, or street cred, as my kids might say, with the community than any of us will simply because they have come out. They have made the arguments justifying acts of—well, they should be—we should have a Web site where you can get all of that. And then it is not because Carie Lemack is here, but the victims are so important, and why don't we know their stories? Why don't we know their dreams? Why don't we know their lives' aspirations? We simply do not.

So this is not to be pejorative, but we need a Facebook of the dead. We need the equivalent of all these voices, all these dreams—faces, visuals, and pictures, not nouns and verbs, actual visuals. And I think that to me has been lacking. The State Department is doing some decent work at the Center for Strategic Counterterrorism Communication right now, but more needs to be done.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. That was a great answer. Thank you. Thanks for mentioning Carie Lemack. I join you in welcoming her. If it was not for her and a lot of the other survivors of 9/11, we probably would not have passed the Homeland Security Act in the first place and would not have created the 9/11 Commission and would not have passed the 9/11 legislation.

Second, your reference to negative campaign advertising is very—it is relevant.

Mr. CILLUFFO. I am all for that.

Chairman LIEBERMAN. It is relevant. So maybe what we should do is form a Super PAC to begin to negative advertise against Islamist extremism.

Mr. CILLUFFO. Sounds good to me.

Chairman LIEBERMAN. I have one or two people I can think of who might contribute to that.

I apologize to my colleagues because my late arrival may have affected the order somewhat because our rule is that we call in order of seniority on the Committee before the gavel, and then after the gavel in order of arrival. So for your information, the order is Senators Carper, Coburn, McCain, Johnson, Brown, and Pryor.

Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. I want to commend you and Senator Collins on assembling really an exceptional panel, and we thank you each for joining us again today and for your testimony and for your responses. This is really time well spent.

I have been slipping back into the anteroom here a couple times during the hearing. We have a group of soybean farmers from the Delmarva Peninsula, and to go back to the point that you raised, Mr. Flynn, we are experiencing a drought on Delmarva, high temperatures, no rain for some time, and it is not just a drought in our part of the country, but it is apparently a nationwide drought. And the threat that poses to our homeland, to our economic security, is really significant and could be severe.

I mention that because the nature of the threats to our country tend to change over time. The war that Senator McCain and I served in in Southeast Asia, the kind of threat and the way we fought that war was different than the war that my Uncle Ed fought in Korea a generation earlier. The Persian Gulf War was different from what we did in the Vietnam War. And the war in Iraq is different from really the Persian Gulf War, although the terrain was pretty much the same. In Afghanistan, it is different still.

We figured out, thanks to people like David Petraeus, how to be successful in Iraq and I think how to be successful in Afghanistan. And we need to figure out how to be successful in this next threat that we face, growing threat that we face, and that is cybersecurity.

This is a panel where, as you know, we get along pretty well here, Democrats, Republicans, occasionally we let in an Independent. [Laughter.]

But we work well on this Committee, and the fellow to my left here, a dear colleague, and the fellow over there, are close friends, and they have a different take on what we ought to be doing on cybersecurity legislation. And we are not going to have a better panel, I suspect, than what we have right now to help us find a little something closer to common ground.

I am going to start with you, General Hayden. Looking at the legislation that Senator Collins and Senator Lieberman have introduced with the support of a number of us, how do we make it better? How do we make it better in terms of more effective, and how

do we make it better in terms of getting something done politically so that we can help address this threat?

One of our dear colleagues is Senator Michael Enzi from Wyoming. He has something called the 80/20 rule. And I said, "What is the 80/20 rule, Michael?" Several years ago, I was talking about him and Senator Kennedy working so well together, and he said, "Ted Kennedy and I agree on 80 percent of this stuff. We disagree on 20 percent of this stuff. And what Ted and I have decided to do is focus on the 80 percent on which we agree."

Now, I do not know in cybersecurity if we should have an 80/20 rule or 70/30 rule or a 60/40 rule, but we need to get something done here this year, and we cannot go home without completing action. And if we only do 60 or 70 percent of the deal, that is a lot better than nothing.

General Hayden.

General HAYDEN. Yes, sir, I will be very brief and probably overly simplistic. I would do it all. I do not view these fundamentally to be competing bills. I would get NSA in on the field. I would try to get standards into our critical infrastructure. And I would take Congressman Mike Rogers and Congressman Dutch Ruppersberger's bill about information sharing, and I would do that, too. I think they are all steps in the right direction. And we can adjust fire in a year or two. With clear, close, and conscientious oversight, we will make adjustments. But sitting here freezing ourselves into inaction is—I hesitate to say any course of action is better than standing still, because obviously there are some that could be very destructive. I do not view any of these in that light at all. I think they will all move in a positive direction, and we can make adjustments as needed.

Senator CARPER. I am going to ask you to say that again. Mr. Chairman, Senator Collins, I am looking for some common ground with Senator McCain over here and the renegade group that he is running around with. But I just said it to General Hayden—Where is the common ground? Where does it lie? And he gave us about one minute that was very insightful.

General HAYDEN. I would do them all. We need NSA in on the field. We really do. We need information sharing. The bill coming out of the House Intelligence Committee, Chairman Rogers and Congressman Ruppersberger, we need standards for critical infrastructure, check, check, check. I would do it all, and I would keep an open mind, and I would adjust fire 1, 2, or 3 years into the future as each of these begin to roll forward.

Senator CARPER. All right. Mr. Jenkins, any thoughts or reactions to that or other thoughts that you have, please?

Mr. JENKINS. No, I certainly would agree with that. Look, we are dealing with a technology that moves at about 150 miles an hour here. Legislation moves at about 15 miles an hour. And our adversaries are somewhere in between. They move very fast and exploit vulnerabilities with the new technologies as fast as they come out. And we spend a long time trying to catch up with them.

The longer we delay in implementing these things, the greater that gap grows. In that particular case—I guess you are going to have two former soldiers here that are agreeing—you do something now. It is not going to be 100 percent right. And you watch it care-

fully, and then you make adjustments as you go forward. So get these things moving, as opposed to waiting to try to find the absolute perfect piece of legislation, and by the time we do that, the technology is going to be 1,000 miles ahead of us.

Senator CARPER. Thank you. Mr. Cilluffo, please?

Mr. CILLUFFO. Senator Carper, I think it is an important question. It is a significant set of issues. I do feel you can meld the various pieces together. There are some areas of that 20 percent of disagreement that are not trivial. But I do not see them as mutually exclusive either/or propositions.

A couple of fundamental things. One, it is not about regulation. It is about building standards, self-initiated, that the various sectors can identify. I kind of feel like it is kids' soccer, and I have a daughter who just made it to the finals in regionals, so they get better when they get older, I promise you. But when they are younger, they all swarm the ball. So at the end of the day, let us not look at the technology du jour. But I can tell you this. If we do not act now, whatever is going to come after something occurs will be much more draconian, and it will not be as constructive as I would argue it could be.

Two, the other thing to keep in mind, we are very reactive. The cyber domain is very much reactive. There is nothing in prevention. We need active defenses. We need to look at deterrents. We need to enhance our offensive capabilities. We need to do so in a way that articulates but does not compromise operations and secrets, to Senator Collins' point. We have not done any of that, which to me is a little frustrating.

So the time to act is now. Long on nouns, short on verbs. Let us get it done.

Senator CARPER. Thanks so much. Mr. Flynn.

Mr. FLYNN. I just want to emphasize again that we will need standards, and the debate really has got to be about just how we can achieve those. We have a number of models, and they are not all regulation, but we need standards, and we need incentives for standards. So let us just move forward on that.

I would suggest a piece that could be quite helpful in getting to a mature end state is missing, which is engaging universities to be a part of the solution. We talk about private-public cooperation, but completely missing from this is the role of universities. A consulting professor out of Stanford University, literally as something is going up on the white board, is thinking about how to market it. The government is coming in multiple years later. The universities are creating some of the problem, but we are trying to retrofit to fix. Let us get them engaged. They can be helpful, honest brokers. They can bring some expertise. And they try to change the culture that you need, or we all need, to be mindful of the risks that are associated with cyberspace. And I do not see much role given to universities a part of the legislation, and I think anything could be added to that. They are one of the few institutions Americans still somewhat respect, so let us get them in the game and make sure that expertise and some of that honest broker role, I think, can be harnessed.

Senator CARPER. Good. Those are very helpful responses. I would just say to my colleagues, Senator Lieberman and I, and probably

Senator Collins, have talked with the Majority Leader just in the last 24 hours about how do we move forward. He has committed to bring cybersecurity legislation to the floor during the course of this work period, and it is imperative that we do that. He is reluctant to provide an unending amount of time. We cannot spend a week or two doing this. But to the extent that we can take some of what you said here today to heart and to enable us to quicken our pace, maybe get something done, we can make very good use of that week, and we need to.

Chairman LIEBERMAN. Thanks, Senator Carper, for your line of questioning, for what you said. Thanks to the witnesses for their response. It was interesting to me that in the response to my questions about the threat to homeland security today and what it would be 5 years from now, there is a clear presence in your answers of the cyber threat and the extent to which you feel it will grow. So we really have to act. We have a chance to act thoughtfully this year, to begin something so that we are doing it not reacting to an attack in which, I agree, what we do in reaction will be much less well thought out. And I agree, we have to find a way to do it all, do information sharing and do standards as well.

Senator CARPER. Mr. Chairman, could I just have another 30 seconds? I will be very brief.

Chairman LIEBERMAN. Sure.

Senator CARPER. Some people think we do not get much done around here. Just in the last 7 months, we have actually agreed on bipartisan legislation on the Federal Aviation Administration reauthorization; on patent reform legislation; free trade agreements with three major countries, trading partners; Export-Import Bank reauthorization; the so-called Jumpstarting Our Business Startups Act to improve access to capital; transportation legislation; Food and Drug Administration reform; and flood insurance. We passed a good postal bill in the Senate, and a good agriculture bill. That is a pretty good track record. And what we need to do, I think, in the Senate, is to try to set the example for our colleagues in the House and just to get something done.

Chairman LIEBERMAN. Thanks, Senator Carper. I know that Senator McCain is inspired by your statement. [Laughter.]

And I could see the smile on his face. You made him very happy with that report. Senator McCain, welcome.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Dare I point out that we have not done a single appropriations bill? Dare I point out that we have not done the defense authorization bill? Dare I point out that we have done literally no authorizing bills with the exception—12 bills have been passed by this Congress. That is the least in any time in history. But we will continue that debate at a later time.

Chairman LIEBERMAN. Senator McCain, you are up. Senator Coburn was next, but he had to leave.

Senator MCCAIN. Thank you, and I appreciate the enthusiasm and the positive attitude of my dear friend from Delaware.

First of all, my friends, in all due respect to your comments, I have been around here 25 years, and I have grown to believe over time that the Hippocratic Oath is the first thing we should observe:

First, do no harm. I have seen legislation pass this body that has done a great deal of harm, so when you say do something, one thing we should not do is not get it right. And one of the things we should not get wrong is giving the Department of Homeland Security the authority to issue a blizzard of regulations unchecked and unmonitored. Also, information sharing has to be done. You mentioned the universities. How about Silicon Valley? They are the people that really know how to react rather than the Department of Homeland Security. The next time you go through an airport, you will go through the same procedure that you went through right after September 11, 2001. So my confidence in the Department of Homeland Security to be the lead agency is extremely limited.

With that, I would like to move on quickly. General Hayden, would you say that these cyber leaks about Stuxnet and these others is a significant blow to national security as well as our relationship with other nations?

General HAYDEN. Senator, the common denominator is the blow to relationships with regard to discreet relationships, the lack of confidence. That has to be very painful, and we will suffer for that over the long term.

Each of the leaks in terms of its specific harm had a different effect. The one about how we do or do not do drone activity, for example.

Senator MCCAIN. I am specifically talking about cyber.

General HAYDEN. On cyber, whether the story was true or false, a publication that the United States was responsible for that activity is almost taunting the Iranians to respond at a time and in a manner of their own——

Senator MCCAIN. I was just going to say, if I were the head of Iranian intelligence, I would have been in the Supreme Leader's office the next day.

General HAYDEN. Senator, it is Qasem Soleimani, and I would have gone in saying "Remember that briefing I gave you about a year ago, and you told me to put it on the back burner? Well, I have brought it forward."

Senator MCCAIN. Would you say that given the nature of it and given the book, I mean, like people being taken up to the presidential suite in Pittsburgh to be briefed on Iran, that these leaks probably came from the highest level?

General HAYDEN. Senator, I will defer. Although I have assigned the book as a textbook, I have not yet read it.

Senator MCCAIN. All right. Mr. Jenkins, let us talk about Mexico really quickly. They just had an election. Obviously, the Mexican people are extremely frustrated. As you pointed out in your testimony, 50,000 people have been murdered. The Mexican people, with some justification, believe that the United States is the destination. Why should they be the fall guy for all these deaths, terrorism, killing of journalists, and all the terrible things that are going on in Mexico?

How much effect do you think over time this situation is going to affect the United States of America as far as violence and also corruption in our country?

Mr. JENKINS. I think it is already having an effect. Look, the criminal cartels in Mexico are acquiring vast sums of money. They are diversifying. They are going into legitimate businesses, and that is going to give them increased revenue flows. But the one thing they are going to do is move downstream; that is, in the drug business, which is their primary form of commerce in this country, the profits increase as one gets closer to the retail level. That is, at the cultivation level, at the production level, the profit margins are narrower. As you go on through the process, the big profits increase.

They are going to move downstream to take control in an alliance with gangs already in the United States, exploiting those alliances to take increasing control of the drug traffic in this country. That is going to set off wars between them and wars with others in this country, and we have seen the quality of violence with which they conduct those wars in Mexico. So this is going to put them in increasing direct conflict with U.S. authorities. They will try first, as they always do, to suborn those authorities with cash and with other means, and when that fails, with the kind of direct challenges to society itself where you get this quality of violence, not just violence as a norm but beheadings, torture——

Senator MCCAIN. I understand.

Mr. JENKINS [continuing]. Things of this sort, as an effort to intimidate the entire society.

Senator MCCAIN. It is my understanding that the price of an ounce of cocaine on the street in any major city in America has not gone up one penny. Is that correct, in your assessment? Which means that we have had no success in restricting the flow, the old supply-and-demand situation. So we can identify the leaders of the drug cartels in Mexico, but we do not seem to be able to identify the leaders in the United States of America.

Mr. JENKINS. I do not know that we cannot identify or actually, I think——

Senator MCCAIN. But if the price has not gone up, isn't the point that we have to do something different?

Mr. JENKINS. That is true. The fundamental strategy, to the extent that we base our strategy entirely upon either crop substitution or interdiction, we have to do those. But that is not the most effective way we can respond. The strategy has to be fundamentally altered.

Senator MCCAIN. Should we have a conversation in the United States about the demand for drugs?

Mr. JENKINS. We have to do demand reduction. If we can do demand reduction, then we can suck the profits out of a lot of this.

Senator MCCAIN. Do you think it will be very interesting what strategy the new President of Mexico is going to adopt?

Mr. JENKINS. The new President of Mexico has addressed the issue where violence in Mexico has become the issue itself, not the criminality that creates the violence, but just the existence of the violence itself.

Senator MCCAIN. And the corruption.

Mr. JENKINS. The solution that he has proposed in his most recent speech is that he is going to basically put the army back into the barracks and respond with police. Now, that sounds good, and

it will create a new police force, and that is what he is promising to do. That will take time and resources.

In the meantime, the only way you can significantly reduce the violence in Mexico is by achieving some level of accommodation with the cartels themselves. Now, that brings us potentially back to the bad old days.

Senator MCCAIN. That brings us back to the Colombian experience under President Pastrana.

Mr. Chairman, I have just a short time. Maybe Mr. Cilluffo and Mr. Flynn would like to comment.

Mr. CILLUFFO. Just very briefly on Mexico, I think it also does require rethinking our own doctrine—it is a mixture, a hybrid threat, a hybrid set of issues from a counterinsurgency, counter narcotics, counterterrorism, even from a tactical perspective, as well as counter crime. So, I mean, it depends how we look at it.

I think you brought up Plan Colombia. When that was rolled out, I do not think one person in any room would have thought that would have been a success many years later. And if you look at it, it is a success. But it also required more than a traditional straight-up law enforcement function. It did address the corruption issues, judicial issues, law enforcement, but ultimately you had a para-law enforcement or paramilitary role that I think played a significant role in its success.

Senator MCCAIN. Mr. Flynn, doesn't it also indicate that we still have significant problems with border security?

Mr. FLYNN. Thank you, Senator. The first time I actually testified before Congress in 1991 was on this issue. In terms of what Mr. Cilluffo just said about Plan Colombia, one of the things that I remember commenting on a decade ago was that while that may have some prospect for success, almost certainly it will displace the drug trade into Mexico, and Mexico is a much more difficult problem for us to deal with being literally on our border. And yet there was no catcher's mitt strategy. We were so focused on who the current bad guys are and how we disrupt it, we were not thinking about how the commodity might actually flow and figure out what the plan to respond should be.

Senator MCCAIN. Which is also true of Central America as well as Mexico.

Mr. FLYNN. Absolutely. At its core, the arithmetic is pretty straightforward which you have laid out. Cocaine is just as available today in terms of price, actually at higher quality, than it was in 1980, adjusted for inflation. That is the reality.

The bulk of the money is made in retail, as Mr. Jenkins just pointed out here, in the United States. The arithmetic is: Take a kilo of cocaine—the amount of dollars that the coca farmer gets is roughly about $100. Then if he turns it into paste, he gets $300. If they turn it into refined the high-quality pure cocaine, then it is up to $1,000. They land in the United States with about 12,000 kilos, and if we distribute it, about $100,000. So that is where the money is. If you do not get at the demand, you are really not going to affect the dollars, and this trend that Mr. Jenkins highlighted of essentially moving retail, capturing where the money is, is something I think should be deeply worrying for us. At its core, though, this is why this is such an ugly problem. Ninety percent of the use

is by addict population. When we reduced half the casual use of drugs in the 1990s, that would affect roughly about 5 percent of the demand. Your addicts consume the overwhelming majority of drugs because they have very high tolerance levels, and it is a daily activity. And so if you do not go after your addict population, you are not going to make a dent on the market, and that is a messy population to try to deal with to drive down demand. But that is the economics of it.

Senator MCCAIN. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator McCain, for focusing on that unique and serious threat to our homeland security.

Senator Johnson.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman, first of all, for your leadership, as well as Senator Collins, on this issue, and for holding this hearing. I would also like to thank the witnesses for their time and very thoughtful testimony.

One common thread here is the power of information, and I would like to go back to what Senator Collins was talking about—and Senator McCain also talked about—in terms of our intelligence gathering and the damage caused by these leaks. I do not want to rerun the testimony in terms of how damaging they have been. I want to talk about how we repair that damage. What is the way we can improve our information in our intelligence-gathering capability if we are going to secure the homeland? And, General Hayden, I would like to go to you.

General HAYDEN. Well, Senator, it is almost better than a locked door because there are many opportunities to do a lot of things better. Let me depart from the first point about protecting sources and methods, and I think that is what Senator Collins was saying is the distinction. You can talk about how law-abiding your force is, maybe even how effective it is. But when you get into revealing sources and methods, it is at a great cost. And so I think we need to be especially protective of that.

Let me give you a bit of a dilemma. Some of the things we are doing—and let me use targeted killings against al-Qaeda as an example because a lot of that has been declassified. So much of that is in the public domain that right now this witness with my experience, I am unclear what of my personal knowledge of this activity I can or cannot discuss publicly. That is how muddled this has become. And I think to a first order, just clarity so that folks understand what is on the one side and what is on the other in terms of public discussion. That would be the first order.

Senator JOHNSON. Mr. Cilluffo, you talked about deterrence when it came to cybersecurity. I guess I would like to ask the question in terms of deterrence so we do not have future leaks. Now, we do have a couple prosecutors assigned to this case, ones that I do not necessarily have confidence in. I think there is some conflict of interest. Is there a way that we can provide that deterrence in a more rapid fashion? I think our Chairman mentioned that the last successful prosecution of a leak was 25 years ago. Can we really rely on the Justice Department to provide that deterrence in the future?

Mr. CILLUFFO. I do not have a good answer for you, but I think it is the right way to look at it, because if there are not consequences, then behavior will continue in whatever space we are looking at.

The big impact is what General Hayden was saying. Potential relationships with third-party and other intelligence services could suffer. And if we are not able to build some of that cooperative relationship, none of whom wants to advertise it, we will know what the impact has been. As to the leakers themselves, that is a question far beyond my ability to answer. But you need consequences, absolutely.

Senator JOHNSON. So in order to get to this in a rapid fashion, I guess, if we cannot rely on the Department of Justice, which I do not believe we can, I believe we have to rely on Congress. And I believe it is really this Committee that has jurisdiction, so I guess I may be unfair to turn to the Chairman here, but I think what we really need to do—and I would like your comments on this—is start holding hearings. If they have to be classified, fine. But I think we need to get to the bottom of these leaks. We need to figure out where the leaks occurred, whether crimes occurred. And I guess I would just ask the Chairman and Senator Collins to potentially consider doing those types of hearings.

General Hayden, can you comment on that?

General HAYDEN. Sure. It has proven very difficult within the judicial system to push this forward in a way you are describing that creates a deterrent—the laws, the First Amendment, a whole host of things. And here we are trying to impose a judicial punishment.

Senator I have not thought it through, but I have begun to think broadly personally that maybe this is best handled by the political branches, that the consequences may be in terms of policy and politics as opposed to judicial. And in that case, the Congress with its oversight authority could use that function to perhaps create the kind of deterrence that you are describing, because we have not been successful going down a purely judicial track for lots of reasons, some of which actually I understand and appreciate in terms of the First Amendment.

Senator JOHNSON. Right, and we have talked about complacency. If we sit back as a Congress and do nothing, doesn't that just feed right into that complacency?

Mr. FLYNN. Yes, I think it certainly can, Senator. One of the concerns that I have—and I have spent a lot of time talking to particularly critical infrastructure owners, the private sector, and folks in the civil, State, local levels—is if the impulse of the Federal folks who have information to share it is to keep it close to the chest because of the fear of consequence, then we really stifle the flow of information that needs to go down. I would just say that there are clearly some things that absolutely are disgraceful in terms of being released, have national security implications, the kind of things that General Hayden said, and we have to figure out how to deal with those.

My worry is sometimes the way bureaucracies respond to those very visual events is essentially to circle the wagons, and then you can have the most common-sense piece of information not passed out to critical players. So you have cases where a former senior Se-

cret Service agent cannot be told something because his clearance has lapsed when it is the bank he now works at is being targeted. Some of that has been improved, but there is still too much of that going on because the impulse is to keep the cards close to the chest, and that is one of the consequences of this challenge.

Senator JOHNSON. You mentioned the word "disgrace," and that might be the best deterrence, to expose it, disgrace the individuals that leak the information, that have harmed our national security, and, again, that is what I think only Congress can do and do it in a timely fashion. So that would be my recommendation.

Let me turn to cybersecurity very quickly. The reality of the situation is it is going to be very difficult to pass a bill, so from my standpoint, I think we start with a step-by-step approach of what is necessary to pass. We talked about standards. I would like to ask just two questions. Who would be best to develop those standards? And then, what would be the next top priority thing that should be passed? Is it information sharing? Is it something else? Let us start with General Hayden.

General HAYDEN. Yes, sir. Information sharing, I think, sets the groundwork. We do not get action because we do not all have a common view of the battle space, so to speak. And the more we can create this common view of the battle space, I think good people will all want to and will do the right things. So I would put an exclamation point next to that one.

Senator JOHNSON. And that is kind of what the House bill does—really centers on that, correct?

General HAYDEN. Yes, sir.

Senator JOHNSON. What about setting standards? Mr. Jenkins, do you have a comment on that?

Mr. JENKINS. I think standards are extremely important here. The fact is, the critical infrastructure is vulnerable to the extent that it is connected to the systems that can be penetrated by hackers and so on. We have to set standards that break that easy access into the operating systems. Now, in my personal view, in many cases, that connectivity was put in there because of convenience, not because of operational necessity. We have operating systems that are hooked up to the Internet that do not have to be hooked up to the Internet. They are not directly hooked to the Internet, but they are hooked to the corporate management structure which in turn is hooked to the Internet, and that provides a path in. And we have to separate those operating systems—somebody can mess with the corporate sites, that is one thing. But to get down into the operating systems, I think that is the real vulnerability.

Senator JOHNSON. Just briefly, again, I come from a manufacturing background where we have International Organization for Standardization standards set by industry. I guess that is what I am getting at. Because technology moves at such a rapid pace, should we be looking to industry to set these standards themselves as opposed to the Department of Homeland Security?

Mr. CILLUFFO. Senator, in my testimony that is my preferred approach. I mean, ultimately the sectors are going to know their systems and vulnerabilities best. How do you ensure that they are meeting certain objectives and goals? So, to me, I almost think the

ideal answer, which may be a bridge afar now, is you have a trusted third party. Think of a Good Housekeeping Seal of Approval. That is neither public nor private. That ultimately has the ability to be able to red team test vulnerability and systems, looking at it across the board.

One thing, though, that I would argue—and General Hayden I think was right—I mean, we cannot allow the information-sharing piece not to occur. You cannot expect the private sector to defend themselves against foreign intelligence services. That information, we need to build on the Defense Industrial Base Initiative, the pilot that is going on right now. That should be to other critical sectors.

So I do not think this should become a cigarette wrapped in asbestos. We do not want the lawyers defining the outcomes. We want the security experts. But if we do not do it now, that is who is going to define it. So, to me, let us get to that level of standards. And as much as it can be self-initiated, we should, they should.

Senator JOHNSON. Mr. Flynn, quickly. I am out of time.

Mr. FLYNN. I think we have some analogues for how to do this, some examples. But I do believe it needs to be the standards that are built with private sector input. They know where the vulnerabilities are. They know what the workable competitive solutions are. There has to be some enforcement, basically because there are often a lot of free riders. Big companies are responsible with brands, but there are small players who come in who do not want the cost. So everybody has to know it is a level playing field. So third parties, that is often a fee-based approach to make sure everybody is playing by the rules, is important.

Security, though, is a public good, so I do think you need to essentially audit the auditors. The model that I come out of, my Coast Guard background, we have standards set for very complicated things—the safety of ships. They are enforced by private third-party players like the American Bureau of Shipping and the fees cover that. But the Coast Guard spot-checks the system, and the way it ends up being enforced is if it stops a vessel that clearly got an approval by a third party but is not up to speed, not only is that vessel held, but everybody else who used that lousy classification society gets held. And that keeps the standards up.

So there is a role for government, I believe, because it is a public good we are talking about. But I think it is that building block. Industry develops the standards. The third party is a largely enforcement role, but government has a role to provide some oversight. I hope we could come to some reasonable closure on this because it is so important, the risk is so great.

Senator JOHNSON. Thanks a lot, Mr. Chairman.

General HAYDEN. Senator, if I may just add one additional thought?

Chairman LIEBERMAN. Go ahead.

General HAYDEN. As we create standards, we all know what the standards should be, and then industry has to decide. There are costs and benefits. There is risk you embrace, risk you cannot embrace, and so on. We need something overarching to help identify and categorize and quantify risk because if an industry is left with its own field of view, the risk will be adjudged based upon how much it costs the industry rather than how much it costs the

broader critical infrastructure. An overly simplified example, we lost power in Northern Virginia a week or two back. That obviously cost something to the electrical industry. But its impact was infinitely beyond the electrical industry. So we need something that infuses that into the calculus when you do cost and gain.

Chairman LIEBERMAN. Thanks, Senator Johnson. Thanks to the panel for their responses. The bill that not only the Committee reported out but that has been negotiated since really follows the model of a lot of what you have described.

Incidentally, I agree with you that if we do not do something, the lawyers will do it, and the lawyers will do it in the sense that there will be an attack and then there will be litigation to hold companies liable for what they did not do to protect customers from the attack. And then it will be done by lawyers arguing in court, and that is exactly the wrong place for it to happen.

We are trying to build a system in our bill where the private sector is involved in a collaborative effort to set standards for who is covered by this, just to get to the point that General Hayden was talking about, and we only want to cover the most critical infrastructure defined in a very demanding way. And then in the same collaborative process, to approve standards but standards that we do not want to be too prescriptive. They are basically outcome requirements, and we are going to leave it to the private sector to comply with those. But at some point—and we are open in the bill to certified third-party auditors, if you will, private sector auditors—it could be universities, probably will be universities in a lot of cases, who the government will say, OK, you are a credible operation, you are not a fly-by-night operation, so we are going to rely on you to tell us whether the companies have met the standards. And once you do that, obviously you get some benefits, one of which is protection from liability.

Mr. Flynn.

Mr. FLYNN. Mr. Chairman, just to add one more thing as you come to closure of the hearing, first, thank you for your extraordinary leadership during your tenure here.

Chairman LIEBERMAN. Thank you.

Mr. FLYNN. I would also like to commend your extraordinary staff, this bipartisan role with you, Senator Collins. I deal a lot across this body, and the staff that works so well together, I think, is a real tribute to the leadership that you both provide and also to the majority and minority staff directors.

One thing I would commend to you is the amount of knowledge that is in your staffs, and it would be, I think, a tremendous service to all of us for that staff to prepare a report of its findings based on what has been learned over the course of this past decade. There is a lot of turnover at DHS.

Chairman LIEBERMAN. Right.

Mr. FLYNN. This used to be a very unpopular business before September 11, 2001. It was a lonely one. It got a little more popular. It is getting a little more lonely again. So harnessing that enormous capability that I see behind you here would be, I think, a service to the Nation.

Chairman LIEBERMAN. Thank you for your kind words, and I agree with you. We have been very lucky with our staff, and I appreciate you giving them that substantial assignment. [Laughter.]

I have one more question, and I think Senator Collins may have one more question, too.

We talk a lot about state-sponsored terrorism. The State Department has a list of state sponsors of terrorism. But, really, we have been focused over the last decade much more on non-state actors, particularly al-Qaeda and the various iterations of al-Qaeda. But as one or two of you have said, we now have the kind of reappearance on a global scale of Iran-backed terrorism.

I wanted to start with you, Mr. Jenkins, and ask you how, if in any way, we should alter our response to this kind of state-based terrorism as compared to non-state terrorism? Or is it basically the same?

Mr. JENKINS. Well, in terms of dealing with the Iranian thing, the terrorist campaign, these incidents that we have seen thus far, is really only one small component of a much broader set of issues in which we are engaging with Iran. And from their perspective, what they are doing with these terrorist attacks is in part saying that there is going to be a cost for what they perceive as a campaign of sabotage and assassination directed against their nuclear program. I will not get into whether that is a correct perception or not, but certainly that is their perception.

Their future use of this terrorism is going to depend very much on what they calculate our intentions are about the Islamic Republic itself. If they believe—and there are radical elements within Iran that I suspect do believe this—that the aim of the United States is to ultimately bring about the fall of the Islamic Republic, then that is going to affect their risk calculations, and they are going to basically conclude they do not have a lot to lose. And they would be willing to—they will be willing to—escalate that.

Now, this implies, by the way, that there is a rational actor model: That is, what they do is in response to what we do, which is in response to what they do. And people who will challenge that rationality model, saying, no, we are dealing with apocalyptic types here who are not always going to behave rationally; but right now, in terms of our efforts to stop their nuclear weapons program, we are depending on that model to work.

How do we respond to this? I think, in fact, we are going to see the continuation of a long-term, complicated, shadow terrorist war, not simply involving the United States and Iran. It will involve Israel, it will involve Saudi Arabia, it would involve others. This is a tool that they have, and here I would go back to underscore a point that Mr. Flynn made, and that is, no one can take us on in an open, conventional way. That simply is not going to work. So they have this as an instrument. They feel righteous about its use. They have capacity, and so I think that capacity is going to be used going forward. And I do not think there is any way, any easy way, out of this contest.

Chairman LIEBERMAN. Barring some shockingly surprising rapprochement with Iran and settlement of the dispute over their nuclear weapons capability program, no, I agree. I think the emergence of Iran-backed terrorist acts or attempted acts over the last

year or so is obviously related to the tension that is going on between us, the Israelis, the Saudis, and a lot of others in the Arab world with Iran about their nuclear weapons development program. So they are sending a message by these acts or attempted acts.

Mr. JENKINS. Well, you said barring some dramatic reversal of their policy with regard to nuclear technology. And, of course, the trajectory can go the other way as well.

Chairman LIEBERMAN. Correct.

Mr. JENKINS. And, that is, the tensions can increase, hostilities can look as if they are imminent.

Chairman LIEBERMAN. Right.

Mr. JENKINS. And then I think our operative presumption has to be that there will be an escalation in the terrorist campaign directed against their targets in the region as well as targets further on.

Chairman LIEBERMAN. And the second scenario, today you would have to say based on what has happened in the P5+1 talks with Iran and in their lack of any change in response to the sanctions, the second scenario is the more likely.

Mr. JENKINS. The most positive assessment would be a continuation of things as they are. That would be good news?

Chairman LIEBERMAN. Yes, right.

Mr. JENKINS. If it is going to move one way or the other, it probably looks as if it will head——

Chairman LIEBERMAN. In a worse direction.

Mr. JENKINS. In a worse direction, yes.

Chairman LIEBERMAN. Mr. Cilluffo, do you want to add something quickly? Then I want to yield to Senator Collins.

Mr. CILLUFFO. Mr. Chairman, I just want to be very brief. The red lines we historically looked at are out of focus today. From Beirut to Bangkok to Baku, I mean, you are starting to see an uptick in activity, by whom precisely is unknown, the Revolutionary Guard, the Ministry of Information, or others.

But at the end of the day you are seeing an uptick in activity. The cyber issue that came up in the conversation—I mean, cyber is made for plausible deniability. That is why the extra shame if what has been said is accurate in the *New York Times* that we are even discussing these sorts of issues. I recently testified on the House side on Iran and cyber before all these leaks, and they are investing heavily in this space. And I would argue that they will not be discriminate. In other words, who really should shed a tear? I think it was the right thing to do to go to stymie Iran's nuclear programs and slow that down a little bit. Do not think that their response in kind would be discriminate. And those same vulnerabilities that can be used there could be exploited in other ways.

So, to me, it is a significant set of issues, and the Los Angeles Police Department, I might note, has elevated the government of Iran and Hezbollah as a Tier 1 threat, highest potential threat. So their intelligence requirements are starting to kick in.

Chairman LIEBERMAN. That is significance. Thank you. Senator Collins

Senator COLLINS. Thank you, Mr. Chairman. First, I am grateful that my friend Senator Johnson has stayed to the very end of the hearing because I do want to put into context, and to some extent counter his commission on cybersecurity and what we need to do by reminding him that General Hayden's first list was we need to do all three, and that includes protecting critical infrastructure.

Mr. Flynn reminded us that critical infrastructure is vulnerable to sabotage. We have seen just in the last week what a natural disaster can do, the chaos, the loss of life, the decreased economic activity, the hardship, and the accidents that occurred at non-working traffic lights. Well, that would be multiplied many times over by a sustained cyber attack that deliberately knocked out our electric grid. And as Mr. Flynn also pointed out, not only is there a lack of protection of our critical infrastructure, but it is not as resilient as it should be, and that is why here we still have people without power in West Virginia and some parts of Virginia as well.

I would also point out as my final comment that while all of us, everybody agrees that improved information sharing is absolutely essential, it is far from a panacea that will lead to improved cybersecurity. A joint report by the Center for Strategic and International Studies and McAfee that was published just last year found that 40 percent of critical infrastructure companies were not taking even the most basic security precautions such as regularly installing software patches or changing passwords, just basic precautions that all of us know we ought to be taking. And given the unending publicity about almost daily cyber attacks—including, I might add, a cyber attack that infiltrated the Chamber of Commerce's own computers for many months without their being aware of it. Given all of that evidence, I think that we can conclude that a completely voluntary system where we do nothing related to critical infrastructure will not solve the problem.

And I would ask all of our witnesses just very quickly, even if you think that information sharing may be No. 1 or some other step, such as better intelligence gathering, may be No. 1, are we truly going to improve the security of critical infrastructure in this country—our electric grid, our transportation system, our financial systems—if we do nothing legislatively related to critical infrastructure? General Hayden.

General HAYDEN. Ma'am, obviously the information sharing helps, but I stand by my original statement, as you pointed out. All three of these are good ideas, and we need to move out on all three fronts.

Senator COLLINS. Thank you. Mr. Jenkins.

Mr. JENKINS. No, I think it is essential that we do something now in terms of addressing the vulnerabilities in our critical infrastructure. I mean, we have seen these threats mount, and to go back to earlier comments made, what is likely to take place in the wake of some type of cyber catastrophe is going to be messier and not nearly as useful as doing something now. So the choice is not doing something or not doing something now. The choice is doing something thoughtful, perhaps 90 percent right, hopefully, versus doing something later on which is likely to be really messy.

Senator COLLINS. Thank you. Mr. Cilluffo.

Mr. CILLUFFO. I think it absolutely does require legislative prescriptions. All my views aside, I do think the intelligence and information-sharing piece is priority No. 1. But you have other pieces that need to be addressed, and quite honestly, we have not made the business case for cybersecurity. So, to me, that is where we need to be looking, because we need to look at what the carrots are as well as the sticks. The fact that the insurance and reinsurance sectors, they have always had more success in inducing changes in behavior, the fact that they are not in this space to me is a little upsetting. The one thing I would argue against is we tend to look at this issue reactively, and I am not just talking legislatively. I am talking cyber generally. Think about it this way: After your system gets broken into, what do you do? You get a patch. That would be like in a physical domain, after someone breaks into your home, you are calling the locksmith first, not a police department, and you are not dealing with prevention.

So let us just make sure we are not only looking at it picking up the pieces after they have already fallen. I want to get a little more proactive. I think we need to invest in active defenses. This will require legislation, too. So these are the sorts of issues I think we need to also include.

Senator COLLINS. I cannot tell you how many chief information officers of major companies have come to me and said, "I know we need to invest in this area. We are so vulnerable. But we cannot get the attention of the chief executive officer." I have heard that countless times.

Mr. FLYNN. I would very much reinforce what has just been said. The need for standards is critical, and they have to be enforced in order to change this behavior, the behavior right now as the system is wide open. And the risk is—and as I constantly say to industry—the morning-after problem. When we have an incident—you will have legislation, and there will not be as much time for industry input. So let us use this moment now when you have a voice at the table where there are clearly trade-offs that have to be made here, engage.

I wanted to really reinforce something that General Hayden said about one of the challenges of dealing with just purely a sector-by-sector approach with each group setting standards. Take the Port Authority of New York and New Jersey. At rush hours, which, of course, it has in the morning and evening, there are 1.8 million people inside Port Authority facilities—on the bridges, in the tunnels, on the trains, or in its airports. When the power goes out, those folks get stranded in those facilities. You have to deal with that. The Port Authority does not produce any power. It is depending on utilities to do that. But its core mission, mobility, depends on that.

The utilities have to go to raise their rates to state-run public review boards in order to get the investment for security. So, again, the tension becomes, absent a regulation or a requirement, how do they make a case when other sectors are being impacted? There is some need for some adult supervision here. And it is also important to insurers and reinsurers. If there are no standards, you are not going to insure. Insurers, if they have to go out and do all the enforcement themselves, which has costs, to make sure that people

buy off on the standard, that is not a profitable market for them to do. They need to know there are standards. They need to know there is a mechanism like third parties to do it. Then they can come up with incentives. But they are not going to give anybody incentives if they do not know anybody is complying with it, and that basically is where this whole thing has broken down.

Senator COLLINS. We often bemoan the fact that there was a failure to connect the dots prior to the attacks on us on 9/11. This time, there have been so many warnings that we are vulnerable to a major cyber attack that shame on Congress if we do not take steps now to try to avert a cyber 9/11. This is not a case where there was a failure to connect the dots. This is a case where every expert has told us that a cyber attack could happen at any time, and indeed happens every day. And this poses a threat not only to our national security but to our economic prosperity, because we are not only in danger of being disrupted from a national security perspective, but we are losing trade secrets and intellectual property, research and development developed by American firms every single day. And to me, that is another compelling reason that we must act.

Mr. JENKINS. Can I add a comment here? This body can pass legislation, and this Committee's responsibilities cut across government. But actually, when you pass that legislation, some portion of government is going to have to have the responsibility for implementing these pieces, and it looks as if DHS is going to have a heavy role here. And that really raises a question of capacity, in terms of the capacity to assess threat, to do the analysis, to ensure that this thing is being implemented properly. And there is a real-question mark about the existence of that capacity right now.

So the legislation, however good it is, is not going to work unless there is the machinery somewhere in government to do it. And I am not sure it is there right now.

Senator COLLINS. Well, that is why, as we did with the Intelligence Reform Act in 2004, we created a National Counterterrorism Center that brought together, as General Hayden well knows, expertise from many agencies, which we do in our bill, and we also tap into the private sector repeatedly in a collaborative relationship.

Finally, I would say that having personally spent a lot of time at the cyber center that DHS has now, I think most people would be impressed with the progress that has been made. And they have done it with cooperation with NSA, which is an absolutely vital player, and with many other agencies as well. But the point is, while we may have differing views on exactly how to structure this, if we let those disagreements sink a bill that requires critical infrastructure to meet certain standards in order to get liability protection, for example, I think we will be failing the American people. And when the attack comes—and it will come—everyone will be saying why didn't we act. And then we will rush to act, and we will do far less good a job, and the damage will have been done. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. I was going to add something, but you have said it all. Senator Johnson, do you have another question you would like to ask?

Senator JOHNSON. No. I would just like to make a comment.

First, I do not really believe there is much I would disagree with anything that has been said by anybody here. The point I was trying to make in my questioning is based on the failure of this Stop Online Privacy Act (SOPA) and PROTECT IP Act (PIPA) legislation. I think it is critical that we do move forward on this, and I am just trying to ask to prioritize it. It sounds to me like standards would be the first thing, to set those so that we can start maybe using the private sector and insurance markets to start enforcing things, then information sharing. I was just trying to get the priority of things that, if we cannot go for the full loaf—I would love to pass a perfect piece of legislation. I just think it is going to be very difficult. What are the confidence-building steps we can pass now to start the process going?

That was the only comment I was trying to make. Thank you.

Chairman LIEBERMAN. I appreciate that, and as you know, there is a lot of, I think, very constructive work going on which Senator Collins and I have encouraged and are keeping in touch with, that is in a bipartisan process being led by Senator Sheldon Whitehouse and Senator Jon Kyl. I do not know that it will produce common ground that everybody will want to occupy, but I am hopeful that it will produce common ground that at least 60 Senators will want to occupy.

I thank the panel. You have really been extraordinary. Just looking at you, each one of you has given great service to our country in various capacities, and I think you have added to that by the written statements that you have submitted for the record and by your testimony here today, and I appreciate it very much.

We will leave the record of this hearing open for 15 days for any additional statements or questions. We will be back here tomorrow morning with part two, which will be a review of the first decade of the Department of Homeland Security and some looks forward into the next decade. The witnesses will be our former colleague, Jane Harman, now at the Woodrow Wilson Center, Admiral Thad Allen, and Richard Skinner, who is a former Inspector General at the Department of Homeland Security.

So, with that, I thank you all, and the hearing is adjourned.

[Whereupon, at 12:21, the Committee was adjourned.]

VerDate Nov 24 2008 13:06 Dec 04, 2012 Jkt 76059 PO 00000 Frm 000042 Fmt 06633 Sfmt 06633 P:\DOCS\76059.TXT SAFFAIRS PsN: PAT

THE FUTURE OF HOMELAND SECURITY: THE EVOLUTION OF THE HOMELAND SECURITY DEPARTMENT'S ROLES AND MISSIONS

THURSDAY, JULY 12, 2012

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, Collins, and Johnson.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning, and the hearing is convened. Thank you all for being here, particularly thanks to the witnesses who we will introduce in a few moments.

This is the second in a series of hearings the Committee is holding on the past, present, and future of homeland security in our country, coincident with the 10th anniversary of the adoption of the Homeland Security Act in November of 2002—obviously following the events of September 11, 2001 (9/11).

Also, Senator Collins has been good enough to support my desire, as I end my service in the Senate, to take a look back at where we have been in homeland security over the last 10 years, but really more importantly, to look forward and to try to discuss some of the unfinished business and to anticipate how we can meet evolving threats. I hope thereby to create a record which will be of help to this Committee in its new leadership next year.

We had a very good hearing yesterday with a panel that was describing the evolving homeland security threat picture. Today we are going to focus in on the Department of Homeland Security (DHS) itself, how it has done over almost 10 years now, and what it should be doing in the years ahead.

The Department of Homeland Security does not include all of the Federal Government's major homeland security agencies. Obviously, the Departments of State, Defense, Justice, Health and Human Services, along with the key intelligence agencies of our government, all play very important roles in protecting our homeland security. And, of course, State and local partners as well as the private sector, and, as we discussed yesterday, the American people themselves all have significant responsibilities. But really

the center of homeland security was intended to be the Department of Homeland Security. It was intended to be not only the center point but the coordinating point of the agencies that were brought within it and also to make sure that we were interacting with a lot of other agencies over the Federal, State, and local governments that had both the responsibility and some opportunity to contribute to our homeland defense.

As I look back, I would say that the Department has come an awful long way in its first decade, but this is a mission that it has that in a sense has no final destination point. It has to continue getting better, and there are ways to meet the evolving threat, and there are ways in which in the first decade there were some things that happened that were not as good as we wanted.

But as I go back to 10 years ago, I think the vision that Congress had for the Department of Homeland Security when we created it was to have a Department that would be more than the sum of its parts, a Department that would integrate key homeland security functions such as border preparedness and infrastructure protection, and a Department that would help ensure, as we said over and over again after 9/11, that we would never again fail to connect the dots so that we would prevent the next 9/11 from happening.

As I said, I think the Department has made tremendous strides forward in the nearly 10 years since the passage of the Homeland Security Act in achieving some of these broad goals that we have talked about and that we had in mind 10 years ago. Al-Qaeda, which we were focused on, of course, because it claimed credit for the attacks against America, and its affiliates have not carried out a successful attack, certainly not one anywhere near the catastrophic dimensions of September 11, 2001 since 9/11, which I think is a credit not only to our offensive forces led by the U.S. military and intelligence communities, but also to the tremendous work that the Homeland Security Department has done.

Let me talk about some of the areas where I think there has been significant progress. We have a screening system now at points of entry into the United States that is integrated with information from the intelligence community and others and has become very effective at detecting bad actors trying to enter our country. Our aviation screening system is vastly improved from what we had before 9/11. We also now have much more robust two-way information sharing on potential threats, not only within the Federal Government but with State and local governments, and that is in large measure due to the leadership of the Department of Homeland Security and its support for State and local fusion centers.

In a different aspect of the DHS responsibilities, our Nation's preparedness and response efforts, led by the Federal Emergency Management Agency (FEMA), have improved significantly in the 7 years since Hurricane Katrina, which obviously showed how inadequate FEMA was at that point, and their response to just about every natural disaster that has occurred in our country since then has been significantly better and drawn very positive reviews.

These are important achievements, and we should not forget them in the occasional griping from people who do not like to take their shoes off or go through magnetometers or whatever else at

airports. But the Department still has a way to go to fully realize what we want it to be, and let me just mention a few of the areas where I think that there is much more to be done. And, interestingly, most of these have to do with the administration of the Department, with process, if you will, but process is important.

For example, the Department's operational components I think are still not adequately integrated with its headquarters and with each other, and that causes problems. That causes at least less than optimal use of the Department's resources.

The Department of Homeland Security continues to have workforce morale challenges, as reflected in the annual ratings done in the Federal Human Capital Survey. These have improved over the years, but nowhere near to the extent needed.

The Department of Homeland Security also struggles with setting requirements and effectively carrying them out for major acquisitions and ensuring that these acquisition programs stay on track while they are underway. The Department of Homeland Security unfortunately is not unique among Federal agencies in this problem, but this is the Department that we helped create, and we have oversight responsibility for it, and we have to be honest and say their performance in this regard has not been adequate.

And, of course, in the years ahead, the Department in a different way will need to take actions to anticipate and respond to evolving homeland security threats, including continuing to increase its improving capabilities with respect to cybersecurity in response to cyber attacks on our country.

The greater challenge, of course, is that the Department of Homeland Security, along with every other Federal agency, will have to find a way to do this in a period of flat or perhaps even declining budgets. In a budget environment like the one we are in today, the natural tendency is to focus on preserving and protecting current capabilities, but the risk of doing only that is that we will be underinvesting in systems needed to meet evolving and new threats of tomorrow.

So I think in its second decade, the Department of Homeland Security will have to be, if I may put it this way, as agile as our enemies, and that may mean that the Department will have to cut back in some of its now traditional areas of responsibility if they seem less relevant to the threat and take that money and invest it in programs to meet new threats that come along.

The three witnesses that we have—Congresswoman Harman, Admiral Allen, and Mr. Skinner—are really uniquely prepared by experience and capability to contribute to our discussion and build exactly the kind of record that I hope this Committee will build to hand over to the leadership in the next session. I cannot thank you enough for being with us this morning, and I look forward to your testimony.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Nearly 10 years ago, the creation of the Department of Homeland Security brought together 22 different agencies into a single Department to focus like a laser on protecting our country and its citi-

zens. Yesterday, as the Chairman indicated, we explored the emerging security threats our Nation is likely to confront. In my judgment, the largest threat in that category is a cyber attack. Today we will examine whether DHS is well positioned to address these emerging threats as well as other longer-standing threats.

The changing threat landscape at home and abroad requires the Department to be nimble and imaginative, effective and efficient—qualities not often associated with large bureaucracies. Yet the men and women of DHS can take pride in the absence of a successful large-scale attack on our country during the past decade and in the Department's contributions to thwarting numerous terrorist plots.

There have been successes and failures over the past 10 years. Information sharing has improved, but remains very much a work in progress. Ten years ago, we envisioned that DHS would be a clearinghouse for intelligence. Although incidents like the failed Christmas Day underwear bomber made clear that information sharing is still imperfect, numerous public and classified counterterrorism successes since 9/11 demonstrate that information sharing has indeed improved.

This is also true with respect to information sharing between DHS and the private sector, an essential partner in the protection of our country since 85 percent of our critical infrastructure is privately owned. The growing network of State and local fusion centers also presents opportunities not only for the improved dissemination of information but also for the collection and analysis of intelligence at the local level.

As we discussed yesterday, however, these centers have yet to achieve their full value. They have yet to truly become successful aggregators and analyze local threat information in too many cases.

The Transportation Security Administration (TSA), the agency within DHS that is most familiar to the public, has strengthened airline passenger risk analysis, but it still troubles many Americans to see screeners putting the very young and the very elderly through intrusive and in most cases unnecessary patdowns. TSA is making progress toward implementing more intelligence-focused, risk-based screening through such efforts as Pre-Check, but many challenges remain for TSA.

DHS has also bolstered the security of our borders and identification documents, yet two Iraqi refugees associated with al-Qaeda in Iraq were arrested in Kentucky last year. When a bomb maker whose fingerprints we have had for some time is able to enter our country on humanitarian grounds, it is an understatement to say that "work remains," as DHS's self-assessment states.

In order to meet and overcome current and future threats, DHS must support its component agencies with stronger management. Since 2003, the Government Accountability Office (GAO) has designated the Department as high risk. It has done so because of the management and integration challenges inherent in any large undertaking. But what people often do not realize is the high-risk designation refers not to just being at risk for waste, fraud, and abuse; it is at risk for program failure and, thus, the consequences of being on the high-risk list are serious indeed. DHS must imple-

ment changes that will hasten the day when the Department is no longer included on GAO's high-risk list.

The roles of the Department's components have evolved over time. As a positive example, I would note the adaptability and can-do attitude of the Coast Guard. I do not believe that there is another agency within DHS that has done a better job of adapting to the new challenges and its expanding mission in the post–9/11 world. This was never more clear than after Hurricane Katrina.

As this Committee noted in its report on Hurricane Katrina, the Coast Guard demonstrated strength, flexibility, and dedication to the mission it was asked to perform, and saved more than half of the 60,000 survivors stranded by this terrible storm.

Many experts have predicted a disaster in the cyber realm that would compare to Hurricane Katrina. Compared to 10 years ago, the cyber threat has grown exponentially. Clearly, this requires an evolution in the Department's mission to secure critical systems controlling critical infrastructure, such as our transportation system, our nuclear power plants, the electric grid, our financial systems—a goal that we hope to accomplish through the enactment of legislation that Chairman Lieberman and I have championed.

Despite the fact that DHS has made considerable strides over the past decade, it still has a long way to go by any assessment. To understand what challenges the Department is facing, what changes are needed, and to prioritize our limited resources, we must learn from the Department's past mistakes and be able to better measure what has worked and what has not. To do so requires metrics and accountability, an area where the Department has been challenged.

I very much appreciate that we have such outstanding experts here with us today to help us in evaluating the Department's progress and its future direction.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

Our first witness, I am delighted to say, is Congresswoman Jane Harman. With Senator Collins, Congresswoman Harman, and myself here, we have three of what we used to call "the Gang of Four."

Ms. HARMAN. "The Big Four."

Chairman LIEBERMAN. "The Big Four." Much better. We could say "The Final Four." No. [Laughter.]

What I am referring to in this inside conversation is that we were privileged to constitute bipartisan and bicameral leadership on the processing and ultimate adoption of the 9/11 legislation, which actually followed the creation of the Department of Homeland Security. And I had known Ms. Harman, of course, before but really got to know her well, greatly admire her, and even like her.

Ms. Harman comes to us today as the President of the Woodrow Wilson Center. Her tenure in the House included service as Chair of the House Committee on Homeland Security's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, and as Ranking Member of the House Permanent Select Committee on Intelligence. So I am really delighted that you could make it, and we welcome your testimony now.

TESTIMONY OF HON. JANE HARMAN,[1] DIRECTOR, PRESIDENT, AND CHIEF EXECUTIVE OFFICER, WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

Ms. HARMAN. Thank you, Mr. Chairman and Senator Collins and friends, for the opportunity to join you and to return to Capitol Hill to testify on a topic I am passionate about, which is the security of our homeland.

I am also honored to be testifying with Admiral Allen, who is here in facial disguise, and Mr. Skinner. They have far more hands-on experience with this topic than I do.

Our collaboration, which you just referred to, over many years I believe shows that bipartisanship—indeed tripartisanship—is possible. We had a good gig going during my nine terms in the House, and our legislative efforts, as you said, yielded significant results—and many special times.

Well over 10 years ago—my goodness how time flies—I joined you, Mr. Chairman, and a hardy little band of legislators who thought a homeland security function made sense in the aftermath of 9/11. What we had in mind, however, was something far less ambitious than the plan ultimately sketched out by then White House Chief of Staff Andy Card.

As I recall, we envisioned a cross-agency "jointness" similar to the concept we were able to enact into law as the 2004 Intelligence Reform Act. And, by the way, yes, we were the Big Four, along with Pete Hoekstra. But I would point out that two of the Big Four happened to be female, so, of course, we did 98 percent of the work, and that is why the bill passed. [Laughter.]

Chairman LIEBERMAN. I want to note from this perspective that the women in the room laughed at that. [Laughter.]

Ms. HARMAN. I saw Senator Carper laugh.

Senator CARPER. That is the feminine side of me coming through. I always thought of you as the "Fab Four." [Laughter.]

Ms. HARMAN. Back to the homeland bill, I remember that once the White House proposal had been announced, we all decided to embrace it because that would ensure presidential support. And so it was.

Although DHS comprised of 22 departments, as Senator Collins said, and agencies, Congress tried to organize that around four main directorates: Border and Transportation Security, Emergency Preparedness, Science and Technology, and Information Analysis and Infrastructure Protection. That is the intelligence function.

The Information Analysis Directorate was supposed to analyze intelligence and information from other agencies, as I think you said, including the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), and the National Security Agency (NSA), involving threats to the homeland and to evaluate vulnerabilities in the Nation's infrastructure—something we definitely need to be doing. Emergency Preparedness would oversee domestic disaster response and training. Border Security would streamline all port-of-entry operations, and the Science and Technology (S&T) Directorate would acquire

[1] The prepared statement of Ms. Harman appears in the Appendix on page 154.

scientific and technological skills, mostly from the private sector—this was the idea—to secure the homeland.

Well, the initial strategy morphed into something different, and we all learned, if we did not know it before, that merging government functions is difficult, and the threats against us are evolving, and so are our enemies. So it is important that we take this look today that you have suggested.

While DHS has experienced real success, there have also been what I would call hiccups and significant growing pains. It is certainly not the first Department to run into problems.

But my bottom line is that, to fix those problems, we should not rearrange the deck chairs again. What we should do is make a clear-eyed assessment of what works and what does not.

Here are some of the functions that execute well:

Last year, as you said, I think, Mr. Chairman, Customs and Border Protection (CBP) stopped more than 3,100 individuals from boarding U.S.-bound aircraft at foreign airports. And CBP was able to process more than 15 million travelers at 15 pre-clearance locations in the same year. That is like picking needles from a haystack.

TSA now fully implements Secure Flight, the program screening all passengers on flights from, within, or bound for the United States against government terror watch lists. Extending our "borders" by using real-time, threat-based intelligence in addition to multiple layers of security is working.

The Department expanded "If You See Something, Say Something" to dozens of States, cities, transit systems, fusion centers, Federal buildings, etc. Local residents are the first line of defense against terror plots in this country because they know what looks suspicious in their neighborhoods.

That is why I think fusion centers are so important. Last year, the Colorado fusion center helped identify an attempted bombing suspect. And fusion centers around the country worked together to share tips and leads necessary to arrest and convict Faisal Shahzad, the 2010 Times Square bomber. There are problems with them which we can discuss, but some are terrific.

Finally, the Office of Infrastructure Protection conducted more than 1,900 security surveys and 2,500 vulnerability assessments on the Nation's most significant critical infrastructure to identify potential gaps.

But the challenges are significant. I do not want to abuse my time here, so I will rush through them.

First, the intelligence function has never fully developed. Part of the reason is that President George W. Bush stood up the Terrorist Threat Integration Center (TTIC), which is now the National Counterterrorism Center (NCTC), outside of the Department of Homeland Security. So a significant portion of its jurisdiction moved out.

Intelligence reports are meant to be consumed by State and local law enforcement, but many of those entities consider what DHS reports to be "spam," cluttering overflowing inboxes. In many cases, law enforcement still reports that State fusion centers provide better information.

The new DHS Strategic Plan for fiscal years 2012–16 said that intelligence is an area needing "enhancement," and we can discuss that if you want.

Chairman LIEBERMAN. Excuse me a second. If you want to take a few extra minutes, you should go ahead and do that.

Ms. HARMAN. Thank you.

One of the enhancements necessary, in my view, is writing reports that are actually useful to local law enforcement, and that was the point of establishing the Interagency Threat Assessment and Coordinating Group (ITACG), which I understand may suffer some funding problems, and I want to thank you, Mr. Chairman, just as a citizen out there for fighting to restore the funds that may be taken away.

Second, the homeland mission is so large that the Department must assess where it can be most effective and where it cannot. For example, I believe that DHS will never be the leader in preventing cyber attacks. But I do think it can perform the mission that you in your legislation suggest, and I think it is absolutely crucial that the legislation Congress enacts include parts that protect critical infrastructure. So I support your bill over the one that the House has been considering, and I hope that Congress will move forward on legislation promptly.

Third, I think that Congress has been a very disappointing player in this process. Not this Committee, but Congress has failed to reorganize its committee structure, and the homeland jurisdiction here, but more significant in the House, is anemic. The Department still has to report to more than 80 committees and subcommittees. We have simplified that somewhat but not enough. And the one recommendation of the 9/11 Commission that remains basically unimplemented is the recommendation to reorganize Congress.

So what are the biggest opportunities?

First, while the Department should be praised for overhauling its privacy and civil liberties office, which I know you care about, it should not stop there. You and I all urged the White House to appoint the membership of the Privacy and Civil Liberties Oversight Board, which is mandated in the 2004 law. In the Bush Administration, that Board barely functioned. I think that would be fair. And in this Administration, finally all the members have been nominated, they have been reported from committee, but they are not confirmed. So we do not have that function yet.

Second, DHS should do much more to reduce overclassification of intelligence. Your Committee worked for a year to help pass the Reducing Overclassification Act of 2010, but very little has happened to implement it. I think it should be a high priority.

And, finally, the Secretary must continue to be the face of homeland security. Janet Napolitano happens to be an old friend of mine, and before she took office, I suggested that she be the Everett Koop of threat warnings—just as he was the Nation's most trusted anti-smoking crusader. And, frankly, this reminds me of a kind of silly thing. Once there was a color-coded system for homeland security warnings. I remember the Department saying that we were moving from pale yellow to dark yellow, and I commented that the Homeland Security Secretary should not be an interior designer. That prompted a hilarious call from Tom Ridge, but the

point of this is there are some homeland functions that only the Secretary can carry out, and one of them is being the respected voice to warn the rest of us of the threats we face and to prepare us.

In conclusion, as you said, Mr. Chairman, no major attack on U.S. soil has occurred since 9/11. DHS deserves some real credit, but so does this Committee.

As you said, soon you will join the ranks of what I would call policy wonks and grandparents—like me—who work outside of Congress. And just this week—I think it happened already. Did Senator Collins break Cal Ripken's record?

Senator COLLINS. Today.

Ms. HARMAN. Today, 5,000 votes. Can we all applaud you?

[Applause.]

And next month, you will taste married life. Both of you bring such skill and dedication to this work. I strongly doubt that your new roles will diminish your passion, and mine remains as strong as ever.

I really salute you, dear friends. Thank you, Mr. Chairman, for the opportunity to testify.

Chairman LIEBERMAN. Thanks very much for your testimony.

I was watching TV the day that Cal Ripken broke the previous record, and it was one of many occasions when my wife was befuddled by my behavior because, as Ripken circled the field, receiving the adulation of the crowd, I began to cry. She did not understand that. But I am going to try to control my tears today. [Laughter.]

Ms. Harman, you said something that I just want to draw attention to because this is the kind of—with all the problems and unfinished work DHS has, you cited some statistics that I did not cite about border security and counterterrorism prevention, and almost nobody in the country knows this, but people ought to have a greater sense of confidence—I believe they do—when they get on a plane. Last year, CBP stopped more than 3,100 individuals from boarding U.S.-bound aircraft at foreign airports for national security reasons. And that is out of 15 million travelers at 15 pre-clearance locations that they cleared.

So it took very sophisticated data systems and implementation of those systems to make that happen, but we are all safer as a result of it. Thank you very much for your very thoughtful testimony.

Next, Admiral Thad Allen served as Commandant of the Coast Guard from 2006 to 2010. As we all remember, he led the Federal Government's response to Hurricane Katrina and the Deepwater Horizon oil spill, and in both really distinguished himself. In Hurricane Katrina, he was the singular source of reassurance to the American people that somebody really was in charge and was effectively coordinating response efforts and aid to the people who suffered, which really was a great moment for our country.

Admiral Allen, I believe Congresswoman Harman suggested you may be undercover as a result of your facial hair, but I know better that you are now currently a senior vice president at Booz Allen Hamilton, Incorporated. Thanks very much for being with us this morning.

TESTIMONY OF ADMIRAL THAD W. ALLEN,[1] U.S. COAST GUARD (RETIRED), FORMER COMMANDANT OF THE U.S. COAST GUARD

Admiral ALLEN. Mr. Chairman, Senator Collins, and Members of the Committee, I have sat before these hearings countless times and said I am delighted to be here. This morning, I really mean it. [Laughter.]

Chairman LIEBERMAN. Thank you.

Senator CARPER. How about all the other times?

Admiral ALLEN. And it is an honor to be here with Jane Harman and Richard Skinner, my colleagues. We have worked together a lot in the past. She has been a tremendous leader at the Port of Long Beach in the past, and Mr. Skinner and I worked very closely in the last 10 years over the evolution of the Department of Homeland Security.

The perspective I am trying to bring this morning, Mr. Chairman, is one of somebody that has worked this problem from the inside out from the onset. I was the Atlantic Commander on 9/11 when we closed Boston Harbor after the planes took off from Logan Airport. We closed New York Harbor, with the tremendous challenge of evacuating people off of Lower Manhattan, and we closed the Potomac River north of the Woodrow Wilson Bridge, and it marks a sea change for the Coast Guard in how we addressed that end of the fall of 2001 and the winter of 2002. As you talked about, there was much discussion about how to aggregate these types of functions and increase the security for the United States.

I consulted with the Commandant at the time, who was Admiral James Loy, and there was some kind of a feeling there would be some kind of an aggregation of functions, as Representative Harman said, and then I believe it was in June 2002, the Administration placed the bill on the Hill proposing the creation of a new Department. Sir, I know you were right in the middle of all of that, including the very robust discussion on work rules.

Chairman LIEBERMAN. Yes.

Admiral ALLEN. I want to settle a context for my testimony by just recounting some of this because I think it is really important to have it on the record.

There was an initial push, as you know, to have this bill passed by the first anniversary of 9/11. That did not happen for a lot of reasons, and you are familiar with that.

When the bill finally passed, the President was in a position where the bill had to be signed right away, and it was signed on the November 25, 2002. It required that the Department be established in 60 days and then by March 1, 2003, the components moved over. So that means from the time the bill went on the Hill until the Department was created was basically about a year. And from the time of the enactment of the bill until the first component had to move over was a little over 3 months.

Now, we are all astounded when government operates at light speed, but when you do it that fast, you lack the elements of deliberate planning and analysis of alternatives on how you want to do it to actually execute the legislation correctly. And I have talked for

[1] The prepared statement of Admiral Allen appears in the Appendix on page 157.

years about how the conditions under which the Department was formed are some of the issues we have had to deal with.

The legislation was passed between sessions of Congress, so there was no ability for the Senate to be empaneled and confirm appointees, although Secretary Ridge was done I believe a day before he was required to become the Secretary. We moved people over that had already been confirmed because we could do that. And it took up to a year to get some of the other senior leaders confirmed.

We were in the middle of a fiscal year. There was no appropriation, so in addition to the money that was moved over from the legacy organizations from the Department where they were at, some of the new entities, we had to basically reprogram funds from across government. It was a fairly chaotic time to try and stand up the organic organization of the Department and put together a headquarters. Emblematic of that would be the location of the Department that still exists, the Nebraska Avenue complex, and the unfortunate situation where we are right now where we have been able to resolve the St. Elizabeths complex there.

Because of that, what happened was we had the migration of 22 agencies with legacy appropriations structures, legacy internal support structures, different shared services, and different mission support structures in the Departments where they came from. And because of that, a lot of the resources associated with how you actually run the components or need to run the Department rest in the components and still do today. And I am talking about things like human resource management, information technology (IT), property management, and so forth, the blocking and tackling of how you have to run an agency in government.

Over the past 10 years, there have been repeated attempts in the Department to try and tackle some of these problems. The two most noteworthy are consolidation of financial management systems and the ability to create a core accounting system, and the other one would be the attempts to create a standardized HR system for personnel across the Department. These are emblematic, in my view, of the difficulty which you encounter when you try and do these things when they are not pre-planned and thought out. When the legislation went to the Hill, they established a Transition Planning Office in the Office of Management and Budget (OMB) under an Executive Order, but they were legally barred from sharing that because the law had not been enacted and there was not anybody to make a hand-off and that caused some duplicative work.

I will not dwell on the past, but when I talk to folks about how the Department was formed, I think we need to understand that was a very difficult time, and we still carry the legacy of that moving forward.

That said, as we look forward, I think we need to understand that we are confronting greater complexity and a kind of challenge as to the way we think about the Department's missions. And I do not think we can look at them as a collection of components with individual authorities and jurisdictions. We have to have more of a systems of systems approach moving forward. And I think that is the challenge in trying to define the mission set because once

you do that, then you know the capabilities and competencies that you need to have a discussion, and then we can talk about the mission support function, which has not matured to where it needs to be and needs to move forward in the future.

If I could take just a couple of examples, there has been a lot of talk about secure borders, protecting our borders, or managing our borders. And when you really think about it, our borders are not a monolithic line drawn in the land. It is a combination of authorities and jurisdictions, some of which have physical and geographical dimensions, some of which are bands of authority, like the ocean, which extend from our territorial sea out to the limits of the exclusive economic zone. We also do many of our sovereign border functions through analysis of data that facilitates trade and does targeting to understand based on manifests and so forth whether or not there is a threat that is coming into the country.

I think as we move forward, we need to understand that we need to take the collective threat environment out there and look at the consolidated authorities and jurisdictions of the Department and whether or not that is a match.

We have had the first Quadrennial Homeland Security Review (QHSR). That basically validated the budget priorities that were established when the Administration came in in 2009, which pretty much focused on terrorism, the border, disasters, and so forth.

I think after 10 years we need to probably take a look at the fact of whether or not we got the legislation right to begin with, some of the confirming legislation about the legacy authorities that have moved over, and what do the aggregate authorities and jurisdictions of the components that have not significantly changed since the Department was created, and aggregated produce the right legislative base for the Department to move forward and meet these emerging threats as we look to the future.

I think there is an opportunity to do that as we move to the second QHSR. That was my counsel when I was the Commandant of the Coast Guard. I know the Department is working on that. But I think we need to take a look at things like the cyber threat, the fact that resiliency involves not only natural disasters but the interface of the human built environment with the ever-changing natural environment, and take a new strategic view on how we approach the missions of the Department of Homeland Security.

I see my time is up. I thank you for having me here this morning. I would be glad to take any questions you may have for me.

Chairman LIEBERMAN. Thanks very much, Admiral. Excellent and very helpful.

Richard Skinner, welcome back. I am sure it has always been a pleasure for you to testify before the Committee.

Mr. Skinner served as Inspector General (IG) of the Department of Homeland Security from 2005 to 2011 and was Deputy IG from the Department's inception in 2003 to his confirmation as IG in 2005. In both of those capacities, Mr. Skinner was enormously helpful to this Committee in carrying out its oversight responsibilities. He comes to us today as an independent consultant, and we welcome you.

TESTIMONY OF HON. RICHARD L. SKINNER,[1] CHIEF EXECUTIVE OFFICER, RICHARD SKINNER CONSULTING

Mr. SKINNER. Thank you, Chairman, and it is good to be back and good to see everyone again, Senator Collins and Members of the Committee. And it is truly an honor to be here today. I was excited about the opportunity to testify today, and I am especially honored to be with such a distinguished panel here.

I have worked with Admiral Allen over the years when I was the IG, and he is one of the leaders in the Department that I have always admired and respected, and I commend him for his service at the Coast Guard and all he has done for the Coast Guard.

When we talk about Homeland Security and its failings or its shortcomings and its successes, we always tend to want to talk about the operational side of the house, that is, our border security, our transportation security, or our intelligence capabilities. And I think what is often overlooked are those functions that are supporting all of that, behind the scene, so to speak, and that is the management support functions, particularly financial management, acquisition management, IT management, and grants management.

Those are the functions which, in my opinion and my experience at DHS, that constitute the platform on which the Department's programs must operate and are critical to the successful accomplishment of the Department's mission. Some of those challenges that were inherited, those management challenges that Admiral Allen hit upon, when we stood up, the management support functions were, in fact, shortchanged. We brought over all of the operational aspects of 22 different agencies, but we did not bring the management support functions to support those operations. And as a result, we have been digging ourselves out of a hole ever since.

Now it has been 10 years. You would think we would have made more progress than we should have, and we have not. There are a variety of reasons for that, and a lot of it is cultural, a lot of it is budget issues, etc. But the Department is not where it should be as far as maintaining an effective management support operation to support its real mission in protecting our homeland.

Financial management is a good example, and this has been a problem since we stood up in 2003. In 2011, the Department made some progress. For the very first time, it was able to get a qualified opinion on its balance sheet. It reduced its management weaknesses, I think from some 18 materials weaknesses to five. That is a significant accomplishment. But it is also unfortunate because the Department is not continuing to invest in taking its financial management systems the next step forward, and if it does not do that and if it does not invest in building an integrated financial management system, it is unlikely that the progress that it has achieved over the last 10 years, which has been slow, but that progress will not continue.

The Department in 2011 decided to change its strategy for financial management or its Financial System Modernization Program. Rather than implement a department-wide integrated financial management solution, which we know it has tried twice and failed,

[1] The prepared statement of Mr. Skinner appears in the Appendix on page 168.

they are now taking a more disciplined, and I think a very wise decentralized, approach to modernize its financial management systems at the component level. However, if we look at the 2012 budget, you will see that these initiatives have been curtailed, and as a result, they have been put on hold indefinitely. It is not now clear whether the Department will resume its modernization strategy, nor is it clear whether this new decentralized approach, if and whenever it is implemented, will ensure that the component financial management systems can generate reliable, useful, and timely information for managers to use to make informed decisions about their limited resources.

Second, with regard to IT modernization, DHS and its components are still struggling to this day to upgrade or transition their respective IT infrastructure, both locally and enterprise-wide. There has been progress. I remember when we first stood up back in 2003, we did not even know how many IT systems we had. It took us 12 months just to do an inventory. And we found we had well over 2,000, many of them archaic, outdated, and actually useless. Within 2 years from the development of that inventory, I think DHS reduced its systems down to 700, and it has been reduced even further.

So there has been progress, but integrating the systems and networks and capabilities to form a single infrastructure for effective communications—and I think someone hit upon that earlier today, how important it is that we can communicate on a real-time basis and exchange information still to this day remains one of the Department's biggest challenges.

Program and field offices continue to develop IT systems independently of the chief information officer (CIO), and they have been slow to adopt the agency's standard information IT development approach. As a result, systems are not integrated, do not meet user requirements, and do not provide the information technology capabilities agency personnel and its external partners need to carry out critical operations in a timely, efficient, and effective manner.

For example, earlier this week, I believe on Monday, the Office of Inspector General (OIG) reported that the IT environment and the aging IT infrastructure within CBP does not fully support CBP's missions. According to the IG report, interoperability and functionality of the technology infrastructure have not been sufficient to support the CBP mission's activities fully. As a result, CBP employees, particularly out in the field, have created workarounds or employed alternative solutions, which could hinder CBP's ability to accomplish its mission.

Technical and cost barriers, aging infrastructure that is difficult to support, outdated IT strategic plans to guide investment decisions, and stovepiped system development have and continue to impede the Department's efforts to modernize and integrate its IT systems.

Third, with regard to acquisition management, as we all know, those that were around here in 2003, we inherited such a large organization with close to a $40 billion budget, but we had a skeleton staff. We were spending about 40 percent of our budget at that time on contracts, very complex, large contracts, yet we had a skeleton staff to provide oversight and to manage those contracts. And,

of course, as a result, a lot of things went south on us, as we know by SBInet, the TSA hiring program, the Coast Guard's Deepwater program, which has since been corrected. But the Department has recognized this. When I was the IG, I would like to point out that Secretary Napolitano and Deputy Secretary Jane Holl Lute both showed a genuine commitment to improve the Department's acquisition management functions and has been working very hard to do that. However, much work remains to fully implement those plans and address those challenges. Most notably, the Department needs to identify and acquire the resources needed to implement its acquisition policies.

The urgency and complexity of the Department's mission will continue to demand rapid pursuit of major investment programs, as we all know. The Department will continue to rely heavily on contractors to accomplish its multifaceted mission and will continue to pursue high-risk, complex acquisition programs. To effectively manage those complex and large-dollar procurements, the Department will need to show a sustained commitment to improving its acquisition function, increase resources to manage those complex contracts, and engage in smarter processes to administer and oversee the contractors' work.

Finally, I would just like to touch briefly upon grants management because this is something that we spend billions of dollars on year in and year out. I believe to date, since the Department's stand-up in 2003 through 2011, FEMA has distributed over $18 billion through the Homeland Security Grant Program. However, according to an OIG report that, again, was just released this past Monday, FEMA still does not have a system in place to determine the extent that homeland security grant funds enhance the States' capability to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

According to the OIG, in their report that was released earlier this week, FEMA needs to make improvements in strategic management, performance measures, and oversight. Many of the States cannot demonstrate what progress they have made or what improvements have actually occurred as a result of these grant programs, and FEMA or the Department of Homeland Security cannot demonstrate how much safer we are today as a result of spending billions and billions of dollars over the years. That needs to change.

I think that the Department has to develop performance metrics and start holding the States accountable. Without a bona fide performance measurement system, it is impossible to determine whether our annual investments are actually improving our Nation's homeland security posture. Furthermore, without clear, meaningful performance standards, FEMA and DHS lack the tools necessary to make informed funding decisions. In today's economic climate, it is critical that FEMA concentrate its limited resources on those threats that pose the greatest risk to our country today.

It is evident that the Department's senior management are well aware of these challenges and are attempting to fix them, and they have actually made some headway. Does the Department have the resolve and wherewithal to sustain these efforts? The ability of the Department to do so is fragile, not only because of the early stage of development that the initiatives are in, but also because of the

government's budget constraints and the current lack of resources to implement planned corrective actions. In today's environment of large government deficits and pending budget cuts, the new challenge will be to sustain the progress already made and at the same time continue to make necessary improvements.

Unless the Department and Congress stay focused on these challenges, it will be harder than ever to facilitate solutions to strengthen the Department's critical management functions and ultimately to ensure the success of homeland security.

This concludes my statement. I will be happy to answer any questions you may have.

Chairman LIEBERMAN. Thanks, Mr. Skinner. You two were very helpful and very direct. I appreciate it a lot.

We will start with 7-minute rounds of questions for each Senator.

It is striking, of course, and not surprising, I suppose, that each of you in different ways has focused on the unfinished work, the deficiencies in the management operations of the Department. There is a natural tendency, as one of you said, to focus on operations, and operations have gone pretty well; but unless the management functions are carried out efficiently, then the operation of the Department is obviously going to suffer.

I thought you all were helpful in reminding us of the circumstances under which the Department took shape, which were quite hurried both because of the sense of threat that remained very much in the air after 9/11, but also just because of the time it took us to get it going.

I have fallen into the habit of saying that this was the most significant change in our national security apparatus agencies since the end of the Second World War. Certainly together with 9/11 changes in the intelligence community it was. But we did them very quickly.

So let me give you a chance just to give a quick answer on what you think, as this Committee and the Department go forward, are the most important things that the Department and we ought to do to improve the management functions of the Department. In other words, is it money? Is it personnel? Is it for some reason a lack of will to focus on management? What needs to be done? Mr. Skinner, do you want to start first?

Mr. SKINNER. Yes, it is a variety of issues, I think, that are holding us back. Of course, one of them is a resource issue. But we could have done a lot better job with the resources that we were given. We were given a lot of opportunities to make changes, and we did not take advantage of them, and we more or less were spinning our wheels, particularly in the areas of financial management. But it is also a cultural issue. The Department and its components need to come together and realize that for the good of the Department, for the good of the country, and for the good of the mission that they have been entrusted to perform, they have to start working better together. They are going to have to give up some of their turf, so to speak, and work in a more collaborative, cooperative, and integrated fashion. And I think that is one of the big things that is really holding everyone back, and this is particularly evident when we talk about the integration of our IT systems. Everyone agrees at the highest level it needs to be done, but when it gets

down into the grassroots where it is going to affect our operations, that is where we start seeing pushback and the tendency of saying, well, no, I do not want to give up my systems to do this.

Chairman LIEBERMAN. Right.

Mr. SKINNER. We have to overcome that.

Chairman LIEBERMAN. And, not surprising, we watched that happen over the decades, really, in the integration of the Department of Defense, for instance. But what you are saying is that a lot of the components agencies—maybe all of them—have still maintained too much of an independent management structure, including something as critical as IT.

Mr. SKINNER. Yes, and the CIO—and I have issued reports, and I think I have testified previously on this topic—needs to be given the authority to ensure compliance and that components are entering into the department-wide domain with their IT enterprise reforms.

Chairman LIEBERMAN. So that is something you think we should do legislatively?

Mr. SKINNER. That is, I think, something that the Department needs to do internally. I think Admiral Allen stated in his testimony that there are three alternatives: One, top-down; two, bottom-up; or, three, the least feasible would be external driven through legislation.

Chairman LIEBERMAN. Right.

Mr. SKINNER. But unless they do something—because now they are 10 years old. They are no longer infants. They are teenagers. Now they can comprehend what is right and what is wrong. So unless they start doing something to ensure that they are going to be moving in the right direction so that they can support its operations, then maybe external forces would have to be brought into play.

Chairman LIEBERMAN. Admiral Allen, let me bring you into this, because in your prepared remarks you focus on the need for improved unity of effort and operational coordination within the Department, and there is no question that was a main objective that we had in mind in the creation of the Department. So I wonder if you would talk a bit about what you think, if anything, we in Congress should be doing to promote or facilitate those efforts in the years ahead.

Admiral ALLEN. Mr. Chairman, in regards to operational coordination and execution, there have been several attempts to establish a robust planning and execution system that takes place through the National Operations Center on behalf of the Secretary. One of the problems is it was kind of a come-as-you-are department, and a lot of people stayed in the facilities where they were at in Washington, and there was a Balkanization of the facilities. There are a lot of command centers around town that are independent of the Department. FEMA runs the National Response Coordination Center at FEMA headquarters. There is a command center at Coast Guard headquarters.

I am not proposing that we go to a joint structure like we have in the military. That is far too organized for the rest of the government to handle, quite frankly, but to create unity of effort, you need to have at a minimum a way to do planning and coordinated

operations that are synchronized to have the Department fulfill the promise that was created in the Homeland Security Act, not only in the Department but, as you said in your opening remarks, to basically help coordinate that process across the Federal Government.

At that point it comes down to two things. Representative Harman talked about the information intelligence analysis sharing that is necessary to create a common intelligence picture, but all this needs to come together at a fused operations center where all the agencies are represented to create that kind of unity of effort. And there was an attempt made to establish an operational planning and coordination cell up there. There was headway made into the fall of 2008, but I think that needs to move forward, and it is going to require the components to have to participate in that, to put some skin in the game, if you will, to have people up there that are actually working the problem set every day that can reach back to their components to create that unity of effort.

Chairman LIEBERMAN. I appreciate that answer.

Congresswoman Harman, my time is running out, but would you want to add anything to that?

Ms. HARMAN. Yes. I think the key is sustained leadership by the Secretary and the Deputy Secretary. You cannot legislate leadership, but they need to articulate what the focus of the Department is, and presumably Congress should support that articulation or participate in making it. But the Department cannot do everything equally well, and I would suggest that some of the functions should be narrowed, including the intelligence function. I think there is a huge role to collect information from all of the agencies inside the Department and fuse that information together. But I do not think the intelligence function at the Homeland Security Department needs to compete with the CIA or NCTC. I think those agencies are better able to do what they do. And as part of the other structure we set up, this joint command over 16 agencies, the homeland function in a more targeted way I think would be accomplished better. And there is an example of doing less but doing it in a much more effective way.

Chairman LIEBERMAN. Good. Thank you.

Admiral ALLEN. If I could add a comment to Representative Harman's statement?

Chairman LIEBERMAN. Please.

Admiral ALLEN. I think to strengthen the language between the Department and the Director of National Intelligence (DNI), there has been an ongoing discussion whether or not there needs to be a domestic intelligence management function that is resident in the DNI that could create that link. And I think that is something that really needs to be put in place.

Ms. HARMAN. But it would be in the DNI.

Admiral ALLEN. Right, in the DNI.

Ms. HARMAN. It would not be in the Homeland Security Department. It would be a coordinating function.

Chairman LIEBERMAN. And, again, that is possible to do without statutory authority.

Admiral ALLEN. Yes, it is, sir.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Congresswoman Harman, you have had extensive experience not just on the Homeland Security Committee in the House but on the Intelligence Committee, and I know you have continued your interest in homeland and national security at the Wilson Center.

Our Committee, over the past decade, has held a variety of hearings to try to highlight possible vulnerabilities that our country has and how we should respond to them. In your testimony, you have pointed out that DHS has evolved and so have our enemies.

One of the problem that I believe DHS has is figuring out what is the greatest threat and what resources should be concentrated on which threats. Is it a weapon of mass destruction smuggled into a cargo container coming into our seaports? Is it an act of bioterrorism? Is it cargo security? Is it homegrown terrorism? Which we have done a great deal of work on, at your suggestion, I might add. Is it a cyber attack?

If you were Secretary of the Department, what would be your priority? What do you believe the Department's chief focus should be?

Ms. HARMAN. That is a very hard question, and my first answer is it should not just be the Department's responsibility. It is a government-wide responsibility. We have coordinated our intelligence agencies under the Office of the Director of National Intelligence, and I think part of the answer to your question has to come from there. DHS has a role, but not an exclusive role. And as I mentioned, I think DHS is not in the prevention business, certainly not in the cyber prevention business, but it is much more in the consequence management business.

So I think we have to keep in mind that our enemies, at least in this era of terror, are attacking us asymmetrically. They are looking for our weakest links. So if we announce we are focusing on three things, they will attack us in the fourth area. So I do not think that is a great idea.

I think we just have to keep agile and keep looking. Cyber security is near the top or at the top of my list now—and I brought a prop. I thought you would be impressed. Today's *Washington Post* has an article about cyber risks, and there are these new gizmos that integrate everybody's information, and that just makes richer targets out of all of us, so this article says, and I actually believe it. So I think this is a place where the Homeland Security Department, if your legislation passes, should beef up its intelligence and prevention and consequence management capability. There is one issue.

Another issue is I think lone wolves are the growing threat, people with clean records who are radicalized on the Internet, something I tried to work on when I was in the House and still care about.

I think the bigger attacks are harder to pull off because we have been quite effective, and we have also decimated at least core al-Qaeda. That does not mean they cannot happen. And they might happen using ingredients inside our country. It is not always a border question. So, for example, something I have always worried about is some of the radiation materials in machines in hospitals which could be compromised and made into dirty bombs.

So it is a huge problem, but we have to keep agile and understand how these people are coming at us.

Senator COLLINS. Thank you.

Mr. Skinner, I was interested when you described the gains made by the Department as "fragile," and I think that is a good cautionary note to us. When I think back over the past decade of this Department, I can come up, off the top of my head, with numerous examples of failures in procurements: the SBInet program; the puffer machines at TSA; the problems with improper and fraudulent payments in the wake of Hurricane Katrina, which approached $1 billion and your office did so much work on; and IT projects throughout the Department—and the Department is not unique in this regard—that have failed. And you talked about some of those management failures and the importance of having a robust acquisition staff. But another important safeguard is having an effective IG, and you were certainly a very effective watchdog who brought to light a lot of those problems.

Right now, the Department is without an IG, just an Acting IG. Could you share with us what qualities you think the Administration and this Committee should be looking for in a new Inspector General? And if you could also describe for us the scope of the office. This is not only a huge Department. Isn't the Office of the IG one of the biggest in the Federal Government?

Mr. SKINNER. Yes, it is. I think it is probably somewhere between the third, fourth, or fifth largest IG in the Federal Government. In my opinion, the next IG is someone who is going to require extensive executive experience with demonstrated leadership skills. This is not a place for training a leader. This is someone that should have already demonstrated their leadership abilities, and preferably someone that has some type of background or appreciation for audits, investigations, and inspections and who can provide the leadership and the vision for the office. Just like the Department, the IG has multi-missions. Although it is just a microcosm of the Department, it does have multi-missions with regards to policy evaluations and with regards to financial audits. The background that we had in the old days—back in the 1950s and 1960s, I hate to say it, when I entered the government—was strictly financial. But now we have learned that you have to be able to recruit and motivate a whole wide range of people, people that are competent in doing policy evaluations, people that have engineering backgrounds, people that have public administration backgrounds. It goes way beyond just the audit and financial management. The individual who leads this organization should have demonstrated management skills and should have, I think, extensive executive experience.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Again, let me just reiterate our thanks to each of you, not just for being with us today but a lot of other days as well, and for your willingness to continue to serve our country in different ways.

I just want to follow up, if I could briefly, on a point that Senator Collins was making. We play what I call "Executive Branch Swiss cheese" from Administration to Administration. It is getting worse, not better. And 2 or 3 years into this Administration, we still have gaping holes in major leadership roles because in some cases the Administration could not figure out who to nominate, but in many cases, when they did, it took forever to vet them, to go through the nomination process, and the confirmation process in the Senate. We have ended up with big problems in a number of departments. One of those is the acquisition side in the Department of Defense. In the Bush Administration we saw it. We saw it again in this Administration. And when you see major weapons system cost overruns growing about $400 billion—and having to go 18 months with having a vacancy in the top watchdog position in the Department of Defense is just, I think, unthinkable.

But I want to come back to the point that Senator Collins was making with respect to filling the position that you once held and performed admirably. I do not know that the Aministration is going to come back to us and say, well, this is who we think ought to be the person or the right kind of person to fill this role. You have given us some ideas what the Administration should be looking for, and they certainly make sense. But this has to be a priority, and I know it is something you care a lot about, and it is something we just need to work together with the Administration to make sure we get it done. Maybe this is one of those deals that we do and it gets done after the election. I do not know. But it is really important.

These are great hearings, and I think it is unfortunate that more of our colleagues are not here, but I just want to thank you, Mr. Chairman, for providing these for us and for our staffs.

At our hearing we had yesterday with three panelists, there was a fair amount of focus on cybersecurity and looking for a to-do list on cybersecurity. Actually what we are looking for was common ground with Senator McCain sitting to my left and Senator Lieberman over here, our Chairman, to my right and Senator Collins to see if the panel could give us some ideas of what we could do to define the 80 percent or the 70 percent on which we agree and do that this year and not waste more time.

I really would like to ask—this is not a fair question, I suspect, for Mr. Skinner, but I think for Congresswoman Harman and for Admiral Allen, in terms of when you look at the different approaches between the two major bills here in the Senate, a bipartisan bill and the legislation that Senator McCain and others have worked on, where do we find the common ground? Give us some advice on how to meld these together in ways that make sense and get that done this year.

Ms. HARMAN. Well, bring back the Big Four. That would be my first answer. But, unfortunately, I think the hangup is this debate that we keep having about the role of government. I think the argument that the better bill's sponsors make is that infrastructure has to be in the bill. If we are not protecting against cyber threats against critical infrastructure, we are not protecting the country. I am there. I think that is right. I do not think it is a Republican or a Democratic argument. I think it is a proper role of government

to provide for the common defense. It is in the Constitution. It is an oath I took and you all still take. And if we are going to provide for the common defense, we have to protect our critical infrastructure. So I start there.

I suppose if I were doing it, I would find any possible way to keep that in the bill, and then I would negotiate on the other stuff. I know that one of the issues that some of the outside groups are concerned about is how information is shared and about violation of privacy. But, of course, again, if we had a Privacy and Civil Liberties Oversight Board that was functioning, that could help us or help the government develop the regulations that would be appropriate to implement the cyber bill. But with no cyber bill, as Keith Alexander has said recently, "Our country is extremely vulnerable, and those of us who have been briefed in classified settings on both offensive and defensive cyber understand the capability of this tool now."

And just one final point: Ten years ago, when we were setting up this Department, I do not think any of us was talking about this. I do not even know what capability existed then. Certainly there was cyber. And as this threat evolves, we have to evolve. This is a core requirement I think now for the Homeland Security Department, and it is overdue that some strong legislation should pass.

Senator CARPER. All right. Thank you. Admiral Allen, help us out.

Admiral ALLEN. I think Representative Harman hit it right off the bat there. This is really a question about what is inherently governmental and what is the role of government. In a really complex regulatory environment, we always have these questions. I am sure the same questions were raised when the nuclear industry came about, and what should the private industry be doing and what should government be doing.

We faced some of the same problems and challenges looking at port security right after 9/11. I will tell you this. We used to say if you have seen one port, you have seen one port. And I guess you could say if you have seen one sector, you have seen one sector. And when you go between the sectors, I think there is probably a different varying ability for the markets to clear this type of functionality and protect their assets. In other cases, there is not a market-driven reason to do that, and there is probably a valid role for government.

I think what we probably need to do is understand what the standards and the performance are trying to achieve to secure the infrastructure and then apply those standards to each sector. That may produce a different outcome in each one, but at least there is a standard way to think about it and move ahead. And in some cases where there is not a market solution, there is inevitably a role for government. If there is a role for government, there is probably already a standing department that has the legal authorities to do that. It becomes a matter of execution and proper oversight regarding private citizen and personal information.

We need a bill. I cannot urge you more strongly to get a bill out this year. Exactly where that line is on the role of the government from a harder regulatory stand that is requiring these audits and

the development of covered assets that are covered in your bill, information sharing, and industry-led organizations, I think those are things that need to be worked in the Congress as a bill moves through. But I think a bill is necessary. There is a valid role for the government if the government is to play. That role is homeland security. We should build on what has already been done there, even if the progress we have seen to date has not been as significant as we think, but we should move to pass a bill.

Senator CARPER. All right. That is very helpful. There is some convergence here, actually a fair amount of convergence here in the views we just heard, and also with the panel that was here earlier this week. That gives me not just cause for encouragement but just strengthens my belief that we have to move.

Mr. Chairman, I do not know if you are keeping a bucket list, a to-do list of things you want to check off before the end of the year. Clearly we want to finish postal reform. We have already spent plenty of time on that, and the House of Representatives continues to delay taking up legislation. We passed very good bipartisan legislation, not perfect admittedly, but instead of actually taking up a bill and passing it, they continue to delay it and the Postal Service loses $25 million a day. It makes no sense. I do not want to come back and have to deal with that next year. I am sure Senator Collins does not. I might not be back next year. You never know. But I hope to have a chance to serve with her and my colleagues for a bit longer.

The other one that is just crying out to get done is cybersecurity. It is crying out to get done, and my hope is that we will do that.

If I could, just one concluding thought. A lot of times at a hearing like this, during an exercise like this, we focus on the stuff we have not done well, the to-do list that still needs to be done. GAO still has management integration on their high-risk list for waste, fraud, and abuse. A lot of good has been done. There are thousands, maybe tens of thousands of people in this country that are still alive, unharmed, unmaimed, they have lives, jobs, families, and so forth because of the protections that are put in place, in no small part because of the work that has been done by the Department that we stood up 10 years ago. I think that is important to keep in mind.

The other thing, I am a Senator, like some of you, who cares a lot about trying to make sure we figure out what works, as Congresswoman Harman said, and to make sure that we are spending taxpayers' money as cost-effectively as we can. We are looking at this fiscal cliff at the end of this year. We are going to have to figure out how to raise revenues. We are going to have to figure out how to spend more cost-effectively. One of the very encouraging things for me, as the guy who was involved, along with Senator Bill Roth years ago, in the creation of the Chief Financial Office and Federal Financial Reform Act of 1990, which said all Federal agencies have to have auditable financials. And lo and behold, Secretary Napolitano announced earlier this year, maybe late last year, they are going to be auditable way ahead of the Department of Defense. Finally the leadership we had been hoping for. And I think you cannot manage what you cannot measure, and I think we are making progress there.

So there is some very good work that has been done in the last 10 years, and we need not lose sight of that. Thank you all.

Chairman LIEBERMAN. Thanks very much, Senator Carper.

Just responding to your question, I do have a bucket list, and, as a matter of fact, I think I have engaged Senator Jon Kyl at least in the formation of a Bucket List Caucus, and I will tell you that at the top of the list is cybersecurity. And Senator Kyl is working very hard now with Senator Sheldon Whitehouse in a bipartisan effort to reach a meaningful compromise on the cybersecurity bill. But the priorities for the Committee I think are clearly cybersecurity and postal.

Incidentally, just to say what I think all the witnesses know, but it cannot be said too much, just reflecting on your strong statements about the need to have a cybersecurity bill adopted this year—unfortunately there seems to be somewhat of a partisan divide on this question in Congress. Among those who have had responsibility for our national and homeland security across the last two Administrations—that is, the Bush and Obama Administrations—there is real unanimity of opinion that we have to adopt a bill, and I think I am not stretching to say that they support a bill like the one that came out of our Committee. So it is not just people in the current Administration and the President, but Secretary Michael Chertoff, Admiral Mike McConnell, who I believe is your colleague, Admiral Allen, at Booz Allen, and Stewart Baker. So I hope that will have an impact in helping us get over 60 votes in the Senate.

Senator CARPER. If I could just add quickly. Senator Collins, you, and I said to our respective leaderships on postal, the only way we are ever going to finish a postal bill is to get the bill on the floor, debate it, amend it, and vote on it. And I think the same is probably true with cyber. We have to get the bill on the floor. I am encouraged that the Democratic leader—and I hope the Republican leader—believes in that and during this work period, while we are here before August, will actually do that.

Chairman LIEBERMAN. Thank you.

Senator Johnson, I was just thinking, as we referred to Cal Ripken, I would say you are the rookie with the most Cal Ripken-like record on this Committee, which I appreciate. You have really been very steadfast in your contributions here.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Well, thank you, Mr. Chairman, and thank you and Senator Collins for holding these hearings. For somebody new, these are extremely helpful. I am learning a lot, so thank you.

And I would also like to thank the witnesses for your time and your testimony and also for all of your service to the country.

As somebody new—I was not around here, you were—I would like to ask each one of you, what was the primary rationale or reason for establishing the Department. I want to go down the list. And if a previous answer is your answer, you can tell me the second one, but I also want you to acknowledge that was the reason. I will start with you, Congresswoman Harman. And, by the way, for the record, I want to say I smiled when you said that 90 percent of the work was done by the women on Fab Four. [Laughter.]

Ms. HARMAN. I appreciate that.

I remember the time vividly. We were all here on 9/11, and I was then a very senior member on the House Intelligence Committee, walking to the dome of the Capitol, which most people think was the intended target of the fourth plane that went down in Pennsylvania, so it focuses the mind. We had no evacuation plan here. We, unfortunately, closed these buildings. A huge mistake. We reopened them later in the day, but, nonetheless, it was terrifying, which is the point of a terror attack.

At any rate, I felt—and I certainly know that Chairman Lieberman did—that our government organization was completely inadequate to the new set of threats, and we needed something different. We had missed clues, obviously. Two of the hijackers were living in plain sight in San Diego, and the FBI did not talk to the FBI internally and, of course, did not talk to the CIA, or we might have been able to find them and unravel the plot. So the goal was to somehow find a better way to put government functions together.

As I mentioned in my testimony, many of us thought there was a simpler way to do this, but we embraced what President Bush proposed because we knew he would support that and we would get something done.

Senator JOHNSON. Admiral Allen.

Admiral ALLEN. Senator, the concept of a border security agency actually predates 9/11. There were discussions about trying to do something like this clear back in the Nixon Administration regarding border control on the Southwest Border. So the concept itself is not novel.

As former Commandant of the Coast Guard and somebody that has worked with these agencies for nearly 40 years before I retired, the relationships between the Coast Guard, FEMA, Immigration, and Customs have never been better. FEMA is a better organization because they are in a Department with the Coast Guard, and the Coast Guard is a better organization because they are in a Department with FEMA. And I testified to that after Hurricane Katrina.

I was also asked by Senator Frank Lautenberg one time, what was the best thing about the Coast Guard being moved out of the Department of Transportation, because he was our Chairman, moving to the Department of Homeland Security. At the time I said we got our appropriations on time. I am not sure anybody can say that anymore.

There was an all-out bureaucratic war between the Coast Guard and Customs in the mid-1980s over who would do air interdiction and maritime interdiction in this country. It was internecine warfare and it was ugly. That does not happen anymore, and while there have been overlaps and things to talk about how we can coordinate better and create unity of effort, some of the bureaucratic struggles that I saw throughout my career have gone away.

Senator JOHNSON. That was how many agencies? About five that you are talking about that you were originally thinking about?

Admiral ALLEN. The original border security, that has been a discussion that has gone on for years. Sometimes it was just border focused.

Senator JOHNSON. But of the 22 agencies, how many of those——

Admiral ALLEN. I think originally they would be talking about Immigration, Customs, Coast Guard—the organizations that actually have a physical presence on the air, land, or sea domains and borders. But it had been something that had been discussed for quite a while.

Senator JOHNSON. Mr. Skinner.

Mr. SKINNER. I agree with Admiral Allen. The whole concept of homeland security predates 9/11 actually. As a matter of fact, I think there was actually a bill that was introduced and it was closeted a couple years prior to 9/11. It was brought out and dusted off, and I think that started the ball rolling for getting the legislation that we now have through the Congress so fast.

Quite frankly, the whole concept was to have unity of effort, to bring together the different functions within government so that they can work better together to not only protect or prevent another terrorist attack, but also to develop a resilience and an ability to respond and recover from a terrorist attack should one occur. So it brought together these different elements that would sit under one roof, one leadership, with one common mission, that is, to prevent, protect, respond, recover, and mitigate against not only a terrorist attack but also natural disasters.

Senator JOHNSON. Here is my concern. My bias, having been part of a small company that got bought by a larger conglomerate and then demerged, I have gone through that merging process on a far smaller scale, I understand that, but I also understand that when you go into a larger organization, so much of your effort then is directed toward basically feeding the beast, trying to do all these things we are trying to do with integration, and I guess that is my question. Have we created something that is simply too big to manage? We have a Department now that is 200,000 people. It has $6.5 billion worth of overhead. And should we be taking a look at maybe splitting out some of those? Should we maybe demerge some of these into some different areas? I guess I always thought it was kind of breaking down the silos, information sharing, maybe take that back to the national intelligence level for that sharing. Is there a more intelligent way of potentially taking a look at this? These agencies were large bureaucracies to start with. Now we have made something even larger, and have we actually made it less effective?

Ms. HARMAN. Well, on the front end, I think we bit off too much, but we made a tactical, political decision that, along with the President's proposal, this was the fastest, easiest way to get something to happen. There have been huge growing pains. It has been 10 years, and still some functions are not done well.

Yes, I would recommend narrowing some of the functions. But I would be against rearranging the deck chairs again because I think that is an extremely painful exercise for any organization, and this one is finally, in many respects, becoming a cohesive organization. More leadership to integrate some functions that are still not integrated would be good. Sustained leadership in the next Administration would be excellent. But I think it has come a long way, and it really has served the function, by and large, of protecting our country along with oversight of Congress.

If I had to pick an area to reorganize right this minute, it would be Congress. I think this Committee should have a lot more jurisdiction than it does, and that is true on the House side, too.

Senator JOHNSON. Thank you.

Admiral ALLEN. Sir, I think it is hard to disaggregate the inelegant conditions under which the Department was formed that I discussed earlier and the issues you talked about, about management, the size, the span of control, and so forth.

We are going to have to get over the first part. It has been 10 years. The country expects the Department is going to start functioning better, and I think that is a mandate for the Department.

I think, on the other hand, there is a leadership management imperative here that has not been exhausted yet, and I would support Representative Harman's comments there. I think we have an opportunity, as we move to a new Administration or continuity of the current Administration, to have a leadership management agenda that is focused on the Department, that takes care of the basic X's and O's of blocking and tackling. And I think until we have done that, we have not exhausted the potential for the Department.

Mr. SKINNER. Senator, I would like to also add that I agree wholeheartedly with Congresswoman Harman. This is not a time to rearrange the deck chairs. If you study the history of the creation of the Department of Homeland Security, you have to understand the environment in which it was created. It was a very emotional environment. This country was very upset with what happened on 9/11, at what happened in New York, here at the Pentagon, and also in Pennsylvania.

This bill was pushed through very quickly, at a historic pace, and we were not given the opportunity to think it through so that we could prepare ourselves. We saw this at TSA when we stood that up, hiring all the screeners in record time, and as a result, we had to go back and redo a lot of that. But that environment in which we stood up created a lot of our problems when we did not think it all the way through. For example, I said earlier we shortchanged the management support functions when we stood it up. We brought in all the operations without the management support to back these operations.

Senator JOHNSON. Let me just close with an interesting article that I read in *Newsweek* where basically Secretary Robert Gates was talking about when he came in, Secretary Donald Rumsfeld said there were 17 layers between his command decision and the implementation in the military. Now it is 30. That is not moving in the right direction in terms of efficiency, and that is my primary concern about the Department of Homeland Security as well.

Mr. SKINNER. Actually, the Department has reduced layers, because when it was originally stood up, the Secretary had the opportunity, and the President, with congressional approval, to reorganize, which they did, and they have actually removed layers. Now I think the layers that remain need to be empowered, particularly in the management support arena. The progress we have made to date I think is substantial. I do not think the Department does a very good job of marketing itself. It still has a long way to go. The biggest threat I think the Department has for its success right now is the budget constraints, the ability to sustain what they have al-

ready started and the ability to make the improvements they need to move forward and to address evolving threats.

Senator JOHNSON. Thanks a lot. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Johnson. That was a really constructive exchange.

Senator Akaka, welcome. Senator Akaka is another Member of our retiring class who is characteristically involved in a very constructive way on our Committee's two priorities, which are the cybersecurity bill and the postal reform bill. So thank you for that, Senator Akaka, and it is your turn for questioning.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, and also I also want to thank Senator Collins for her efforts on this Committee and for holding this hearing to examine DHS, and also to discuss some reforms that can improve the efficiency and delivery of services of this Department for our country. So I want to thank you very much for this opportunity.

I also want to take the time to thank the Federal workers. As you know, I have always been concerned about our human capital, and here it is, one of those situations where our Federal workers have responded, and I want to thank them for their response, called to service since September 11, 2001. And so here we are now examining what has happened and how we can improve it.

I would like to ask Congresswoman Harman, your written testimony notes improvements of the DHS Privacy Office and an urgent need to stand up the Privacy and Civil Liberties Oversight Board. I strongly agree. As you know, dramatic technical advances in the past decade allowed DHS to obtain and use Americans' personal information in new ways.

What are the key privacy challenges that DHS will face in the future? And is the Department really equipped to address these challenges?

Ms. HARMAN. Well, thank you for that question, Senator Akaka. And, by the way, life outside of Congress is quite sweet. I want to assure you and Senator Lieberman that I am really OK and enjoying my life.

On this, I watched carefully as the Department developed, and I have seen progress and good effort in the privacy protection area. So I do not want to be critical. What bothers me as a more general matter is the absence of people inside the Executive Branch as policy is formulated there, as regulations are developed or new actions are contemplated, who say, wait a minute, there is another way to think about this or there are more things to think about. As I have often said—in fact, Benjamin Franklin said it first, I am sure, better than I am going to say it—security and liberty are not a zero sum game. You either get more of both or less of both. You have to factor them both in on the front end. If you think of them as a zero sum game and we have threats against us, then we are going to basically shred our Constitution. None of us wants to do that. And if you, alternatively, just punt, then after we are attacked, we are definitely going to shred our Constitution. Bad idea.

So my basic point is we need advocates all over, in the right rooms, at the right time, as the Executive Branch contemplates se-

curity actions. What DHS is doing inside of DHS is pretty good, although I have seen some problems. They relate to what information is collected, how long it can stay there, and who has access to it—the usual stuff like that. But, again, I think the others here, maybe Mr. Skinner, more than any of us, can answer whether the systems are working.

But I saw a couple of things there that I was able to stop. One of them was the National Applications Office (NAO). It was going to task satellites, basically our defense satellites, to accomplish certain homeland security missions over the continental United States, and that worried me because I did not think the guidelines were specific enough. And what ended up happening was NAO, I think, was discontinued, which I thought was a very good outcome.

Senator AKAKA. Thank you, Congresswoman Harman. This week the *National Journal* poll released information that almost two-thirds of respondents said that the government and businesses should not be allowed to share cybersecurity information because it would hurt privacy and civil liberties. You also note in your testimony the need to protect personal information in the event of a cyber attack.

Will you please discuss the importance of including robust privacy and civil liberties safeguards in any cybersecurity legislation considered on the Senate floor?

Ms. HARMAN. I think it is very important. What the final version of the legislation should look like I do not know. But, again, it is the same point, that security and liberty are not a zero sum game. We have to think about how to protect information as we also are blocking access by either business interests that are stealing information or government interests that pose, I think, a grave threat to all of the dot-mil, dot-gov, and dot-com space. These are serious tools, and the point of cybersecurity legislation, obviously, is to protect our personal information, but also our government secrets. So that is the point of the legislation. But individuals should not be forced by the legislation to share data that it is unnecessary to share.

So it is complicated. I just have to look at the specific language. But I think the bill authored by Senator Lieberman and Senator Collins is closer to what I think would keep our country safe and protect our critical infrastructure.

Senator AKAKA. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Akaka.

If the witnesses have time, I have just one more line of questions, a little bit different than we have focused on, and it builds on yesterday's hearing when we discussed with the experts an interesting, in some ways unsettling range of potential future homeland security threats. And I wanted to ask you what your assessment is of the current capabilities within DHS to assess and identify future threats and then obviously to take actions to address them, and if it is not adequate, what we might do about it. And I do want to go down the road, and, Admiral Allen, as you well know, the Coast Guard has an internal futures planning initiative called Project Evergreen, and I would like you to talk about that and how it might relate, if it does, to DHS overall.

Congresswoman Harman, do you want to begin that? Is there within DHS the capability to accurately, or adequately anyway, anticipate changing threats and respond?

Ms. HARMAN. I think I am least qualified on this panel to answer that because I have not been in the operating mechanism of the Department. But I think it is uneven, would be my answer. I think some threats are better understood than others. And as I mentioned in my answer to Senator Collins, if we give a pat answer to that question, then the bad guys will somehow plan around us. We cannot do that. We have to be ever agile and reassessing that all of the time.

But I do not think most of the planning mechanisms are that good. The ones I have seen that I like the best have to do with airplane and airport security, which I think work very well. And we authored legislation, Senator Collins and I, on port security, which involves—and obviously Admiral Allen knows all about that—pushing borders out and layers of protection. And I think that one works pretty well. But I do not know how to answer that across the whole range of threats.

Chairman LIEBERMAN. Good enough. Admiral Allen.

Admiral ALLEN. Yes, sir. To answer your first question, about 10 years ago or 12 years ago, the Coast Guard initiated a project called the Longview Project, and this was trying to look strategically into our future using alternative scenario planning, which is a planning method the Royal Dutch Shell Company had put in about 20 years ago, a leading consultative method to try and figure out what you should do to plan for the future. To summarize it, you get your senior leaders, you look at the consequential trends that are out there, and you develop alternative worlds that you might see. And then you reduce that to the four or five highest risk or most consequential. Then you isolate teams, and they come up with strategies on how you would cope with that world. And they do not talk to the other ones.

When you bring them back in, you compare what they all said, and if you have five very different worlds, of the 10 strategies they come up with each world, three or four of them the same—those are robust, apply to a variety of threats, that is something you should probably look at as you try and look at your own capabilities and competencies.

The Coast Guard is on its third or fourth iteration. We termed it the "Evergreen process" because our goal was to regenerate it about every 4 years. It has been extremely helpful to us. When I became chief of staff of the Coast Guard after 9/11, I actually graded our performance on 9/11 against what we thought was going to happen when we did not know the events in New York were going to occur, and there were 10 things that we said we should do. We did six or seven of them. The three that we did not do would have helped us had we done them. And my response was from that old management book, "Who Stole My Cheese?" What would you do if you were not afraid? And we thought it was very insightful.

Regarding the larger question, what I said in my written testimony—and I will try and summarize it succinctly here—you cannot stand at a port of entry and view homeland security and say, "What is it I should do?" You cannot stand at a screening line ei-

ther in the country or in Dublin and say, "What should I do regarding airline passengers?" I think we need to understand that we have both a physical and a virtual dimension of our borders where we need to carry out sovereign responsibilities. And for ease of explanation, what I usually say is we have air, land, sea, and actually a space domain, and they are all surrounded by cyber. And through those domains we have flows of things we need to be concerned about.

Deputy Secretary Lute has a good way of saying it. We need to interrupt the supply chain of trouble. And the things that flow through those domains are things like people, cargo, conveyances, but it is also weather, germs, electrons, and money.

I think what we need to start understanding is, notwithstanding the components and their individual authorities and jurisdictions, as I alluded to earlier, at the departmental level, in both principle as well as policy and operational planning and coordination, how do we sense those domains and those environments? What is passing through them? What represents the threats in those domains? You can almost look at a portfolio and you can start making tradeoffs based on risk of where you need to put resources, including redeploying workforces on the Southwest Border, redeploying maritime forces, heightening threat levels in advance of a national security event, and so forth. It requires, in my view, to step back and view the homeland security enterprise radically different than the collection of the authorities and jurisdictions of the components.

Chairman LIEBERMAN. Thank you for that. You give us a lot to think about. Mr. Skinner, do you have a reaction to the question?

Mr. SKINNER. It would be hard to add to what he just said.

Chairman LIEBERMAN. That was a pretty good answer.

Mr. SKINNER. It certainly was. As the IG, I do recall doing some reviews with the Department, particularly in TSA and CBP. We were always looking for emerging threats because they knew if they shut down one lane, they would find other avenues to smuggle contraband or illegal items onto airplanes or through our borders. So I know that from a stovepipe perspective we were always looking at what are they going to do next now that we have identified this technique.

As far as strategic planning and strategic assessments of what our threats are, I am not aware of that occurring within the Department, but that does not mean that it is not occurring.

Finally, I would just like to make the point that when we talk about evolving threats, this is not just a DHS responsibility. This is a governmentwide responsibility.

Chairman LIEBERMAN. Right.

Mr. SKINNER. And we have to rely heavily within the Department on what is going on outside government, and I think Admiral Allen put it very well. It is the intelligence that we garner, dealing with what is going through our systems or what is happening inside that cyber circle. So people who have those expectations saying this is solely a DHS responsibility—I think it would be misleading or a big mistake just to focus on DHS.

Chairman LIEBERMAN. Yes, I agree. I just want to come back and ask you a final question, Admiral Allen, about that exercise you went through with the Coast Guard. I assume you were looking at

a lot of factors that might not to the immediate observer seem like they were relevant to the Coast Guard function. In other words, it seems to me that one of the things I would hope that DHS does is look at worldwide demographic trends. I also mean, of course, with regard to natural disasters, environmental, or meteorological trends. But I also hope they think about the terrorism threat, what is happening out in the world that we may not be thinking about now that, nonetheless, could—or what is happening in the technological world that may be converted to a weapon against us, as you know, planes and cyberspace have been.

Admiral ALLEN. That is what we try to do, sir. One of the scenarios was you try and drive at the polar extremes. One is globalization where financial markets drive to the point where it starts to question the value of nation-states. The other one is a pandemic that basically goes global and redefines socio-political boundaries and implications related to that, or natural disasters. And what you do is you try and bring your leaders in and try to understand which one of those are most consequential or impactful or provide the greatest risk. And you can talk about it from an agency standpoint.

There was a project called Project Horizon where the State Department tried to do this on an interagency basis about 10 years ago.

Chairman LIEBERMAN. Yes.

Admiral ALLEN. But it really never got the traction inside the government. It is a useful project. It requires some investment in time. It requires some championship at the leadership level. But it also allows you to learn about some junior and mid-grade people that take part in these things as a leadership grooming process. There are current admirals in the Coast Guard that I first met as lieutenants in these work groups talking about what they thought might happen in a port after a weapon of mass destruction event. You were able to see these people being very thoughtful and very resourceful in how they bring their thinking to the problems.

Ms. HARMAN. Senator Lieberman, could I just add one thing?

Chairman LIEBERMAN. Yes, ma'am.

Ms. HARMAN. As we think about these big, huge threats or potential catastrophic threats, it is still important to drill down on the smaller threats. Senator Collins mentioned the underwear bomber who was unable to detonate—good news—a bomb that was external to his body. Now the worry is that tradecraft has evolved so that there can be internal bombs. Much like human mules carrying drugs, that will evade some of our detection systems. And at that level, I think we need very sharp focus because I think that things of that kind are going to continue to happen. There is one particular bomb maker in Yemen—who seems to be the ace bomb maker of all time—who still is alive and well and doing this. Maybe there will be others, and maybe there will be others in this country. So it is not just a question of borders. It is a question of very smart, focused thinking about what these people could do next.

Chairman LIEBERMAN. Good point.

Admiral ALLEN. You mentioned technology, Mr. Chairman. I think when you look at the advances in nanotechnology, mass com-

putation in smaller areas, battery technology, and things like that, you start creating the art of the possible and ways where threats can be applied in different ways. So I think there is a technological thing that we have to keep our eye on.

Chairman LIEBERMAN. Yes, I agree. This is a tall order, but investing a little bit in this kind of future thinking out of the box for right now probably would save us a lot in the years ahead. Thank you very much. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Admiral Allen, it was very helpful to hear from you some of the problems that existed prior to the Department of Homeland Security's creation to remind us that it is not as if all these agencies were working cooperatively before they were brought together and somehow bringing them together made them not work as well.

Nevertheless, as I was reading your testimony, I could sense a certain frustration with how the Department could be functioning better. For example, you talk about a lack of uniformity, comparability, and transparency in budget presentations across the Department. You say that the Department has struggled to evolve in operational planning and mission execution coordination capability. And you say in your conclusion, "Something has to give."

What do you believe needs to be done to solve some of the problems that you illustrated in your written testimony?

Admiral ALLEN. If I could, as I did in my written testimony, I would like to divide it into two answers. One involves mission execution, and one involves mission support. I used to tell the people that worked for me in the Coast Guard, "If you go to work every day, you either execute the mission or you support the mission. And if you cannot explain what you are doing, we made one of two mistakes. Either we have not explained your job or we do not need your job." So I would like to give you two answers.

On the mission support side, let us go to appropriations, because I think you hit the place where there is discretion to do something.

We moved components into the Department with different appropriations structures from the legacy departments. And you are all familiar with this. I am talking about the appropriations level, the project, program, and activity levels that create the firewalls which you need to reprogram between and how you represent personnel costs, operating costs, capital investment costs, IT costs, and so forth.

Right now, because of the way the budgets were formed in the legacy departments, you cannot put the budgets side by side and look at comparability on personnel costs, salaries, operations and maintenance, and capital investment. There are two sides to this. The Administration needs to put forward a budget that has comparability in the way the numbers are presented, and the Appropriations Committees are going to have to understand that there is going to have to be some flexibility to put this together where we have a comprehensive and understandable basis by which to us how we are funding the Department and the costs associated with that.

That is something that does not need any legislation. That is a management activity both in the Department, at OMB, which plays a big part in this, and on the Hill.

One key thing regarding this is the requirement in the Homeland Security Act to have a Future Years Homeland Security Plan like the Future Years Defense Plan. We have never realized that. There are a lot of forces inside the Office of Management and Budget that do not want to commit to a 5-year projection, but this really kills capital investment and acquisitions management. We have breaches in acquisition programs that are budget-induced, but you do not see that because there is never an open discussion about having a sustained, consistent 5-year capital budgeting plan.

On the mission execution side, it has everything to do with unity of effort, which is undergirded by operational coordination and planning. If you talk about the threat environment that I discussed and all the different domains, that is hard to do at a component level. But we need to create the capacity and the competency at the departmental level to be able to look at this thing as a portfolio and to talk about future cases, to look at how do you trade off what can pass through those domains—germs, electrons, money, people, conveyances, and so forth.

We have to create the capacity to be able to discern the important few from the many that are out there that they have to deal with every day. And we have to create the capacity and the capability to do that close to the Secretary so the Secretary can be consequential in the planning and the execution of ongoing operations, then export that competency with credibility across government.

Senator COLLINS. Thank you.

Mr. Skinner, you talked about how the Department initially had, I think it was 2,000 different IT programs and that had been narrowed down, but there are still many different IT programs operating within the Department. And I was thinking when Senator Johnson was talking about the tension between being part of a great big organization versus a smaller organization, which can be more efficient and effective, that a fundamental issue that has never really been answered about the Department has to do with the amount of authority at the Department level, the Chief Information Officer (CIO), the Chief Financial Officer (CFO), Chief Acquisition Officer, all of those positions should have.

What is your view on that? Should the Secretary-level positions have authority over the component agencies in the area of information technology, for example?

Mr. SKINNER. If you go back and look at some of the work that we have done over the years, we have always had concerns, first, that the CFO did not have the appropriate authorities to compel the components to follow certain guidelines or to perform in a manner in which the Department or the Secretary had envisioned. Second, I had reported and made recommendations that the CIO did not have sufficient resources in the Office of the CIO. And the same holds true with the Chief Financial Officer. We have studied and made recommendations that the Chief Financial Officer as well be given additional resources and authority to ensure compliance at the component level.

One of the things I would like to add is that because when we stood up and the components were brought together, they retained their authority, oftentimes because it was the environment in which we were living, and it was a very emotional environment—

expectations were too high. We thought now that we have the Homeland Security Department, all of our problems are going to be solved. Well, we knew that was not going to happen, but the public did not know that, and the media took advantage of that. And, second, it was that the mission demands that were put on us at that point in time in our history trumped good business practice, because we were hearing we expect this to happen, we expect to secure our borders, stop illegal immigration—everything had to be done yesterday, and that trumped good practice. We made a lot of mistakes, and I think we have learned from that. The dust has settled. Now we are able to analyze exactly what we have done, what lessons were learned, and where we want to go. Now it is just a matter of getting the resources and authorities to get it done.

Senator COLLINS. Thank you. Admiral Allen.

Admiral ALLEN. Coming back to Senator Johnson, because your analogy to the business world, and I understand it, you have every right to ask that question. This was probably done without due diligence.

Chairman LIEBERMAN. Thanks, Senator Collins.

I want to give Senator Johnson and Senator Akaka a chance to ask questions if they have more. Congresswoman Harman, I understand you may have to leave soon. If you do, we will understand—and still love you.

Ms. HARMAN. Is that a hint?

Chairman LIEBERMAN. No. I do not think I have ever said that to a witness before. [Laughter.]

Ms. HARMAN. Well, thank you, Mr. Chairman. I love you, too.

Chairman LIEBERMAN. Thank you.

Ms. HARMAN. If it is one more round of questions by two people?

Chairman LIEBERMAN. Just Senator Johnson and Senator Akaka.

Ms. HARMAN. Yes, I would be happy to stay.

Senator JOHNSON. Just a quick one. When we were talking about cybersecurity yesterday, I was asking about, again, the priorities of what needed to be done, and I really came away from that as the first thing is we have to set the standards. So I just want to quickly ask all three of you: Who do you believe is best capable of setting the standard on cybersecurity?

Ms. HARMAN. I think the technical expertise on cybersecurity is in the NSA and should remain there. They are best at it.

In terms of being the public face to do the cybersecurity work that is especially not in the dot-mil and dot-gov space, I think the Homeland Security Department has to do it, implement it. But I do not think it should try to re-create the technical expertise of the NSA.

Admiral ALLEN. I think there is a role for government in oversight of the standards. If I could give you an analogy, the blowout preventer that failed in the Deepwater Horizon spill 2 years ago was built to industry standards, but was not subject to independent third-party inspection mandated by the government. It is now. So I think we need to understand what the role of government is and how we produce the effect. I think there should be oversight. I think it is logical it should be in the Department of Homeland Security. How you evolve the standards can be part of how the legislation is put together, but that has to be affirmed, there has to be

accountability, and somebody has to be able to act on behalf of the American people.

Senator JOHNSON. Thank you. Mr. Skinner.

Mr. SKINNER. I believe it is going to be a collaborative effort. I think NSA plays a major role. I also believe the National Institute of Standards and Technology (NIST) plays a role, and the Department of Homeland Security plays a role as far as establishing standards. And those standards are not going to be set in stone. They are going to evolve over time because cybersecurity is evolving over time.

And as far as providing the oversight at least on the domestic side of the house, I believe that should rest within the Department of Homeland Security. That is a logical home for it.

Senator JOHNSON. Those were very government-centric answers. Is there any role outside in terms of the private sector in terms of the service providers and that type of thing?

Admiral ALLEN. If I could just add, I think that is a performance outcome. My basic training in public administration is in executive, legislative, and regulatory management. I worked in the regulatory field for a couple of decades. One of the things we have to watch out for is we do not get this into a rulemaking process that takes 10 years. That just cannot work. So whatever we do that involves government has to break the paradigm to bring the best of the private sector and get to a conclusion. What we want is a violent attack of sanity. The question is how to do it.

Ms. HARMAN. And if I could just add, as Senator Collins said, 85 percent, I think, of our capacity is in the private sector, and the private sector in this area is much more agile than the government sector. So this has to be a collaborative effort. I thought you were asking about the standard setting. Yes, the legislation should set the standards or set up the process to set the standards. The point I was making is that inside government, our technical competence on this is at the NSA.

Senator JOHNSON. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Johnson. Senator Akaka?

Senator AKAKA. Thank you very much, Mr. Chairman. I know time is valuable to the Congresswoman, and I just want to say I do not have any more questions for you if I am the last here, meaning you can leave if you need to.

Mr. Skinner, I want to say that we have a great panel of leaders and experts here today, and we are fortunate to have you. Mr. Skinner, as you noted in your written testimony, DHS has relied heavily on contractors since its inception, in particular in service contractors working side by side with Federal workers. I have worked closely with the Department on its efforts to right-size its Federal employee-to-contractor mix.

Does the Department currently have the right Federal employee-to-contractor balance to achieve its mission in the future?

Mr. SKINNER. I can only say at the time of my retirement, no, it did not. But at the same time, I was aware of the initiatives to bring that right balance, and I have been reading reports and observing what is going on within the Department. I am still emo-

tionally attached, even though I am retired. And I see that there is progress being made there.

But, nevertheless, there is still an imbalance. I know recently the Coast Guard has made tremendous progress in bringing in in-house employees to do what was inherently governmental jobs instead of relying on contractors. But at the same time, they still do not have—and this is as recently as maybe 2 to 3 months ago that I read this—sufficient resources to complete their mission. So they are still relying on contractors to do what they would like to be doing themselves. But there is a very concerted effort, and I think this has been at all the components as a result of the leadership that I have seen Secretary Napolitano and Deputy Secretary Lute bring to the acquisition management process.

Senator AKAKA. Admiral Allen, as you know, the Department has worked very hard to improve its strategic human capital functions. However, DHS still faces challenges in implementing its department-wide workforce objectives and goals, such as improving employee morale and retention.

What are the most pressing challenges facing the DHS workforce? And how do we address them going forward with DHS?

Admiral ALLEN. Thank you for the question, Senator. I have provided the staff with a statement I made, and they can provide it for the record.[1] In March, I testified before Representative McCaul's subcommittee, the House Homeland Subcommittee on the Partnership for Public Service rankings and morale at the Department. There is a more extensive discussion on that there. I will try and highlight some of the issues here.

Some of the issues derive from the nature by which the Department was formed that I have talked about. Let me hit those real quick because they are technical, and then I will get to the other ones, which I think are equally important.

I will give you a good example. When the Immigration and Naturalization Service went away and we formed Immigration and Customs Enforcement (ICE) and the CBP, we recombined two different workforces that came from two different departments with different appropriations structures, different pay/benefit structures, different work rules, and different grade structures. The ability to try and estimate salaries in that environment continues to be a problem today in CBP, plus a lot of their salaries are funded by, I think, five or six different fees that are legacy fees from Agriculture, Immigration, and Land Border Entry. That is a pretty difficult environment to try and manage and create a human resource program and adequately address and estimate salaries.

The implications of that is there is not enough money, they have to do things in the middle of the year, employees know that, and it affects morale. So I think fixing some of these structural issues will have a salutary effect on the workforce, in my view.

Now, separate from that, on the discussion of morale of the Department, what I said in my previous testimony was morale is not something that you mandate or set out as a goal and achieve. Morale is a by-product of performance in the workplace, where employees feel they are empowered and have the right tools and un-

[1] The testimony referenced by Admiral Allen appears in the Appendix on page 186.

derstand that their leadership are doing the things that are going to enable them to be successful. When you have that, you have morale. And so I think what the Department needs to do is put the conditions in place which improve the performance that we have talked about here today, and I think morale becomes a natural by-product of that.

I think we need to understand people do not leave organizations. They usually leave bad bosses. So I think there is an imperative on leadership training in the Department. There is a DHS fellows program. They have just established a Department of Homeland Security capstone program for senior executives. We now have a leading edge program for executives across the Federal Government.

I believe there ought to be some leadership development programs that are created, fenced off in the budget to become programs of record that do not require the people that are managing these programs to go hand to hand every year and try to deal with reprogrammed funds or what is left over at the end of the year.

Senator AKAKA. Well, thank you very much for that.

I would like to finally ask Mr. Skinner, in particular, it seems as though we have had morale problems, for instance, in TSA. The turnover there is great and has been, and it seems as though it is a part of DHS where the workers have problems.

Can you make any expressions on that and the problem and the challenges that we face in particular in TSA?

Mr. SKINNER. Senator, this is something I have never studied with regards to TSA. I was well aware of the turnover issues there, and we did discuss this with the TSA administrators when I was there in private meetings.

One of the problems that we have observed with regards to TSA is just the pure nature of its work. It is very tedious, hard work, and people's expectations when they take these jobs are not always met.

Second, when you talk about the leadership, this is the leadership up and down the chain of command. At the individual airports themselves there was oftentimes a lack of leadership, and people's expectations of their leaders were not being met. But to actually come up with empirical information or a conclusion as to why there is a high turnover rate, at least when I was the IG, we had never completed a study in that area.

Senator AKAKA. Thank you. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka.

This has been a very productive morning. I want to thank the three witnesses. Each of you in different ways has given great service to our country, and if I may say so, I think you added another step in that direction by both your prepared testimony, which was very thoughtful and will be part of the permanent record, and by your testimony this morning. You have given the Committee a lot to think about. I think you will give the new Committee leadership in the next session a lot to think about. And, frankly, I think you will give both the current and new leadership of the Department an agenda for action to continue what has been a first decade of real progress, but obviously a lot of work to be done.

Senator Collins, do you want to add anything?

Senator COLLINS. I just want to add my thanks to those of the Chairman. I have enjoyed working with all three of our witnesses over the years, and it is terrific to have them back today to share their extraordinary experience and insights with our Committee. So thank you all.

Chairman LIEBERMAN. Thank you.

So the record of the hearing will remain open for 15 days for any additional statements or questions. Again, thank you very much.

The hearing is adjourned.

[Whereupon, at 12:17 p.m., the Committee was adjourned.]

APPENDIX

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph I. Lieberman
Homeland Security and Governmental Affairs Committee
""The Future of Homeland Security: Evolving and Emerging Threats"
Washington, DC
July 11, 2012

Good morning and welcome to our distinguished panel of witnesses to this first in a series of hearings where we will begin looking at the evolution and future of homeland security.

This coming November will mark the tenth anniversary of the signing into law of the Homeland Security Act legislation created in this Committee in the aftermath of al Qaeda's attack on 9-11. Given this coming milestone, it seems appropriate not only to reflect on the major homeland security developments of the last decade but also to look ahead to the next ten years, and examine whether we are adequately prepared to address them.

The preeminent threat to our homeland security today remains the threat of terrorism, but our enemies have grown and evolved since 9-11. Core Al Qaeda, based on the Afghanistan-Pakistan border has suffered significant losses but remains dangerous. Its affiliates in Yemen, Somalia, Iraq, and North Africa continue to grow, as do allied groups such as Lashkar-e Taiba and Tehrik-e Taliban in Pakistan.

Homegrown terrorists, inspired by violent Islamist extremism, like Maj. Nidal Hasan, remain a danger. Increasingly in the last year we've also seen stepped-up efforts from Iranian-linked groups to plan attacks and recruit terrorists. We also see increasing threats domestically and in Europe from both right-wing and left-wing extremist groups.

One key question for today is how the terrorist threat is likely to evolve in the next decade, in response to political developments such as the Arab Spring and technological developments - like the Internet and social media - that have altered the way terrorist organizations can recruit and radicalize. How prepared are our key counterterrorism organizations for major shifts in the threat?

The cyber threat is the second most significant threat to the United States that we face today, and as FBI Director Mueller has noted, could surpass terrorism as America's top national security threat in the coming years. Attacks from cyberspace by rival nations, terrorists, criminal gangs and individual hackers are already costing us billions of dollars in economic damage through theft of money as well as intellectual property. Beyond this dollar loss, there is the potential to use computers to sabotage critical infrastructure, like electric utilities and pipelines that could lead to loss of life and environmental and economic disasters.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

Cybersecurity has been a major focus of this Committee and Sen. Collins and I are working hard at getting our bipartisan cybersecurity legislation brought to the floor of the Senate during this work period and signed into law this year.

Other significant threats to our homeland security have gained increased attention in recent years. The violence in Mexico by drug trafficking organizations has reached the level where it is now a direct threat to our national security. Transnational organized criminal groups are becoming increasingly sophisticated and are engaged in a wide variety of activities, from human smuggling to Medicare fraud.

All of these national security threats – terrorism, cyber threats, drug violence, and organized crime– should not be looked at in isolation, but in terms of how they relate to each other. Increasingly we see cases where these different threats are interwoven. For example, last year Iranian agent Mansour Arbabsiar attempted to hire a hit man from the drug trafficking organization known as the Zetas in Mexico to carry out his plot to assassinate the Saudi Ambassador to the U.S. here in Washington.

But while our threats are becoming increasingly interrelated, we continue to address them in a fragmented way, with different agencies responsible for different threats. While the efforts of agencies are robust within each of these threat domains, too often there is limited information sharing and coordination across these different domains.

One key question for our witnesses today is whether and how the US government needs to evolve to address these increasing linkages among our adversaries.

Finally, we are also looking today not only at deliberate homeland security threats but also future trends related to threats from natural hazards or man-made accidents. The fact of climate change is becoming increasingly apparent, and we are seeing increasingly severe weather events as a result.

We also see increasing examples of natural disasters having cascading effects – most notably in Japan last year with the earthquake and tsunami leading to the Fukushima nuclear disaster. But also on a much smaller scale, in the DC metro area last week, we saw the 'derecho' storm system lead to wide-scale power outages that disrupted the water lines, gasoline supplies, and emergency communications in our nation's capital region. The fallout from extreme weather has caused more than two dozen deaths nationally and put countless more lives at risk.

I look forward to discussing all of these issues with our witnesses today, in order to get a better understanding of the evolving types of threats that DHS and its partners are likely to face in the coming decade. We need to focus on anticipating these threats and then use our understanding to make the prudent investments to address them.
Senator Collins.

-30-

Opening Statement of
Senator Susan M. Collins
Anticipating Evolving and Emerging Threats
Committee on Homeland Security and Governmental Affairs
July 11, 2012

The terrorist threats facing our country have evolved since the horrific attacks on 9/11. That awful day steeled our national resolve and drove us to rethink how our intelligence agencies were organized and how our instruments of national power ought to be used.

Since then, we have taken significant actions to better counter the terrorist threat, but the terrorists have constantly modified their tactics in an attempt to defeat the security measures we have put in place. The October 2010 air cargo plot involving explosives hidden in ink cartridges shipped from Yemen is just one example. The bomb-makers from Al Qaeda in the Arabian Peninsula apparently sought to avoid improvements in passenger and baggage screening by exploiting vulnerabilities in cargo security.

Let me emphasize that it is extremely troubling that terrorists have been aided in their efforts to circumvent our security by the all-too-frequent leaks regarding our counter-terrorism activities and capabilities. As we consider the challenges posed by emerging threats, we cannot tolerate giving our adversaries information they can turn against us.

When Chairman Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our goal was to create a coordinated effort among the Department of Homeland Security, the Director of National Intelligence, and the National Counterterrorism Center, as well as other federal partners and stakeholders.

One instrument used in these collaborative efforts has been the network of 77 state and local fusion centers that help manage the vital flow of information and intelligence across all levels of government. These centers are recipients of national intelligence products, but must also become robust aggregators and analyzers of information from their own areas that can be shared so that trends can be identified and the understanding of threats in our homeland can be strengthened.

An example of the effectiveness of fusion centers occurred on June 25th, 2011, when the Colorado State Patrol attempted to pull over a man driving erratically, who fled authorities and eventually crashed. As the police processed the driver and information about his pickup truck, they learned from the Colorado fusion center that he was linked to an attempted bombing of a bookstore. The driver is now in custody facing federal charges.

This type of grassroots teamwork is essential to combat a deceptive and often elusive enemy. As discussed in a recent report by the Homeland Security Policy Institute at George Washington University, however, fusion centers have yet to achieve their full potential.

Questions have been raised about their analytic capabilities and about whether they duplicate the work of the Joint Terrorism Task Forces.

The reforms enacted in response to the 9/11 attacks have helped to ensure that there have been no other large-scale attacks in the U. S. The absence of such attacks in the U. S. and our success in thwarting terrorist plots should not lull us into a false sense of security – for this is no time to rest, as gaps in our security net remain.

We continue to witness the growing threat of violent Islamist extremists within our borders. Sometimes these terrorists have been trained overseas; others have taken inspiration from charismatic terrorists via the Internet – plotting attacks as lone-wolves.

Last year, as members of this committee well know, two alleged Al Qaeda terrorists were arrested in Bowling Green, Kentucky. This highlighted a gap where elements of our security establishment had critical fingerprint information that was not shared with those granting these men access to our country.

Another growing and pervasive threat is that of cyber-attacks. Earlier this year, the FBI Director Robert Mueller warned that the cyber threat will soon equal or surpass the threat from terrorism. Just last month, several former national security officials wrote that the "cyber threat… is imminent, and that it represents one of the most serious challenges to our national security since the onset of the nuclear age sixty years ago." They further wrote that "protection of our critical infrastructure is essential in order to effectively protect our national and economic security from the growing cyber threat."

Chairman Lieberman and I have been working with our colleagues on legislation to address the cyber threat to our nation's most critical infrastructure, such as the power grid, nuclear facilities, water treatment plants, pipelines, and the transportation system. I can think of no other area where the threat is greater and we've done less.

There is also the growing threat from Transnational Organized Crime. Director of National Intelligence James Clapper has testified that transnational criminal organizations, particularly those from Latin America, are an "abiding threat to US economic and national security interests." Our intelligence community needs to focus on their evolution and potential to develop ties with terrorists and rouge states.

The 9/11 Commission devoted substantial attention to the challenge of "institutionalizing imagination." In an understatement, the Commission's report observed that, "[i]magination is not a gift usually associated with bureaucracies." Yet, imagination is precisely what is needed to address emerging threats. We must persistently ask: Where are the future threats? What technology could be used? Do we have the intelligence that we need? Are we prepared to thwart novel plans of attack? What will our enemy look like in two, five, or even ten years?

Surely we are safer than we were a decade ago, but we must be relentless in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden has proved, America's resolve and creativity are our most powerful weapons against those who seek to destroy our way of life.

STATEMENT FOR THE RECORD

BY THE HONORABLE MICHAEL V. HAYDEN
PRINCIPAL OF THE CHERTOFF GROUP
FORMER DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
AND NATIONAL SECURITY AGENCY

FOR THE UNITED STATES SENATE COMMITTEE
ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
JULY 11, 2012

I want to thank Chairman Lieberman, Senator Collins and members of the committee for inviting me to submit a Statement for the Record and for the opportunity to testify here today.

I am submitting this Statement in my personal capacity, but for the record, I am a principal at The Chertoff Group, a global security and risk management firm that provides strategic advisory services on a wide range of security matters, including the threat areas that will be discussed today. I am also a visiting professor at George Mason University's School of Public Policy.

Let me thank you especially for having me here today among such a talented group of co-panelists.

I think my fellow panelists will give the committee quite a lot to think about with regard to specific homeland security threats and our response.

So, if I might, I would like to take just a few minutes to provide a broader context for today's discussions.

General Brent Scowcroft wrote recently for the Atlantic Council (and I am paraphrasing here) that he had spent his professional career dealing with a universe that was dominated by nation states and was susceptible to what you and I these days would call "hard power."

No longer, he writes. Because of globalization, the international structure that was created by the Treaty of Westphalia more than five centuries ago is no longer dominant. General Scowcroft points out that most of the attributes of the age of industrialization made the state stronger and more relevant. Most of the effects of today's globalization make the state weaker and less relevant.

In addition to eroding the traditional role the of the nation state, globalization has introduced new actors on to the world stage and made immediate and direct threats that a few decades ago were distant and oblique.

But here we sit with institutions optimized and practiced for the earlier age: methodical, thorough, stable.

That really suggests our challenge. How do we adapt to these new dangers, be they terrorism, cyber dangers or transnational crime—all of them merely specific expressions of this new reality of an intensely interconnected world that empowers individuals and small groups beyond all previous experience?

Let me illustrate both the challenge and the difficulty of forming an appropriate response. Prior to 9-11 we all believed (wrongly) that we had little to fear personally from religious fanatics living a world away in camps in Afghanistan. How wrong we were.

Prior to that attack we saw no need for a Department of Homeland Security and more importantly we were comfortable protecting both our liberties and our safety by creating barriers to separate things that were foreign from those that were domestic, dividing things to do with intelligence from those that touched on law enforcement.

Those models had served us reasonably well as a country for more than two centuries (in a largely Westphalian world). But the old models failed us and we are still adapting on the fly.

And with a great deal of controversy. In my own experience there was the Terrorist Surveillance Program that aimed to close an obvious gap—detecting the communications of foreign terrorists operating from within the homeland. And you Senators later debated changes to the Foreign Intelligence Surveillance Act over the same objective and concerns, and even today you are debating its extension.

The controversy remains. We all agreed in the 9-11 Commission Report that we needed a domestic intelligence service and it would be best to house it in the FBI. But look at the reaction even today when the bureau tries to collect information without a criminal predicate, in that area we called "spaces between cases."

And heaven save us from the Associated Press if the New York City Police Department tries to do the same thing.

Over two Administrations we have had measurable success against those who attacked us on September 11th, but dangers clearly remain: AQ main could still reconstitute if we ease up pressure on it; AQ franchises continue to pose danger and one in particular, AQAP, is clearly intent on showing global reach; and finally, quite disturbingly, the home grown radicalized threat persists. Also persisting is what constitutes an appropriate, lawful and effective response from us.

We are seeing this debate replayed in the cyber domain where threats are all too obvious but where our response is clearly late to need. This committee knows more than most how many of our secrets (state and industrial) are being stolen by foreign governments; how much of our wealth is being pilfered by criminal gangs; and how much of our infrastructure is vulnerable to cyber enabled anarchists and malcontents.

But here our response (as I know the Chair and senior member realize) is even slower and more difficult than it has been in the fight against terror. There are those who fear burdensome regulation. Others fear a loss of civil liberties.

And yet all of us should fear the loss of privacy, ideas, jobs and wealth that is now occurring.

As we encountered ten years ago in the fight against terrorism, the old forms don't fit the new cyber dangers and—absent the catastrophic stimulus of a 9-11—we are moving all too slowly to adapt.

There are other expressions of dangers enhanced by a world made more intimate and I know we will touch on trans-national crime here today. I should add that cyber, terrorist and criminal threats today all merge in a witches' brew of danger.

Our response has to be equally synchronized, but the overall challenge remains. We have optimized our institutions across three branches of government for a different world and now we have to undertake the same tasks our political ancestors undertook more than two centuries ago. How do we best ensure our liberties and our security in our time?

This committee has been relentless in its efforts to answer that question in a way consistent with our enduring values and I congratulate you for that.

It is hearings like today's that help push the necessary debate forward.

Thank you again for the opportunity to contribute my personal views and I look forward to your detailed questions and discussion.

TESTIMONY

New Challenges to U.S. Counterterrorism Efforts

An Assessment of the Current Terrorist Threat

BRIAN MICHAEL JENKINS

CT-377

July 2012

Testimony presented before the Senate Homeland Security and Governmental Affairs Committee on July 11, 2012

Brian Michael Jenkins[1]
The RAND Corporation

New Challenges to U.S. Counterterrorism Efforts
An Assessment of the Current Terrorist Threat[2]

Before the Committee on Homeland Security and Governmental Affairs
United States Senate

July 11, 2012

The United States confronts a more diverse terrorist threat in 2012 than it has in the past. Al Qaeda, still our principal concern, has exploited the turmoil created by the Arab uprisings to make tactical advances and open new fronts. In addition, several incidents in the past year suggest a resurgence of Iranian-sponsored terrorism. Mexico faces what some analysts have called a "criminal insurgency" by the country's drug cartels, which could expose the United States to the kind of savagery seen in that country. The global economic crisis has spawned mass protests. These are legitimate expressions of popular discontent, but they attract violence-prone anarchists and may generate their own violent fringe groups. Anti-federal-government sentiments, a continuing current in American history, have become more virulent, fueled in part by economic dislocation that transcends the current economic crisis, deep national divisions, and the rancorous partisanship that characterizes contemporary political debate.

This is a catalogue of potential dangers, not a forecast of many dooms. Later in this testimony, I will review the post-9/11 terrorist attacks and plots in order to draw some broad conclusions about the targets, tactics, and scale of today's terrorist violence.

Al Qaeda Remains Our Principal Concern

Nearly 11 years after 9/11, there is still a remarkable lack of consensus among analysts about the current threat posed by al Qaeda and, in particular, about whether al Qaeda is near defeat or remains a significant threat.[1] In part, the differences reflect the fact that al Qaeda is many things at once—an ideology of violent jihad, a universe of like-minded fanatics, a global terrorist

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT377html.

enterprise—and it operates on a number of fronts in both the physical and virtual worlds. It therefore must be assessed in its different dimensions. Differences also arise over interpretation of available evidence. And there are differing views of al Qaeda's future trajectory and about the level of risk America can tolerate as a "postwar" norm.

We have made undeniable progress against al Qaeda. Its operational capabilities have been degraded. Its central leadership has been decimated. It has been forced to operate in a more vigilant, more hostile environment. Its ability to carry out another 9/11-scale (or greater) attack has been much reduced. Apart from the tragedy at Fort Hood, al Qaeda has not been able to launch or inspire a significant successful terrorist attack in the West since 2005.

Today's al Qaeda is more decentralized, more dependent on its regional affiliates and like-minded groups and on its ability to inspire and activate homegrown terrorists. Its historic core has been pounded. Its remaining operatives on the Afghan-Pakistan border must devote most of their attention to survival. Their fate depends on the fortunes of the Afghan Taliban. If the Taliban are able to expand their territorial control and political influence in Afghanistan, al Qaeda will find some measure of sanctuary, if not immunity from continued U.S. attacks.

U.S. forces in Afghanistan should be significantly reduced to a level that is indefinitely sustainable. This will entail risks for our counterterrorist efforts. Whether the Afghan national forces will be able to contain the Taliban as foreign forces withdraw remains uncertain. Thus far, the Taliban have shown no willingness to abandon their historic relationship with al Qaeda as part of a political settlement. It will be more difficult to continue the pursuit of al Qaeda in the area after U.S. withdrawal from Afghanistan.[2]

Al Qaeda Exploiting the Arab Spring

Al Qaeda poses a new array of threats in Africa and the Middle East. Surprised by the Arab Spring, al Qaeda then made the undeserved claim that its 9/11 attacks had, in fact, set in motion the events that led to the Arab uprisings. At the same time, al Qaeda positioned itself to take advantage of the political and economic disillusion that will inevitably follow. Meanwhile, it is exploiting tactical opportunities.

The chaos in Yemen has allowed al Qaeda in the Arabian Peninsula, along with its local jihadist allies, to strengthen its hold on portions of the country. This branch has become the principal source of attacks on the United States. Egypt's domestic political distractions have enabled local smuggling rings and radicalized Bedouin tribesmen to operate more freely in the Sinai. The latter

have formed Ansar al-Jihad, which, although not yet a formal branch of al Qaeda, has pledged its loyalty to al Qaeda leader Ayman al-Zawahiri. Al Qaeda veterans from Iraq appear to be supporting a terrorist bombing campaign in Syria. Although al Qaeda militants have little direct influence in Libya, they gained combat experience fighting the Qaddafi regime in that country and possibly acquired some of Qaddafi's arsenal. Local jihadists connected with al Qaeda have seized control in northern Mali, and al Qaeda is said to have links with Boko Haram extremists in northern Nigeria.

Al Qaeda finds fertile ground in failed or failing states where it can attach itself to local insurgencies. It may provide only modest material assistance and operational advice, but the diffusion of al Qaeda-affiliated and connected movements in the region demonstrates that its brand name still carries prestige.

Al Qaeda's presence in a particular part of the world does not always present an immediate terrorist threat to the United States. The local contests where al Qaeda can make a connection or purchase a foothold are likely to remain local. And while local insurgents may welcome al Qaeda assistance, this does not necessarily mean that they embrace al Qaeda's war on the "far enemy." The longer-term threat is that al Qaeda will be able to deepen relationships that ultimately provide it with new safe havens, operational bases, and experienced veterans for international terrorist operations, which remain al Qaeda's hallmark.

In this context, large-scale military intervention and ambitious American efforts to fix failing states are likely to be counterproductive. They are long, costly, and no matter how experienced and well-trained in counterinsurgency American forces are, their presence will be seen to confirm al Qaeda's allegations of infidel aggression, while necessary military operations inevitably will provoke local resentment. The United States must develop counterterrorist strategies that enable it to avoid major commitments of American forces.

Drone strikes have disrupted al Qaeda's command and communications, and must remain a component, not the entirety of U.S. strategy. Small contingents of Special Forces, not acting exclusively as commandos, but in their more traditional role, can work with local government and irregular forces to deny al Qaeda elements sanctuary. Any such mission must be sustainable for many years.

Al Qaeda's Failing Campaign to Market Its Brand of Jihad in the U.S.

Unable to directly attack the West, al Qaeda has embraced a do-it-yourself strategy, exhorting volunteers to do whatever they can wherever they are. But this online recruiting effort thus far has failed to inspire a domestic terrorist campaign. Between 9/11 and the end of 2011, there were 96 cases involving 192 U.S. citizens or residents who were charged with providing material support to jihadist groups, joining or attempting to join jihadist fronts abroad, or, more seriously, plotting to carry out terrorist attacks in the United States. (This excludes the activities of Hamas and Hezbollah, actions of individuals radicalized abroad who came here to carry out attacks, and cases that are not clearly jihadist.)[3]

It is a very low yield, suggesting that al Qaeda's ideology has very limited appeal in America's Muslim community. As a marketing campaign for terrorism, it is failing. There is no evidence of an organized jihadist underground. Decisions to join jihad appear to be highly personal, not community-supported. Embracing al Qaeda's violent jihad apparently has become a way to express individual discontents.

The year 2009 saw a sharp uptick in the overall number of cases, the number of terrorist plots, and the number of individuals arrested, but this is partly explained by the increased recruiting of Somali Americans following Ethiopia's invasion of Somalia, and by the culmination of investigations of activities going back to the middle of the decade. The number of individuals arrested declined in 2010 and again in 2011.

Of the 37 identified jihadist plots to carry out terrorist attacks in the United States, 34 were thwarted by the authorities. The majority of the plots involved a single individual. Most of the plots were immature and amateurish. Although most of them involved bombings, only two individuals attempted to build devices. Only two attacks resulted in fatalities; both of them were carried out by lone gunmen.

A Resurgence of Iranian-Sponsored Terrorism

Jihadists are not the only terrorist concern. Growing tensions with Iran could result in an escalation of Iranian-sponsored terrorist attacks on American targets abroad or in the United States, as recent events attest. In February 2012, Iranian operatives were linked to terrorist plots or attempts targeting Israeli diplomats in India, Georgia, and Thailand. In March, authorities in Azerbaijan arrested 22 Azerbaijani citizens who had been hired and trained by Iran to carry out

terrorist attacks on the American and Israeli embassies, as well as Western companies. This was third set of arrests of Iranian-trained agents in Azerbaijan since the beginning of the year. In July, Kenyan authorities reportedly uncovered another Iranian plot to attack Israeli, British, American, or Saudi targets—Iran's principal foes—in Mombasa.

Finally, in October 2011, U.S. authorities uncovered an Iranian plot to assassinate the ambassador of Saudi Arabia in Washington. Killing a Saudi diplomat on American soil in an attack that could also have killed American citizens would have enormous consequences. The United States must recalibrate Tehran's willingness to take risks.

Several factors may explain this apparent recklessness. Radical elements may have acquired greater influence among Iran's ruling clerics. Iran may feel obliged to retaliate for what it sees as Israeli and American efforts to slow its nuclear program, not only through sanctions but also through sabotage of its facilities and assassinations of its nuclear scientists. To the extent that Iran's leaders perceive these efforts as a campaign aimed not just at preventing the country from developing nuclear weapons but, rather, at bringing down the Islamic Republic, they may reckon that they have little to lose.

The future threat posed by Iranian-sponsored terrorism will be contingent upon Iran's calculations of risk. The current shadow war could escalate further if Iran thinks military attack by either Israel or the United States is inevitable and imminent or, obviously, if hostilities begin. Under such circumstances, Iran could launch attacks on U.S. military and civilian targets in the region, including oil facilities and shipping. It could also attempt to carry out a strategic strike (a 9/11-scale attack) or something greater on U.S. soil. And it could rely on its own operatives, try to activate Hezbollah's international networks, or conceivably assist other groups, including al Qaeda, to escalate their terrorist campaigns. Hezbollah has criminal networks in the United States, primarily engaged in fraud and smuggling, which remit a portion of their proceeds to the organization and possibly could be converted into terrorist cells.

Violence South of the Border

Mexico is hardly a failed state. It boasts of a tumultuous democracy and a vibrant economy closely linked to that of the United States. There is no threat of civil war. Its government is not about to fall. But this modern, sophisticated state cohabits the country with rich and powerful criminal cartels that wage war on one another and challenge any authority that gets in their way, creating in effect a "criminal insurgency."[4] For now, the cartels are interested in the profit that

comes with territorial dominance, but they are investing their profits in the legitimate economy and eventually will seek political power.

Mexico's violence is notable not merely for the scale of killing but for its deliberately savage quality. Kidnappings, mass killings, and mass graves are common. Victims are brutally tortured and often beheaded. Messages are sent pinned to corpses. The purpose is terror, but the violence exceeds what is required to eliminate rivals and intimidate authorities. A subculture of barbarity has emerged in parts of the country where violence is normalized, even celebrated. To crack the power of these criminal barons and restore government authority when police were unable to, Mexico's president sent in the army. The military has made progress against the cartels, but the violence worsened. In the eyes of the Mexican public, the high level of violence itself has become the issue, not the criminality that generates it.

The new president-elect has promised to address the violence by bringing the army back to its barracks and deploying a more effective police force. Building that force, however, will require significant resources and take time. In the interim, some fear that peace can be purchased only through local accommodations with at least some of the cartels, which would not displease those who blame Mexico's violence on the Yankees' insatiable appetite for illegal drugs. An accommodation strategy also raises opportunities for corruption, such as existed in the old days when high-ranking Mexican officials allegedly kept the peace by allocating smuggling routes while taking a share of the profits. Supporters of the new president say there is no longer any tolerance for that kind of behavior, and anyway, the cartels have become too powerful and too violent to be easily kept in check.

U.S. officials fear that the northern tier of Mexican states will remain a chaotic, violent, ungovernable badlands abutting our southern border, pushing vast quantities of drugs and thousands of refugees north. The cartels themselves will come north as they link with domestic Hispanic gangs to expand their criminal empires into U.S. territory. This will create competition among trafficking networks, which could lead to the kind of savagery seen in Mexico. It will also bring the cartels into direct confrontation with U.S. law enforcement, which they will try to suborn with vast sums of money. Failing that, they will likely not hesitate to employ the same violent tactics that they have used to intimidate police in Mexico. That transforms the threat in Mexico from a matter of law enforcement to a national security problem. A bigger, better wall is not the total solution.

Intelligence Remains a Crucial Component of U.S. Efforts

Much of the success in preventing major terrorist operations in the West for the past seven years is owed to the unprecedented worldwide cooperation among intelligence services and law enforcement organizations that has been achieved since 9/11. However, the continuation of this cooperation is not guaranteed and may begin to fray as the imminent danger of a major terrorist strike recedes and other issues compete for attention and resources.

The jihadist threat itself has become murkier as it blends with Islamist politics in countries affected by the Arab uprisings. Counterterrorism is no longer a priority for countries confronted with the daunting task of constructing new political institutions while meeting pressing demands for economic development and rapid job creation. In some Middle Eastern countries, cooperation requires working with governments that many see as repressive while in principle supporting those struggling to bring about greater democracy. In others, it requires cooperation with new governments that represent Islamist tendencies and have very different ideas about terrorism. The newly elected president of Egypt, for example, has made it his first order of business to bring about the release of Abdel Rahman, the so-called "Blind Sheik," imprisoned in the United States for his role in the 1993 World Trade Center bombing and subsequent terrorist plots.

To the extent that intelligence from abroad becomes harder to obtain, the burden on domestic intelligence collection increases. This is always a delicate undertaking in a democracy, especially one where citizens tend to view federal authority with suspicion. Although not optimized into a coherent national system, America's domestic intelligence efforts have achieved remarkable success in uncovering terrorist plots and preventing attacks.

These intelligence efforts are now under assault, driven in part by sincere concerns about the protection of civil liberties but also by personal, ideological, and political agendas in both Muslim and non-Muslim communities, and fueled by organizational rivalries. The timing exploits the greater sense of security felt by many. It is legitimate to review such efforts—no reviews thus far have found any illegal conduct, but dismantling the intelligence effort, which is the politically correct goal of some critics, would be dangerous..

The Return of Anarchism

The continuing global economic crisis has led to worldwide demonstrations and occupations protesting against capitalist greed, government bailouts, and reductions in social spending and other austerity measures to reduce government deficits. These are legitimate protests, not acts of

terrorism. However, they attract violence-prone anarchists who see them as opportunities to escalate confrontations with police and foment riots, which provide diversions and cover for direct attacks on symbols of the capitalist system, which the anarchists see as the source of society's ills.

Some carry on their campaigns beyond the venues of protest. In Europe since 2008, anarchists have carried out bombings, arson attacks, and acts of sabotage and have inflicted other damage in Greece, Italy, Germany, and France. Investigators in New York have linked anarchists to a series of small bombings in the city in 2005, 2007, and 2008.

Five anarchists were arrested in March 2012 for allegedly plotting to blow up a major bridge in Ohio. Initially, the conspirators had considered attacks on financial institutions in Cleveland to coincide with the Occupy Cleveland protest, but they later decided on attacking the bridge. In May 2012, three men were arrested in Chicago for planning arson attacks on police stations during the NATO Summit protests.

Anti-capitalist violence may not come solely from those identified as anarchists. Radicalized protesters, frustrated by their inability to bring about fundamental change may also take the field. In the 1960s, the mass protests, driven mainly by opposition to the Vietnam War but also incorporating other social issues, spawned on their extremist fringe tiny groups determined to carry on the struggle with bombing campaigns that persisted into the 1980s.

Potential Anti-Federal-Government Violence

The inclusion of anti-federal-government extremists in an assessment of the terrorist threat may seem controversial. Our focus here is not on a single specific group, but on the nebula of shared ideologies and beliefs from which terrorist conspiracies have emerged.[5]

Hostility toward the federal government is nothing new in America. Its currents can be traced back to the first days of the American republic. Over the years, it has involved issues of taxation, states rights, slavery, segregation, religious beliefs, and gun control. Anti-government extremists demonize the federal government, seeing it as a tyranny controlled by hostile elements determined to disarm and destroy any domestic resistance to its accumulation of power.

The extremists view themselves as "patriots," standing up against the government as American revolutionaries did in 1776, or in some cases, as heirs of the Confederate States in the Civil War.

The number of groups promoting such ideas has increased in recent years, although it is difficult to estimate the number of people who subscribe to such beliefs. Several factors may explain the growth.

One is the state of economy. Hard times increase hostility. But this time, the discontents may transcend eventual economic recovery. Technological advance and increased global competition, combined with failures in the education system, have caused a significant group of Americans without advanced education to face bleak economic futures. They confront the prospect of permanent unemployment or low-paying jobs at best. This economic decline of a significant portion of the population coincides with the immense accumulation of wealth by a few, creating a deep divide, with what many see as a corrupt government clearly on the side of big finance.

Demographic shifts play a role as well, especially as America's white population in several decades will become a minority. Immigration further fuels nativist instincts and hostility toward a federal government, which is seen as unwilling or unable to stem the tide. Many feel they have lost *their* country.

The cause of greatest anger, however, is the federal government's perceived tyranny, which is expressed in taxes, gun control, health-care mandates, pat-downs at airport security checkpoints, and other impositions. These blossom into paranoid ideas that the government has plans to disarm the population or round up dissident patriots and intern them in concentration camps secretly being built by the Department of Homeland Security. But some concerns have a basis in fact. Measures passed to enhance U.S. efforts against terrorism, such as increased electronic surveillance and confirmation of the government's authority to indefinitely detain U.S. citizens, cause deep apprehension, which is not confined to anti-government crazies. These measures are seen as tools that will eventually be used to suppress domestic dissent.

Growing political partisanship in the United States, along with the injudicious rhetoric it has generated, does not help. At worst, it delegitimizes political opponents and fuels the idea that politics is war. At best, it denigrates all political leadership.

Anti-government extremists have engaged in acts of violence, most dramatically in the 1995 bombing of the federal building in Oklahoma City, which killed 168 people—the worst incident of terrorism on U.S soil until 9/11. Authorities have uncovered a handful of more recent plots. For now, however, anti-government extremists are content to talk about justified armed resistance and the coming civil war. Nevertheless, the causes of hostility run deep and reflect long-term

trends. The potential for violence is there, and if realized, would represent a far greater threat to the republic than al Qaeda or any other foreign terrorist group.

Terrorist Targeting

It is an axiom of terrorism that terrorists can attack anything, anywhere, anytime, while governments cannot protect everything, everywhere, all the time. Finite resources require decisions about allocation. A threat assessment, therefore, must identify not only the groups that may carry out terrorist attacks but what they may attack and how.

Jihadist training manuals urge attacks on targets of iconic or "emotional" value, such as New York's World Trade Center, the Pentagon, and Mumbai's Taj Mahal Hotel; attacks that jihadists think will cause economic disruption, such as attacks on stock exchanges or banks; and attacks aimed at concentrations of people that will bring high body counts, such as a tourist-filled Times Square, crowded train stations, Portland's Christmas tree lighting ceremony. Body count often seems to be the most important criterion.

A review of terrorist attacks and foiled terrorist plots since 9/11 shows that jihadist terrorists have contemplated a wide range of mostly unprotected targets, including government and commercial buildings; churches and synagogues; restaurants and nightclubs; shopping malls and markets; hotels and tourist sites; power stations, tank farms, gas stations, and pipelines; bridges and tunnels; subways, trains, buses, and ferries; public officials and those deemed by fanatics to have offended Islam; police and military personnel, especially those readily accessible, such as recruiting officers; and public gatherings.

Among these, government buildings predominate along with public surface transportation, followed by hotels and tourist sites, religious institutions, commercial buildings, and aviation.

Terrorists remain obsessed with attacking commercial aviation. With improved passenger screening, locked and armored cockpit doors, armed air marshals, armed pilots, and, most importantly, airline passengers no longer willing to remain passive bystanders but more likely to assault would-be hijackers, terrorist hijackings may no longer be viable, but sabotage of aircraft with concealed explosives remains a favored terrorist tactic.

Since 9/11, terrorists have made eight attempts to smuggle bombs on board commercial aircraft. Four of the attempts involved planes flying to the United States (the shoe bomber in 2001, the underwear bomber in 2009, and the two bombs aboard cargo aircraft in 2010). There also were

several thwarted plots, including the 2006 Heathrow plot, the recovery by an undercover agent of an improved underwear bomb in 2012, and the recent discovery of another plot in the United Kingdom to sabotage a U.S. airliner. Aviation security remains a matter of national security.[6]

While terrorists apparently consider airliners to be their gold-medal target, public surface transportation offers easier access and concentrations of people in confined environments, enhancing the effects of explosives and unconventional weapons. Surface transportation has become a terrorist killing field. Between 9/11 and the end of 2011, there were 75 terrorist attacks on airplanes and airports worldwide, resulting in 157 deaths. During the same period, there were 1,804 terrorist attacks on trains and buses, resulting in more than 3,900 fatalities.[7]

Most of the attacks on surface transportation resulted in only handfuls of deaths and therefore attracted little attention, but 11 of the attacks caused 50 or more fatalities, and three resulted in nearly 200 deaths each—in all, the equivalent of seven airline crashes. The solution is not the implementation of an aviation security model on surface transportation, which would be too expensive and would be unworkable because of the huge volumes of passengers. Other security approaches must be developed, including greater participation by staff and riders themselves. Some level of risk is inevitable.

Anarchists in the 19th century assassinated political leaders but also did not blink at blowing up bourgeoisie-filled cafes. Their ideological descendants have shied away from indiscriminate attacks and instead have focused on symbols of capitalism and political oppression. Corporate offices predominate, but a recent anarchist plot involved blowing up a bridge in Ohio, demonstrating that terrorist targeting can be idiosyncratic and capricious.

Anti-federal-government extremists attack government targets that they see as symbols of tyranny. The 1995 bombing of the federal building in Oklahoma City is an example. But they also have contemplated indiscriminate attacks on the civilian population, for example, blowing up large propane tanks or dispersing ricin in populated areas.

Terrorist Tactics

Bombings have remained the most common mode of attack for all terrorist groups since the emergence of contemporary terrorism in the late 1960s. Large vehicle-borne explosive devices predominated through the first half of the post-9/11 decade as al Qaeda sought to carry out continued spectaculars, then declined. Improved intelligence, government crackdowns, and increased vigilance over explosives and chemical ingredients made it more difficult to amass the

large amount of explosives required, at least outside of conflict zones. Vehicle-borne bombs continue to be the norm in Iraq, Afghanistan, and Pakistan. In the West, the vehicle-borne devices have been seen mostly in foiled plots and FBI stings.

Jihadists began exploring devices that use readily available flammables, for example, in the 2007 attempts in London and the 2009 attempt at Times Square, but they encountered technical difficulties in creating a blast. They have also employed smaller devices that could be easily delivered and concealed or carried on a person and detonated in suicide bombings. These appear in the majority of the post-9/11 plots uncovered in the United States, although none succeeded. American jihadists have shown little inclination to carry out suicide attacks, although American Somalis blew themselves up in Somalia.

Assaults carried out by heavily armed gunmen account for comparatively few attacks. Ten trained attackers armed with automatic weapons, ample ammunition, grenades, and small explosive devices terrorized the city of Mumbai in 2008, ultimately killing 162 people.[8] Since 9/11, the only two jihadist attacks causing fatalities in the United States were carried out by lone gunmen.

Given the availability of guns in the United States, it is surprising that jihadists have not used this tactic more often. Homicidal rages by mentally disturbed or temporarily crazed gunmen regularly illustrate the possibilities, but American jihadists have shown little inclination to go down shooting. Perhaps this is due to the fact that they are unwilling to participate in any mission that ends in certain death, or they may be put off by the association of this type of attack with crazy behavior as opposed to martyrdom.

Examination of unrealized or foiled terrorist plots offers glimpses into terrorist ambitions. Those plots are more ambitious than the attacks that have succeeded. For example, since 9/11, authorities have reported seven plots to crash hijacked airliners into targets. None of these got much beyond the thinking stage.[9]

Eight jihadist plots early in the past decade involved chemical weapons or ricin, reflecting the newly acquired skills of a handful of terrorists who trained with al Qaeda. None of these plots succeeded, and chemical and biological weapons have largely disappeared from jihadist plotting, although anti-government extremists still contemplate their use.

Al Qaeda's central leadership clearly had nuclear ambitions and made an effort to acquire fissile material and technical expertise. However, there is no evidence that they acquired or even came close to acquiring nuclear weapons, and at some point in the last decade, the organization's

nuclear weapons project turned from an acquisition effort to a propaganda program calculated to excite its followers and frighten its foes.[10]

Estimating the Scale of Terrorist Violence

The last decades of the 20th century saw a steady escalation in terrorist violence, from incidents involving scores of fatalities to incidents involving hundreds of fatalities, culminating in the thousands killed in the 9/11 attacks. It was natural in the circumstances to view the 9/11 attacks not as an anomaly but as an indicator of worse to come. Now, more than ten years later, that view is being revised.

The 9/11 attacks, however, left deep psychological scars and continue to have an insidious effect on analysis of the terrorist threat. The United States has adopted the debilitating habit of catastrophizing every terrorist threat. Terrorism analysts fear failure of imagination more than they fear causing unnecessary alarm. Competition for limited resources, especially in the current fiscal environment, encourages exaggeration of favored threats. And it is difficult to mobilize popular and political support for action without a worst-case scenario. Without asserting any predictive value, it is nonetheless useful to look at what actually has occurred.

Before 9/11, the bloodiest terrorist incidents involved deaths in the low hundreds. These included incidents of airline sabotage or very large truck bombs. Since 9/11, the worst terrorist attacks, outside of war zones in Iraq and Afghanistan, have ascended to almost the same level. Terrorists achieved these casualty levels with large vehicle bombs or coordinated multiple bombings. Outside of Iraq and Afghanistan, there were fewer than 20 such attacks. Foiled terrorist plots, had they succeeded, also would have caused casualties on this scale.

Attacks with smaller improvised explosive devices involve both single and multiple bombings. Multiple bombings can be deadlier than attacks with single large, vehicle-borne devices.

Since 9/11, terrorists have attempted on a number of occasions to bring down airliners with bombs smuggled on board. They succeeded in bringing down two planes in Russia, killing 88 persons. Had the shoe bomber succeeded in bringing down the plane in 2001, 197 people would have been killed; 290 persons were on board the flight targeted by the underwear bomber in 2009. The 2006 Heathrow plot envisioned bringing down several wide-bodied jets flying across the Atlantic, which could easily have pushed fatalities past a thousand.

Armed assaults appear to be the deadliest tactic, primarily reflecting the 2008 attack on Mumbai. The median number of fatalities in such attacks, however, is seven.

On the basis of these admittedly rough calculations, keeping terrorists off of airplanes, preventing them from amassing large quantities of explosives for vehicle-borne bombs, or assembling conspiracies large enough to field multiple bombers or gangs of shooters will deprive them of the means they have used to kill hundreds.

That leaves smaller-scale attacks—tiny bombing conspiracies or individual shooters—with potential fatalities in the low tens. These are difficult to intercept, although thus far, the authorities have achieved a near perfect record. Whether this level of risk is tolerable is a question of public reaction.

Common Will and Common Purpose

Terror is just as much an enemy as the terrorists who try to create it. Our reactions to terrorism are part of any assessment. America has come through the dark shadow of 9/11, but as a nation, are we stronger?

Individual acts of courage inspire us, but Americans remain anxious rather than confident in the country's ability to survive the threats we face. Fear-mongers and doomsayers still find a receptive audience.

Instead of our traditional self-reliance, Americans look too much to government to protect them, in part the reflection of rhetoric that, rather than involving us in a national effort, tells us that as individuals we can do nothing beyond remaining vigilant.

Americans have come to hold unrealistic expectations about security, believing that risk can be abolished. We are too ready to seek someone to blame when security fails.

Instead of the stoicism needed for a long fight, Americans remain vulnerable to overreaction. A terrorist attack of even modest scale could provoke paroxysms of panic.

Whatever one thinks about the wisdom, or the folly, of the wars in Iraq and Afghanistan, the sacrifices of war have been borne unequally. Our sense of community has eroded.

Terrorists did not create America's anxieties. Terrorism acted as their condenser. Nor will America's homeland be secured in the mountain passes of Afghanistan, the Arabian Peninsula, or the sands of the Sahara. Our commonwealth, our common defense, will come only from the recovery our own sense of common will and common purpose.

---

[1] Brian Michael Jenkins, "Is the War on Terror Over? Not Yet," *National Journal* National Security Experts Blog, April 30, 2012.
[2] Brian Michael Jenkins, *Al Qaeda in Its Third Decade: Irreversible Decline or Imminent Victory?* Santa Monica, CA: The RAND Corporation, 2012; see also Brian Michael Jenkins and John Paul Godges (eds.), *The Long Shadow of 9/11: America's Response to Terrorism,* Santa Monica, CA: The RAND Corporation, 2011, and; Seth G. Jones, *Hunting in the Shadows: The Pursuit of al Qa'ida since 9/11,* New York: W. W. Norton & Company, 2012.
[3] Brian Michael Jenkins, *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11,* Santa Monica, CA: The RAND Corporation, 2011; see also Emma Disley, *Individual Disengagement from al Qaeda- Influenced Groups,* Santa Monica, CA: The RAND Corporation, 2011.
[4] John P. Sullivan, "From Drug Wars to Criminal Insurgency: Mexican Cartels, Criminal Enclaves and Criminal Insurgency in Mexico and Central America. Implications for Global Security" Paris: *Fondation Maison des sciences de l'homme.* No. 9, April 2012. See also: Brian Michael Jenkins "Could Mexico Fail?" *Homeland Security Today,* Vol. 6, No. 2, February 2009.
[5] Jerome P. Bjedopera, *The Domestic Terrorist Threat: Background and Issues for Congress,* Washington, D.C.: Congressional Research Service, 2012.
[6] Brian Michael Jenkins, *Aviation Security—After Four Decades of Reactive Policies, Its Time for Something New,* Santa Monica: The RAND Corporation, forthcoming; see also *Brian A. Jackson, et.al., Efficient Aviation Security: Strengthening the Analytic Foundation for Making Air Transportation Security Decisions,* Santa Monica, CA: The RAND Corporation, forthcoming.
[7] These statistics are taken from the Mineta Transportation Institute's Database of Attacks on Surface Transportation. See also: Brian Michael Jenkins and Joseph Trella, *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface Transportation,* San Jose, CA: Mineta Transportation Institute, 2012.
[8] Angel Rabasa, et.al. *The Lessons of Mumbai,* Santa Monica, CA: The RAND Corporation, 2009.
[9] Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves,* Santa Monica, CA: The RAND Corporation, 2006.
[10] Brian Michael Jenkins, *Will Terrorists Go Nuclear?* Amherst, New York: Prometheus Books, 2008.

"The Future of Homeland Security:

Evolving and Emerging Threats"

U.S. Senate Committee on

Homeland Security & Governmental Affairs

July 11, 2012

Statement of Frank J. Cilluffo

Director, Homeland Security Policy Institute

The George Washington University

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to testify before you today. This first in a series of hearings looking both back at what has been accomplished and ahead to what remains to be done in the area of homeland security is a prudent and thoughtful approach. While a host of constructive and valuable changes to policy and practice have been formulated and implemented in the decade plus since 9/11, there remain important gaps and shortfalls in our homeland and national security posture and readiness. Though we do not often laud those individuals, such as yourselves, who have remained steadfast and dedicated to the cause of improving the safety and security of Americans day in, day out, for years—even when the public mind and public opinion may have made the task more challenging than it already was—it bears remembering that we have made significant strides and in a relatively short period of time. Having said that, some significant shortcomings still exist, and some of these are more urgent than others to remedy or at least redress in part.

My remarks today will focus on two major areas: counterterrorism and cybersecurity. My approach, which I hope will be helpful, is to identify weaknesses and vulnerabilities in U.S. strategy and operations on both counts—with an eye to offering recommendations on how best to move forward, particularly in an economic climate in which resources are limited. Indeed, to the extent that we can derive greater bang for our buck, it is our shared responsibility to do so. What I would urge against however, is a more broadbrush approach (from a financial perspective) which runs the risk of privileging convenience over thoughtful strategic action, and may thereby do damage to our national/homeland security posture, even if inadvertently. Blunt cuts are simply not the answer. Instead we should prune and trim carefully, by prioritizing according to risk, by allowing good programs to live, and by taking off life support those programs that should rightfully expire.

Counterterrorism

As many counterterrorism officials have observed recently, al Qaeda's Senior Leadership is back on their heels. Key leaders have met their demise including, of course, Usama Bin Laden and Anwar al-Awlaki. Nevertheless, the ideology that Bin Laden and others such as the culturally fluent American-born extremist and self-styled cleric al-Awlaki have propounded lives on. This ideology is the lifeblood that continues to sustain the vitality and growth of the global jihadist movement. Make no mistake: while the core of al Qaeda may be seriously and significantly diminished, thanks largely to targeted U.S. military action overseas, the threat now comes in various sizes, shapes and forms. There are still many and varied al Qaeda affiliates that continue to thrive, most notably in Yemen and the Sahel, and in Somalia. Indeed, there is an arc of Islamist extremism that stretches across Africa from east to west, through the Sahel and the Maghreb, incorporating Boko Haram in Nigeria and Ansar Dine in Mali. At the same time, a veritable witch's brew of jihadists exists in Pakistan, including for example, the Haqqani network, Lashkar-e-Taiba (LeT), Tehrik-i-Taliban Pakistan (often dubbed the "Pakistani Taliban"), Harkat-ul-Jihad al-Islami (HuJI), Jaish-e-Mohammed, and the Islamic Movement of Uzbekistan. We have seen in the past and continue to see substantial evidence of cooperation and collaboration between these latter groups and al Qaeda. Though some of these groups may be more regionally or locally focused, they increasingly ascribee and subscribe to al Qaeda's goals and the broader global jihad, with U.S. and western targets increasingly in their crosshairs..[1] Nor can we take our eye off the ball of state-sponsored terrorism, such as that perpetrated by the Government of Iran and proxies such as Hezbollah.

[1] Frank Cilluffo "Open Relationship: The United States is doing something right in the war on terror" *Foreign Policy* (February 15, 2012). http://www.foreignpolicy.com/articles/2012/02/15/open_relationship. See also Sudarsan Raghavan "In Niger refugee camp, anger deepens against Mali's al-Qaeda-linked Islamists" *Washington Post* (July 7, 2012). http://www.washingtonpost.com/world/africa/in-niger-refugee-camp-anger-deepens-against-malis-al-qaeda-linked-islamists/2012/07/07/gJQAS25SUW_story.html

Unfortunately, our efforts to counter and defeat the jihadist ideology have been lacking, with the result that the terrorist narrative lives on and continues to attract and inspire those who wish us harm—despite and in some cases even empowered by—--the so-called Arab Spring. This is the biggest element missing from our statecraft on counterterrorism. This sustaining pool of recruits is, as Defense Secretary Panetta recently observed, the fundamental challenge: "the real issue that will determine the end of al-Qaida is when they find it difficult to recruit any new people...".[2] Arguably the most difficult challenge is the so-called "lone wolf" who self-radicalizes and prepares to commit violence without directly reaching out to al Qaeda or others for support and guidance. The term lone wolf is a bit of a misnomer, however, since individuals in this category have at least been inspired, goaded and in some cases facilitated by external forces—which in turn blurs the line between the foreign and domestic. In such cases, the mission of prevention is all the harder because there may be little for law enforcement or counterterrorism professionals to pick up on ahead of time, when we are still left of boom. The mission remains critical, though, as evidenced by the discovery of 58 "homegrown" jihadi terrorism plots since September 11, 2001.[3] Keeping eyes and ears open, at home and abroad and in partnership with our allies, is perhaps the best safeguard (and I will offer key recommendations on the intelligence front, below).

Notwithstanding the importance that non-state and individual actors have taken on, in an era when their actions can have profound impact and consequences, it bears reinforcing that traditional State and State-sponsored threats have not gone away. To the contrary, the latter are in some instances resurgent and reinvigorated. Consider for example Iran. The Director of National Intelligence recently stated that Iran is "now more willing to conduct an attack in the United States"[4] — a concern that has also been voiced by LAPD's Deputy Chief, Michael Downing, and by NYPD's former Director of Intelligence Analysis, Mitchell Silber.[5] To wit: the recently thwarted Iranian plot to assassinate Saudi Arabia's ambassador to the United States. Note also that up until 9/11, it was in fact Iran's chief proxy, Hezbollah, which held the mantle of deadliest terrorist organization, having killed more Americans up to that point than any other terrorist group. The October 23, 1983 bombing of the U.S. Marine Barracks in Beirut, Lebanon, cost the lives of 241 Soldiers, Marines and Sailors.

In addition, law enforcement officials have observed a striking convergence of crime and terror.[6] Hezbollah's nexus with criminal activity is greater than that of any other terrorist group. Within the United States, there were 16 arrests of Hezbollah activists in 2010 based on Joint Terrorism Task Force investigations in Philadelphia, New York, and Detroit; and the organization has attempted to obtain equipment in the U.S., including Stinger missiles, M-4 rifles, and night vision equipment. These links, including with gangs and cartels, generate new possibilities for outsourcing, and new networks that can facilitate terrorist travel, logistics, recruitment, and operations. Authorities have noted significant terrorist interest in tactics, techniques, and procedures used to smuggle people and drugs into the United States from Mexico. According to Texas State Homeland Security Director, Steve McCraw, Hezbollah operatives were captured trying to cross the border in September 2007.

---

[2] "Al Qaeda Senior Leadership Nearly Eradicated: Panetta" *Global Security Newswire* (June 22, 2012). http://www.nti.org/gsn/article/al-qaida-senior-leadership-nearly-eradicated-panetta-says/?utm_source=BNT+June+25%2C+2012--AoH&utm_campaign=BNT+06252012&utm_medium=email

[3] Jerome P. Bjelopera "American Jihadist Terrorism: Combating a Complex Threat" *CRS Report for Congress* (November 15, 2011). http://www.fas.org/sgp/crs/terror/R41416.pdf (but note that numbers have increased since the Report was published)

[4] Testimony of James R. Clapper before the Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community" (January 31, 2012). http://www.dni.gov/testimonies/20120131_testimony_ata.pdf

[5] "Tensions with Iran raise US safety concerns, but intelligence official says attack unlikely" *Associated Press* (February 17, 2012). http://www.foxnews.com/politics/2012/02/17/tensions-with-iran-raise-us-concern-possible-terror-attack/

[6] See for example "The Hybrid Threat: Crime, Terrorism and Insurgency in Mexico" *Joint Study of HSPI and the U.S. Army War College Center for Strategic Leadership* (December 2011). http://www.gwumc.edu/hspi/events/resources/Hybrid%20Threat%20Monograph%20(Internet%20version).pdf

Law enforcement officials also confirm that Shia and Sunni forces are cooperating to an extent. For instance, Shia members of Lebanese Hezbollah and Sunni (Saudi/Iraqi) militant forces are drawing on each other's skills. That said, competition persists even within Shia circles, including between Lebanese Hezbollah and Iran's Quds Force. It is also important to note that Iran itself is not a monolith when it comes to its terrorist (or cyber) activities. Indeed, Iran's Islamic Revolutionary Guard Corps (IRGC) operates as a semi-independent entity—and it is unclear just how much they coordinate with Iranian intelligence (the Ministry of Intelligence and Security, or MOIS). Notably, the IRGC has a substantial economic enterprise internal and external to Iran, including telecommunications. Given its close connections with Hezbollah and active training of terrorists, that makes Iran a key threat—and despite the imposition of sanctions on Iran, it is quite clear that the IRGC is not running out of money.[7] Taken as a whole, the various developments above suggest that our longstanding frames of reference and the "redlines" they incorporated have shifted. Correspondingly, we must re-examine our long-held assumptions, challenging them in light of current evidence, and recalibrate our stance and response mechanisms as needed.[8]

These developments draw warranted attention to the risk posed by hybrid threats—threats in which an adversary acquires from a third-party the necessary access, resources, or know-how, needed to attack or threaten a target—and how such might be employed strategically against the United States.

As is the case with the Federally Administered Tribal Areas (FATA) in Pakistan and Afghanistan, ungoverned and under-governed spaces, such as Yemen and the Sahel as well as Somalia, pose a different but still potent challenge. There, failed, failing or weak states, offer a propitious climate for jihadists to recruit, regroup, train, plan, plot, and execute attacks. In recent weeks, General Carter Ham, head of U.S. Africa Command (AFRICOM), warned that al Qaeda in the Islamic Maghreb (AQIM—operating in southern Algeria, northern Mali, and eastern Mauritania, and spreading elsewhere in the Sahel), al-Shabaab in Somalia, and Boko Haram in Nigeria "are seeking to coordinate and synchronize their efforts." He characterized each of these groups as "by itself, a dangerous and worrisome threat," but was particularly concerned by the emerging trend of them sharing "funds, training and explosive material."[9] Granted, some of these groups' top goals may be inward-focused, targeting the specific states in which these groups are primarily rooted. Their activities, however, breathe life into the larger jihadist movement and give it continued currency at a time when the Senior Leadership core has been seriously weakened.

So what can and should we do about all of these concerning realities? For starters, at the level of principle, we need to be as flexible and adaptive as our adversaries, who are nothing if not creative and ever-thinking. A static posture is an ineffective one. After all, each time we raise the security bar (often at great cost to the U.S. Treasury) our adversaries devote themselves determinedly to crafting a reasonably inexpensive and clever way around the latest security measure(s). Their ingenuity and inventions are often vivid, and include body and "booty" bombs. Now is not the time to ease off the gas pedal. Rather we should and must keep up the pressure and exploit this unique window of counterterrorism opportunity by maintaining, if not accelerating, the operational tempo. The threat would look and be markedly different otherwise.

---

[7] Julian Borger and Robert Tait "The financial power of the Revolutionary Guards" *The Guardian* (February 15, 2010). http://www.guardian.co.uk/world/2010/feb/15/financial-power-revolutionary-guard

[8] Testimony of Frank J. Cilluffo before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence; and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, "The Iranian Cyber Threat to the United States" (April 26, 2012). http://www.gwumc.edu/hspi/policy/testimony4.26.12_cilluffo.pdf

[9] David Lerman "African Terrorist Groups Starting to Cooperate, U.S. Says" *Bloomberg* (June 25, 2012). http://www.bloomberg.com/news/2012-06-25/african-terrorist-groups-starting-to-cooperate-u-s-says.html

Overall, Yemen-based al Qaeda in the Arabian Peninsula (AQAP) remains the most adaptive and lethal terrorist threat to the United States. Despite the past year's drone and Special Operations Forces' (SOF) achievements, al-Asiri, AQAP's innovative bomb-maker remains alive and continues to craft increasingly sophisticated attacks against Western airliners. Yet drones and SOF remain critical counterterrorism tools for denying AQAP safe haven in Yemen. Although an imperfect tool, drone strikes suppress terrorists, deny them safe havens, and limit jihadists' ability to organize, plan, and carry out attacks. These strikes help shield us from harm and serve our national interests. Along with SOF, the targeted use of drones should constitute key components of U.S. counterterrorism efforts for many years to come.

Having said that (and as former CIA officer and former State Department Coordinator for Counterterrorism, Ambassador Hank Crumpton, pointed out when featured in a recent HSPI roundtable), drones are important but cannot be a substitute for human intelligence (HUMINT). Indeed, intelligence remains our greatest need in Yemen. Improved intelligence will have an added benefit, too, by helping continue to improve the accuracy of drone strikes while minimizing collateral damage to civilians.[10]

From a counterterrorism standpoint, it is crucial to focus on and seek to enhance all-source intelligence efforts. This is the key to refining our understanding of the threat in its various incarnations, and to facilitating the development and implementation of domestic tripwires designed to thwart our adversaries and keep us "left of boom."[11] Disruption should be our goal. Planning and preparation to achieve this end includes information gathering and sharing—keeping eyes and ears open at home and abroad to pick up indications and warnings (I&W) of attack, and reaching out to and partnering with State and local authorities, especially law enforcement.

Searching for I&W will require fresh thinking that identifies and pursues links and patterns not previously established. The above-described nexus between terrorist and criminal networks offers new possibilities to exploit for collection and analysis. To take full advantage, we will have to hit the beat hard, with local police tapping informants and known criminals for leads. State and local authorities can and should complement what the federal government does not have the capacity or resources to collect (or is simply not best suited to do), and thereby help determine the scope and contours of threat domains in the United States. Further leveraging our decentralized law enforcement infrastructure could also serve to better power our Fusion Centers. The post-9/11 shift of U.S. law enforcement resources away from "drugs and thugs" toward counterterrorism is, ironically, in need of some recalibration in order to serve counterterrorism aims.

To obtain a truly "rich picture" of the threat in this country, we must focus on the field—not the Beltway. As history shows, the intelligence community has come to just such a field bias. For the counterterrorism community to do otherwise is to risk stifling and stymieing the good work being done where the rubber meets the road. Fusion Centers, for instance, should be given ample opportunity to flourish. The equivalent of Commanders' Intent, which gives those in the field the leeway to do what they need to do and which incorporates an honest to goodness "hotwash" after the fact to determine what went wrong and how to fix that, is needed in present civilian context for counterterrorism and intelligence purposes. Simple yet powerful steps remain to be taken. This was revealed starkly in multiple rounds of survey work (first with the major metropolitan intelligence

[10] Clinton Watts and Frank J. Cilluffo "Drones in Yemen: Is the U.S. on Target?" *HSPI Issue Brief* (June 21, 2012). http://www.gwumc.edu/hspi/policy/drones.pdf

[11] Frank J. Cilluffo, Sharon Cardash, and Michael Downing "Is America's View of Iran and Hezbollah Dangerously Out of Date?" *FoxNews.com* (March 20, 2012). http://www.foxnews.com/opinion/2012/03/20/is-americas-view-iran-and-hezbollah-dangerously-out-date/

chiefs and later with the fusion centers) that HSPI recently completed in an attempt to bring a little science to the art of intelligence. For example, too few Fusion Centers currently do threat assessments. This is unacceptable, especially in a climate of limited resources in which allocation decisions (regarding human, capital, and financial resources) should be priority-ordered, meaning that scarce resources should be directed to those counter-threat measures, gaps and shortfalls that constitute areas of greatest need. And Fusion Center-specific threat assessments are just a start. Regional threat assessments are also needed. Our adversaries do not respect local, State, or even national boundaries hence our response posture must be similarly nimble and cohesive. Yet, according to HSPI survey research published last month, only 29% of Fusion Center respondents reported that their Center conducted a regional threat assessment on at least a yearly basis. Almost half reported that their Centers simply did not conduct regional threat assessments.

Those working in the Fusion Centers have yet to be invested with the analytical skill-craft and training necessary for them to accomplish their mission. Current incentive structures place too much emphasis on information processing and not enough on analytical outcome. Greater resources should be allocated to the professional development of those working in the Centers. Within them lies untapped collection and analysis potential. Realizing and unleashing that potential will further bolster State and local law enforcement efforts, and help develop anticipatory intelligence to prevent terrorist attacks and the proliferation of criminal enterprise operations.[12]

Intelligence to support operations is certainly crucial but we must not lose sight of the long game either. To that end and from a strategic perspective, it would most helpful for the Secretary of Homeland Security to establish an Office of Net Assessment (ONA) within the Department of Homeland Security (DHS) to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats. The ONA would fill the much-needed role of producing long-term assessments and strategy, acting as a brain trust of creativity and imagination, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the U.S. requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable—in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends.

In order to accomplish this tall order, the duties of ONA would include studying existing threats in order to project their evolution into the future; studying trends in the weapons, technologies, modalities, and targets utilized by our adversaries (i.e., the events that can transform the security landscape); reviewing existing U.S. capabilities in order to identify gaps between current capabilities and the requirements of tomorrow's threats; conducting war games and red team scenarios to introduce innovative thinking on possible future threats; assessing how terrorist groups/cells could operate around, and/or marginalize the effectiveness of, policies and protective measures.

Notably, this proposal is not new. To the contrary, it was in fact contained in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served

---

[12] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires "Counterterrorism Intelligence: Fusion Center Perspectives" *HSPI Counterterrorism Intelligence Survey Research (CTISR)* (June 2012). http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf. See also Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing "Counterterrorism Intelligence: Law Enforcement Perspectives" *CTISR* (September 2011). http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf

as Vice Chairman together with Chairman Lee Hamilton.[13] Now is the time—indeed it is well past time—to take this recommendation off the page and enact it. Our adversaries are patient and they are long-term thinkers whose horizons extend well beyond weeks and months. To help counter them effectively, the ONA should be an independent office that reports directly to the Secretary of Homeland Security.[14]

Before turning from counterterrorism to cybersecurity, I would add some closing thoughts on combating violent Islamist extremism (CVIE). The fact is that addressing specific outbreaks of violent Islamist extremism will not prevent its virulent spread unless the underlying extremist ideology is exposed, unpacked, dissected, and combated. Government agencies currently involved in various aspects of the CVIE mission do not note systemic failures so much as the complete lack of a system at all. Absent clear interagency directives instructing how to distribute resources and coordinate aspects of the mission, individual and broader agency efforts are improvised. As a result, an inconsistent and haphazard approach to dealing with the force underlying today's terrorist threat is all but guaranteed.[15]

Counter-radicalization is an essential complement to counterterrorism. Elements of a cohesive national strategy could incorporate a range of approaches that have proven effective in other contexts. The power of negative imagery, as in a political campaign, could be harnessed to hurt our adversaries and further chip away at their appeal and credibility in the eyes of their peers, followers, and sympathizers. A sustained and systemic strategic communications effort aimed at exposing the hypocrisy of Islamists' words versus their deeds could knock them off balance, as could embarrassing their leadership by bringing to light their seamy connections to criminal enterprises and drug trafficking organizations. Brokering infighting within and between al Qaeda, its affiliates, and the broader jihadi orbit in which they reside, will damage violent Islamists' capability to propagate their message and organize operations both at home and abroad. Locally administered programs are especially significant, as many of the solutions reside outside the U.S. government and will require communities policing themselves.[16] In the last year or two, the United States has made some headway on these fronts, including through the efforts of the Department of State's Office of Strategic Communications—but we could do more and we could (and should) hit harder, especially when our adversaries are back on their heels. Indeed, now is the time to double down rather than ease up on the pressure. In short, we must encourage defectors, delegitimize and disaggregate our adversaries' narrative, and above all, remember the victims.

Cybersecurity

To my mind, the cybersecurity community's state of development is akin to that of the counterterrorism community as it stood shortly after 9/11. Although much work remains to be done on the counterterrorism side, as I emphasized above the country has also achieved significant progress in this area. On the cybersecurity side however, the threat (and supporting technology) have markedly outpaced our prevention and response efforts. Despite multiple incidents that could

---

[13] http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf

[14] James Carafano, Frank Cilluffo, Richard Weitz et al. "Stopping Surprise Attacks: Thinking Smarter About Homeland Security" *Backgrounder* (April 23, 2007). http://www.heritage.org/research/reports/2007/04/stopping-surprise-attacks-thinking-smarter-about-homeland-security

[15] Frank J. Cilluffo, J. Scott Carpenter, and Matthew Levitt "What's the Big Idea? Confronting the Ideology of Islamist Extremism" *Joint Report of HSPI and the Washington Institute for Near East Policy* (February 4, 2011). http://www.gwumc.edu/hspi/policy/issuebrief_confrontingideology.pdf. See also: Letter from Senators Lieberman and Collins to the Honorable John Brennan, Assistant to the President for Homeland Security and Counterterrorism and Deputy National Security Advisor (April 2, 2011).

[16] Cilluffo, Carpenter, and Levitt "What's the Big Idea? Confronting the Ideology of Islamist Extremism."

have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed, and not just within Government, we have yet to take those necessary steps.

The cyber threat is multifaceted and may emanate from individual hackers, hacktivists, criminal or terrorist groups, nation-states or those that they sponsor. The threat spectrum is multifaceted, and affects the public and private sectors, the interface and intersections between them, as well as individual citizens. National security, economic security, and intellectual property are just some of the major interests at stake. Prevention and response requires cooperation and collaboration, in real-time, against sophisticated adversaries. By and large, from a homeland security perspective, at least in terms of sophistication, foreign states are our principal concerns—specifically those that pose an advanced and persistent threat, namely Russia and China. Their tactics may also be exploited by others. Beyond the cited states, other countries such as Iran and North Korea, are not yet on a par with Russia and China insofar as capabilities are concerned—but what Iran and North Korea lack in indigenous capability they make up for in terms of intent.[17] Where there is motivation, persistence tends to follow. The challenge is not only asymmetric in character, but complicated by the nuclear backdrop, as Iran drives towards acquiring nuclear weapons. It would not be wise to ignore these potential threat vectors. Iran is increasingly investing in bolstering its own cyberwar capabilities. Bear in mind also that many of the capabilities that do not exist indigenously may be purchased—making it possible to craft a hybrid threat. There is a veritable arms bazaar of cyber weapons. Our adversaries just need the cash.

Making a complex situation even more complicated, evolution in the cyber domain has taken place so rapidly that the concepts and categories that would ordinarily underlie policy have yet to be fully debated and defined. There is a void in terms of doctrine because fundamental operating principles have yet to be elaborated and developed. Some discussions are underway, such as within the Department of Defense (DoD), where the rules of engagement to apply in this newest domain are currently top of mind. The nature of the challenge, however, requires a national conversation and we as a country have yet to have that talk. Only recently, in the wake of "Stuxnet" and "Flame" and other operations targeting our adversaries and networks of interest, have we begun to see editorial boards as well as current and former senior military and civilian leaders place the issues squarely on the table with an eye to airing them openly and encouraging a whole-of-society consideration of both problem and solution. For instance, former head of the CIA and the NSA, General Michael Hayden, has (rightly I would suggest) characterized Stuxnet as both "`a good idea'" and "`a big idea'"—suggesting also that it represents a crossing of the Rubicon.[18] Developing doctrine, especially in terms of cyber offense, requires this type of engagement so as to ensure that policy is carefully crafted and widely supported.

As we carve out the contours of what is an act of war in cyberspace and formulate answers and options to other crucial questions, foreign intelligence services are engaging in cyber espionage against us, often combining technical and human intelligence in their exploits.[19] Everything from critical infrastructure to intellectual property is potentially at risk. These exploits permit others to leapfrog many bounds beyond their rightful place in the innovation cycle, by profiting from (theft of) the research and development in which private and public U.S. entities invested heavily. At worst, these exploits hold the potential to bring this country and its means of national defense and national

---

[17] Cilluffo Testimony, "The Iranian Cyber Threat to the United States" (April 26, 2012). http://www.gwumc.edu/hspi/policy/testimony4.26.12_cilluffo.pdf

[18] CBS News, "Fmr. CIA head calls Stuxnet virus `good idea'" *60 Minutes* (March 1, 2012). http://www.cbsnews.com/8301-18560_162-57388982/fmr-cia-head-calls-stuxnet-virus-good-idea/

[19] Frank J. Cilluffo and Sharon L. Cardash "Commentary: Defense Strategy Avoids Tackling the Most Critical Issues" *Nextgov* (July 28, 2011). http://www.nextgov.com/cybersecurity/2011/07/commentary-defense-cyber-strategy-avoids-tackling-the-most-critical-issues/49494/

security to a halt, and thereby undermine the trust and confidence of the American people in their Government. Indeed, one wonders what purpose the mapping of critical U.S. infrastructure by our adversaries might serve other than what is known in military terms as intelligence preparation of the battlefield. To my mind, the line between this type of reconnaissance and an act of aggression is very thin, turning only on the matter of intent.

Unfortunately, there is no lack of evidence of intent. By way of example, U.S. officials are investigating "reports that Iranian and Venezuelan diplomats in Mexico were involved in planned cyberattacks against U.S. targets, including nuclear power plants." Press reports based on a Univision (Spanish TV) documentary that contained "secretly recorded footage of Iranian and Venezuelan diplomats being briefed on the planned attacks and promising to pass information to their governments," allege that "the hackers discussed possible targets, including the FBI, the CIA and the Pentagon, and nuclear facilities, both military and civilian. The hackers said they were seeking passwords to protected systems and sought support and funding from the diplomats."[20]

In June 2011, Hezbollah too entered the fray, establishing the Cyber Hezbollah organization. Law enforcement officials note that the organization's goals and objectives include training and mobilizing pro-regime (that is, Government of Iran) activists in cyberspace. In turn and in part, this involves raising awareness of, and schooling others in, the tactics of cyberwarfare. Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. Even worse, each such exploit generates additional opportunities to gather yet more data, as new potential targets are identified, and tailored methods and means of approaching them are discovered and developed.

Officials in the homeland security community must therefore undertake contingency planning that incorporates attacks on U.S. infrastructure. At minimum, "red-teaming" and additional threat assessments are needed. The latter should include modalities of attack and potential consequences. The United States should also develop and clearly articulate a cyber-deterrence strategy. The current situation is arguably the worst of all worlds: certain adversaries have been singled out in Government documents released in the public domain, yet it is not altogether clear what we are doing about these activities directed against us.[21] The better course would be to undertake and implement a cyber-deterrence policy that seeks to dissuade, deter, and compel both as a general matter, and in a tailored manner that is actor/adversary-specific. A solid general posture could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This would free up resources (human, capital, technological, etc.) to focus in context-specific fashion on the remainder, which constitute the toughest threats and problems, in terms of their level of sophistication and determination. To operationalize these recommendations, we must draw lines in the sand or, in this case, the silicon. Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach will not be tolerated. The entire exercise must, of course, be underpinned by all-source intelligence. Lest the task at hand seem overly daunting, remember that we have in past successfully forged strategy and policy in another new domain devoid of borders, namely outer space.

---

[20] Shaun Waterman "U.S. authorities probing alleged cyberattack plot by Venezuela, Iran" *The Washington Times* (December 13, 2011). http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all

[21] See Bryan Krekel et al. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," *Report of the U.S.-China Security and Review Commission* (2011); Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Secrets in Cyberspace" *Report to Congress on Foreign Economic Collection, 2009-2011* (2011) for the espionage activities of China and Russia in particular.

An "active defense" capability—meaning the ability to immediately attribute and counter attacks—is needed to address future threats in real-time. Active defense is a complex undertaking however, as it requires meeting the adversary closer to their territory, which in turn demands the merger of our foreign intelligence capabilities with U.S. defensive and offensive cyber capabilities (and potentially may require updating relevant authorities). Sometimes, however, the best defense is a good offense. Having a full complement of instruments in our toolkit and publicizing that fact, minus the details (which is not to confused with harmful leaks regarding specific operations), will help deter potential adversaries—provided that we also signal a credible commitment to enforcing compliance with U.S. redlines. Again history provides guidance, suggesting two focal points upon which we should build our efforts. One is leadership—we must find the cyber equivalents of Billy Mitchell or George Patton, leaders who understand the tactical and strategic uses of new technologies and weapons. The other is force protection—not only must we develop offensive capabilities, but we ought to make sure we develop second-strike capabilities. We cannot simply firewall our way out of the problem. U.S. Cyber Command must both lend and receive support, if our cyber doctrine is to evolve smartly and if our cyber power is to be exercised effectively.

While it is up to the Government to lead by example by getting its own house in order, cybersecurity and infrastructure protection do not constitute areas where Government can go it alone. With the majority of U.S. critical infrastructure owned and operated privately, robust public-private partnerships are essential, as is a companion commitment by the private sector to take the steps necessary to reinforce national and homeland security. Government and industry must demonstrate the will and leadership to take the tough decisions and actions necessary in this sphere. While we cannot expect the private sector to defend itself alone from attacks by foreign intelligence services, we need to do a better job (as a country) of making the business case for cybersecurity. Failure to shore up our vulnerabilities has national security implications. Yet crucial questions remain open, such as how much cybersecurity is enough, and who is responsible for providing it?

The facts that prevail support the need for standards. Ideally these should be identified and self-initiated (along with best practices) by the private sector, across critical industries and infrastructures, together with an enforcement role for Government, to raise the bar higher—in order to protect and promote, not stifle, innovation. The economic and intellectual engines that made this country what it is today (not to mention the inventors of the Internet) are, arguably, our greatest resource. They will power us into the future too, so long as we act wisely and carefully to foster an environment in which they can continue to thrive and grow. To be blunt, legislation along these lines is needed, and it is needed now, in order to remedy crucial gaps and shortfalls, and hold critical infrastructure owners and operators accountable, by focusing on behavior rather than regulating technology. The call has come from a range of powerful, thoughtful and well informed voices including former Secretary of Homeland Security Michael Chertoff in a joint letter with former Director of National Intelligence, Admiral Mike McConnell, and others[22]; and even from industry such as Northrop Grumman Corporation's Chairman, CEO and President, Wes Bush.[23] At the same time though, a mix of incentives is needed, to include tax breaks, liability protections, and insurance premium discounts, for private owners and operators of critical infrastructure to take the steps needed to help improve our overall level of security. These measures must also be accompanied by a mechanism to enable and encourage information sharing between the public and private sectors. In addition, as Admiral McConnell has suggested: the information exchanged must be "extensive,...sensitive and meaningful," and the sharing must take place in "real-time" so as to

[22] Chris Strohm, "Chertoff Urges Swift Action by Senate on Cybersecurity Measures" *Bloomberg Businessweek* (January 25, 2012). http://www.businessweek.com/news/2012-01-25/chertoff-urges-swift-action-by-senate-on-cybersecurity-measures.html
[23] "Effective Cybersecurity: Perspectives on a National Solution" *The 13th Annual Robert P. Maxon Lecture* (April 9, 2012). http://www.gwumc.edu/hspi/events/gwsbBush.cfm

match the pace of the cyber threat. There must be "tangible benefits" for those yielding up the information.[24]

Now is the time to act. For too long, we have been far too long on nouns, and far too short on verbs. The imperative is further underscored if we are to have, as I have recommended, a robust offensive capability. In short, if we are going to do unto others, then we should first be fully inoculated and prepared to defend against others doing the same unto us. This principle is all the more applicable in the cyber context, where blowback against the party initiating first-use of a cyber-weapon is more likely than not, once that weapon is released into the wild and the so-called law of unintended consequences kicks into effect. But readiness is no simple matter in this context, certainly not across the board. Put another way, one of the cyber-related challenges facing this country is that the departments with the greatest capabilities (such as NSA) do not have all the authorities, whereas the departments whose capacities are more nascent (such as DHS) are endowed with relatively greater authority. This misalignment of authorities and capabilities presents and poses challenges in a range of contexts including computer network exploit and attack (CNE and CNA) as well as computer network defense (CND) and cybersecurity more generally. Figuring out how best to bridge the gap between authorities and capabilities is a vexing challenge, but one that would serve us well to think through carefully and in clear-eyed fashion in order to achieve the best possible outcome for the Nation.

Before closing, I would stress that as much as technology matters in this area, HUMINT remains crucial as well. As a general matter, there is simply no substitute for a human source, whether a recruit in place inside a foreign intelligence service, a criminal enterprise, or a terrorist organization. The "rich picture" of the threat, mentioned above in the counterterrorism context, cannot and will not be generated without input and insights from the private sector including the owners and operators of critical infrastructure. To help keep blind spots at a minimum, these owners and operators should be part of our Fusion Centers—yet for more than half of the nation's Centers this is not the case. This notwithstanding the fact that a sizeable majority of the country's Centers are believed by their membership to have "relatively weak capabilities in regard to the gathering, receiving, and analyzing of cyber threats."[25]

Clearly we are just beginning work on the long list of to-do's that pertains to the cyber domain. Having said that, it is important to remember that even in this area, we have already learned much and that knowledge will help us chart a constructive path forward. By way of illustration, the history of the Conficker Working Group, captured in a DHS-sponsored lessons learned document, provides examples of the types of relationships that need to be established and maintained.[26] Yet there is still a long way to go. At the end of the day, the ability to reconstitute, recover, and get back on our feet is perhaps the best deterrent. The storms that recently battered the National Capitol Region, leaving close to a million people without power during a week-long heat wave, are instructive in terms of our shortcomings on resilience. Mother Nature may be a formidable adversary, but just imagine the level of damage and destruction that a determined and creative enemy could have wrought. There is no lack of trying, as a recently published DHS report makes clear, noting the spike in attacks (from 9 incidents to 198) against US critical infrastructure from 2009 to 2011.[27] The good news, on the other hand, is that the most serious of these incidents could have been avoided

---

[24] Remarks delivered at HSPI roundtable (February 22, 2012). http://www.c-spanvideo.org/program/CyberSecurityL
[25] CTISR June 2012. http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf
[26] "Conficker Working Group: Lessons Learned" June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf
[27] Suzanne Kelly "Homeland security cites sharp rise in cyber attacks" *CNN.com* (July 4, 2012). http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/

through the adoption of basic security steps and best practices. The bad news, of course, is that these fundamental measures were not yet put into place. Plainly we have not yet made the requisite business case for doing so. The urgency for doing so needs no further explanation, but we must take care to strike just the right balance of carrots and sticks and of course measures that ensure both privacy and security.

* * *

More than a decade after 9/11, and in an environment in which resource scarcity prevails, there is opportunity as well challenge—namely an opportunity to reflect and recalibrate, and move forward smartly. While there are many subjects that I have not touched on (such as chemical, biological, radiological, and nuclear weapons, from both a proliferation and terrorism perspective) my aim was to confine comment to two broad subject areas at a strategic level, thereby leaving detailed analysis and option-framing on certain important and complex areas, such as those referenced parenthetically, to other experts. Again, I wish to thank both the Committee and its staff for the opportunity to testify today, and I would be pleased to try to answer any questions that you may have.

KOSTAS
Research Institute
for Homeland Security

"The New Homeland Security Imperative: The Case for Building Greater Societal and Infrastructure Resilience"

Written Testimony
prepared for a hearing of the

Committee on Homeland Security and Governmental Affairs
U.S. Senate

on

"The Future of Homeland Security: Evolving and Emerging Threats"

by

Stephen E. Flynn, Ph.D.
Founding Co-Director
George J. Kostas Research Institute for Homeland Security &
Professor of Political Science
Northeastern University
s.flynn@neu.edu

Dirksen Senate Office Building - Room 342
Washington, DC

10:00 a.m.
Jul 11, 2012

"The New Homeland Security Imperative:
The Case for Building Greater Societal and Infrastructure Resilience"

by

Stephen E. Flynn, Ph.D.
Professor & Founding Co-Director, Kostas Research Institute
Northeastern University

Chairman Lieberman, Ranking Member Collins, distinguished members of the Committee on Homeland Security and Government Affairs, thank you for the opportunity to testify before you as a part of this important series of hearings on the future of homeland security. Mr. Chairman, I first testified on this topic on October 12, 2001, when you held the gavel of the predecessor of this committee, the Committee on Governmental Affairs. That was just one-month after the tragic attacks of September 11, 2001. At that time, I concluded my testimony by observing: "Terrorists have declared war on this homeland. This nation is extremely vulnerable to these kinds of attacks. We need to come to grip with that fact and recognize that we have to fundamentally rethink and reorganize how we provide for the security of this nation in this new and dangerous era." Thanks to the leadership provided by this Committee and especially both you, Mr. Chairman, and Senator Collins, considerable progress has been made towards repairing what was essentially a broken system for managing the kind of threat posed by al Qaeda more than a decade ago. I want to personally express my deepest respect and gratitude for the extraordinary service you have provided this nation. But the threat continues to evolve, and the challenge of securing the American homeland is an extremely complex one. Accordingly, it could not be more timely and appropriate to take stock at this juncture of where we are and where we need to go to advance the homeland security mission.

Assessing the Threat:

As my fellow witnesses can speak to in more detail than I, the state of the al Qaeda threat in 2012 is a good news and not-so-good news story. The good news is that the successful dismantling of so much of al Qaeda's senior leadership infrastructure including the May 1, 2011 death of Osama bin Laden, has reduced the capacity for al Qaeda to plan and execute sophisticated large-scale attacks on North America. The not-so-good news is that there is a continued risk of small-scale attacks executed by homegrown and other affiliated terrorists of al Qaeda and that these attacks are more difficult to prevent. Major attacks require a group of operatives directed by a leader, communications with those overseeing the planning, and time to conduct surveillance and rehearse the attack. Money, identity documents, safehouses for operatives, and other logistical needs have to be supported. All this effort ends up creating multiple opportunities for detection and interception by intelligence and law enforcement officials. Alternatively, small attacks carried out by 1-3 operatives, particularly if they reside in the United States, can be carried out with little planning and on relatively short notice. As such, they are unlikely to attract the attention of the national intelligence community and the attacks, once underway, are almost impossible for the federal law enforcement community to stop.

While the move towards carrying out smaller-scale attacks undoubtedly reflects a practical necessity of a much diminished core al Qaeda, these attacks also reflect a growing realization that terrorist attacks on the United States do not have to be spectacular or catastrophic to be effective. As the attempted bombing of Northwest Airlines Flight Number 253 on Christmas Day 2009 dramatically illustrated, even near-miss attacks can generate considerable political fallout and a rush to impose expensive and economically disruptive new protective measures. Since relatively small and unsophisticated attacks have the potential to generate such a big-bang for a relatively small investment, the bar can be lowered for recruiting terrorist operatives, including those who belong to the targeted societies.

The October 2010 air cargo incident involving explosives hidden ink cartridges shipped from Yemen is consistent with this trend towards smaller attacks, but with the added element of aspiring to create significant economic disruption. The would-be bombers had no way of knowing that the cartridges would end up on a commercial airliner with hundreds of passengers or a dedicated air cargo carrier with a small crew. That was not important since they understood that destroying any plane in midair would trigger U.S. officials and others to undertake an extremely costly and profoundly disruptive response that would undermine the movement of global air cargo.

Beyond the threat posed by al Qaeda, there is a more worrisome reality that arises from the otherwise enviable position associated with the United States standing as the world's sole superpower. Quite simply, it has become reckless for our current and future adversaries to challenge the United States by engaging in the kind of warfare we are best prepared to fight. Their better option is to take the battle to the civil and economic space as opposed to engaging in direct combat with our second-to-none armed forces. Targeting innocent civilians and critical infrastructure such as the intermodal transportation system, mass transit, refineries, food supply, and the electric power grid holds out the best promise for producing mass disruption to essential systems and networks, and in generating widespread fear. As such, even if al Qaeda disappeared tomorrow, acts of terrorism and cyber attacks will be the asymmetric weapons of choice for state and non-state actors intent on confronting U.S. power in the 21st Century. We need to improve our capacity to defend against those attacks by reducing our vulnerabilities and building greater resilience so as to assure the continuity or rapid restoration of critical functions, services, and values in the face of disruptive events.

The Limits of Going on the Offense

In response to the attacks on 9/11, the Bush Administration mobilized U.S. national security capabilities to go after al Qaeda and those within the international community who supported them. To an overwhelming extent, the strategy was one of prevention by way of military force supported by stepped-up intelligence. On May 19, 2004, Vice President Dick Cheney summarized the effort this way: "Wars are not won on the defensive. To fully and finally remove this danger (of terrorism), we have only one option—and that's to take the fight to the enemy." The hoped for outcome of engaging the threat in Iraq and Afghanistan and around the world, President George W. Bush declared on July 4, 2004, was "so we do not have to face them here at home." This

strategy has involved a considerable amount of national treasure. According to the Congressional Research Service, between 2001 and 2011, Congress approved $1.28 trillion dollars for the Operation Enduring Freedom (OEF) Afghanistan and other counter terror operations; Operation Noble Eagle (ONE) providing enhanced security at military bases; and Operation Iraqi Freedom (OIF).[1] That amount translates into a burn-rate of $350 million for each and every day for ten years. By contrast, the cost of one-hour of these war operations—$15 million—has been the most that has been invested in the entire annual budget for the Citizens Corps Program which was initiated after 9/11 to engage citizens in the homeland security mission by volunteering to support emergency responders.

While a case can be made that going on the offensive in the global war on terrorism has paid off in preventing another catastrophic terrorist attack on U.S. soil, as the testimony of this panel today makes clear, the danger of terrorism has not been removed. Instead it has changed, while other evolving threats to the homeland continue to grow.

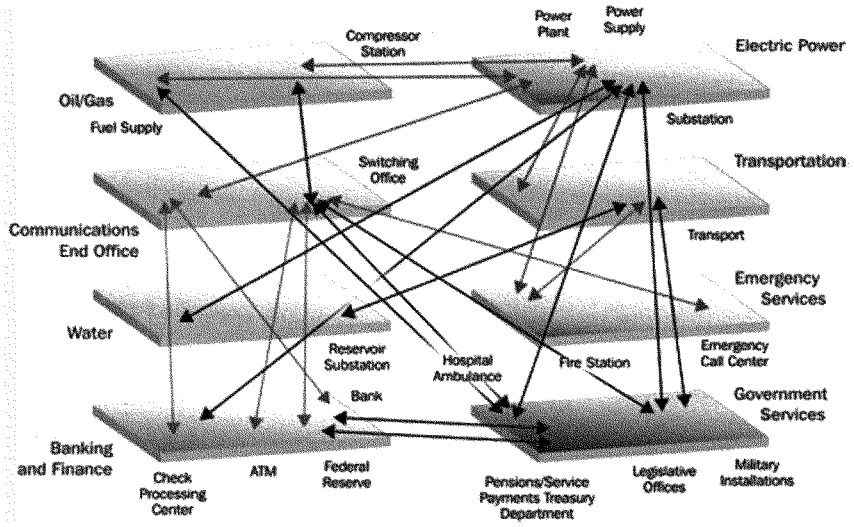
The Growing Cyber Threat:

The cyber security threat is clearly one of the most serious economic and national security challenges we face as a nation. Quite simply, the United States is at risk of becoming a victim of its own success. Our position as the world's dominant economic power can be attributed in no small part to the speed at which Americans have developed and embraced information technology systems and applications. But while we have been leading and benefiting from the information age, there has been too little consideration to the security implications of our growing reliance on information technologies.

A particularly worrisome vulnerability is the extent to which over the past decade, more and more Internet Protocol (IP) devices have been replacing legacy hardware, software, and communications protocols for the nation's physical infrastructure. As industrial control systems (ICS) become increasingly accessible to the Internet, cyber attacks can be launched at the electrical power grid; water and waste management systems; oil pipelines, refineries, and power-generation plants; and transportation systems ranging from mass-transit to maritime port operations. An attack on these systems by a state or non-state actor, not only places at risk the security of sensitive data and the disruption of essential services, but the potential for catastrophic loss of life and destruction of property. This is because computer hackers are not only able to infiltrate systems, but they are increasingly in a position to actually take control of such systems – turning off alarms or sending bad data that falsely triggers an alarm. Unfortunately, these cyber attacks need not be terribly sophisticated in order to accomplish substantial harm. Because of the interconnectivity of our networks, successful disabling of just one critical system can generate cascading consequences across multiple systems.

[1] Amy Belasco, The Cost Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11. Congressional Research Service, Mar 29, 2011, http://www.fas.org/sgp/crs/natsec/RL33110.pd.

POTENTIAL CASCADING EFFECTS OF ELECTRIC POWER FAILURE



Source: Department of Homeland Security[2]

The ongoing vulnerability of transportation systems to mass disruption:

Mass transit systems and rail freight are likely to become increasingly attractive targets for terrorist organization. These systems are relatively easy to access since they provide multiple entry points, very often over a vast geographic area, with little to no physical security barriers to entry. Homegrown terrorists are likely to be familiar with these systems. Attacks on mass transit, especially stations, particularly when undertaken during peak-commuting hours, can potentially be even more deadly than an attack on a single aircraft. At the same time, should such an attack lead to the shutting down of a transit system, the resultant denial of service can be crippling to the operation of a major urban economy.

The intermodal transportation system also remains extremely vulnerable to mass disruption. Despite new security initiatives advanced in the aftermath of 9/11, there

[2] National Aeronautics and Space Administration. NASA Science News. Severe Space Weather – Social and Economic Impacts. June 2009 at http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather/

remains too few meaningful measures in place for detecting and intercepting a determined terrorist that is intent on placing a shielded nuclear device in a container with the goal of generating fear that leads to the slowing or stopping of the flow of cargo containers into U.S. ports or across our land borders. Particularly worrisome is that virtually all containers that Customs and Border Protection currently targets as suspicious enough to warrant an inspection, are not actually examined until after those containers arrive at a U.S. port which are often in major urban areas where other critical infrastructure is concentrated. This remains the situation despite the fact that CBP currently has inspectors in 58 overseas ports as a result of the Container Security Initiative that was begun in 2002 for the stated purpose of facilitating collaboration with foreign customs officials so that targeted containers would be inspected before they are shipped to the U.S. ports.

On February 6, 2012, CBP Acting Assistant Commissioner Kevin McAleenan testified before the House Subcommittee of Border and Maritime Security that the total amount of containers inspected overseas in 2011 was just 45,500. This represents 0.5% of the 9.5 million manifests that CBP stated that the agency reviewed overseas in advance of loading. If the 45,500 number is divided by the 58 CSI ports and 365 days per year, the result is CSI inspectors are examining with their foreign counterparts on average, 2.15 containers per day per overseas port before they are loaded on carriers bound for the US--two containers each day.[3] This does not represent much of a deterrent. As the ongoing incidence of contraband smuggling, trade fraud, and cargo theft make clear, we have a long way to go in securing global supply chains against the threat of proliferation as well as the nightmare scenario of transportation conveyances being used as a WMD delivery device.

Natural Disasters as the clearest and most present homeland security danger

In addition to the ongoing risk associated with terrorism, there is an even more clear and present danger to the safety of Americans that should animate the homeland security mission: natural disasters. One need look no further than the news headlines from the past 2-3 weeks for confirmation of this reality: severe storms and power outages across the mid-Atlantic states, wildfires in Colorado and Utah, and devastating floods in Minnesota and Wisconsin. It turns out that 91 percent of Americans live in places at a moderate risk of earthquakes, volcanoes, tornadoes, wildfires, hurricanes, flooding, high-wind damage according to an estimate calculated for *Time* by the Hazards and Vulnerability Research Institute at the University of South Carolina.[4] This translates into virtually all of us being on tap to experience several major disasters in the course of our individual lifetimes. Then too, there is the risk of major pandemics and the occasional large industrial disasters such as the Deepwater Horizon oil spill and the nuclear

[3] "Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Security the Supply Chain." Joint Testimony of David Heyman, Paul Sukunft, and Kevin McAleenan before the House Committee on Homeland Security, Feb 7, 2012: 10.
[4] Amanda Ripley, "Floods, Tornadoes, Hurricanes, Wildfires, Earthquakes ... Why We Don't Prepare, TIME, Aug 20, 2006.

meltdown at Fukushima Daiichi Nuclear Power Plant. The bottom-line is that our safety requires greater levels of preparedness to deal with risk at home.

Recalibrating the Homeland Security Enterprise

Coping with the array of threats and vulnerabilities that remain more than a decade after 9/11 requires a recalibrated approach that places new emphasis on localized, open, and inclusive engagement of civil society. Recently, it has been the actions of ordinary citizens that have been critical to thwarting terrorism threats on U.S. soil. In the case of the attempted car-bombing on New York's Time Square in May 2010, it was a sidewalk T-shirt vendor, not a nearby police patrol officer who sounded the alarm about Faisal Shazhad's SUV. On Christmas Day 2009, it was courageous passengers and flight-crew members, not a federal air marshal, that disrupted the suicide-bombing attempt by Umar Farouk Abdulmutallab aboard Northwest Airlines Flight 253.

Everyday civilians, supported by state and local officials, will need to be better informed and empowered to play a meaningful role. This role includes not only preventing acts of terrorism, but making investments that mitigate the risk of disruption to our communities and critical infrastructure. This will require a homeland security enterprise centered around three efforts: (1) setting appropriate expectations, (2) increasing transparency, and (3) building community and infrastructure resilience.

Setting Appropriate Expectations. Elected officials with the support of national security professionals need to avoid promising more than the federal government can reasonably deliver. As a stepping-off point, leaders of both political parties should publicly acknowledge that there are inherent limits to what can be done to prevent acts of terror. No security regime is foolproof. Risk is a fact of life and making decisions about how best to manage those risks involves difficult tradeoffs. When new technologies and security protocols are deployed, they should not be oversold. Creating unrealistic expectations guarantees public anger, disappointment, and mistrust when a terrorist attack succeeds. The goal should be for a security regime to be able to survive a "morning-after-test;" that is; it should be able to withstand a postmortem where the public concludes that the regime consisted of reasonable safeguards, even if they were not infallible. The goal should be to have adaptive security systems that adjust based on an ongoing assessment of threat, vulnerability, and consequence.

Increasing transparency. U.S. national security and federal law enforcement agencies need to resist the secrecy reflex. On the surface, it seems sensible to tightly control information about vulnerabilities or security measures that potential adversaries might exploit. But these restrictions can undermine the defense of critical infrastructure, such as seaports, dams, and waterworks. In determining the best way to protect a suspension bridge, for example, the bridge's chief engineer is likely to have ideas that would not occur to a law enforcement or national security professional. But strict rules that preclude the sharing of homeland security information with unvetted individuals too often translates into leaving essential expertise on the sidelines. Even when security information is shared with vetted company security officers, they are precluded from passing along the details to their bosses who do not hold active security clearances. As a

result, investment and operational decisions are often made with scant attention paid to the potential security stakes.

The federal government should make a concerted effort to increase transparency with the broader public as well. Many policymakers believe that candor about potential dangers may generate excessive public anxiety. However, people are most frightened when they sense not only their vulnerability to threats, but feel powerless to address them. U.S. officials have stated for nearly a decade that terrorism is a clear and present danger, but they have given citizens little information about how to cope with that hazard. Instead, citizens are told to proceed with their daily routines because their government is hard at work protecting them. The psychological effect of this is similar to that of a doctor telling a patient that she is afflicted with a potentially life-threatening illness and then providing only vague guidance about how to combat it. No one wants to receive disturbing news from his physician, but a prognosis becomes less stressful when doctors provide patients with all the details, a clear description of the available treatments, and the opportunity to make decisions that allow the patient to assert some personal control over the outcome. In the same way the federal government can decrease the fears of terrorism by giving the American public the information it needs to better withstand, rapidly recover, and adapt to the next major terrorist attack.

Building Resilience:

Terrorist attacks perpetrated by homegrown operatives who act along or with one or two-accomplices are more difficult to detect and intercept. As a result there is a greater probability that these less-sophisticated attacks will be successful. At the same time, the resultant damage from a small-scale attack is likely to be localized and far less than typically experienced during and after a natural disaster that Americans have become largely accustomed to coping with. Therefore, the incentive for launching small-scale attacks on U.S. soil lies with causing our society to react in a way that amplifies the direct damage generated by the attack. In other words, how we respond to acts of terrorism effects our adversaries' calculation about undertaking these attacks. If we provide them with a "big bang" for their relatively modest, buck, we end up fueling the incentive for terrorist activity. Alternatively, if the result was something of a fizzle, there will be little to be gained from carrying out these attacks.

As a way forward, Washington should place greater emphasis on developing adequate societal and infrastructure resilience. Resilience is the capacity of individuals, communities, companies, and the government to withstand, respond to, recover from, and adapt to disruptive events. Since disruptions can come not just from terrorism but also from natural and accidental sources as well, advancing resilience translates into building a general level of preparedness.

Ideally, a program of resilience would address the most likely risks that people, cities, or enterprises may face. This would minimize the potential for complacency while assuring a level of basic skills, such as first aid and effective emergency communications, which are useful no matter the hazard.

A program of resilience requires individuals, communities, and companies to take precautions within their respective areas of control. Success is measured by the continuity or rapid restoration of important systems, infrastructure, and societal values in the face of an attack or other danger.

Resilience begins on the level of individuals. A program of resilience would promote self-reliance in the face of unexpected events, encouraging civilians to remain calm when the normal rhythms of life get interrupted. It would also teach individuals to make themselves aware of the risks that may confront them and to be resourceful by learning how to react to crises. And it would make preparedness a civic virtue by instructing civilians to refrain from requesting professional assistance unless absolutely necessary, thus freeing up manpower for those in the greatest need.

Promoting individual resilience involves acknowledging that many Americans have become increasingly complacent and helpless in the face of large-scale danger. Reversing this trend demands a special emphasis on educating young people. Students should learn to embrace preparedness as both a practical necessity and an opportunity to serve others. These students, in turn, can teach their parents information-age survival skills, such as texting, which may offer the only means to communicate when cellular networks are overloaded (800 text messages consume the same bandwidth as a one-minute call). As demonstrated in the aftermath of the 2010 Haitian earthquake and the Deepwater Horizon oil spill that same year, social media are transforming the way rescuers and survivors respond to crises. These new tools have the power to turn traditional, top-down emergency management on its head.

Resilience also applies to communities. The U.S. government can promote resilience on the communal level by providing meaningful incentives for collaboration across the public, private, and nonprofit sectors before, during, and after disasters. Much like at the individual level of resilience, communities should aspire to cope with disasters without outside assistance to the greatest degree possible.

Building resilient communities requires providing community leaders with tools to measure and improve their preparedness based on a widely accepted standard. The Community and Regional Resilience Institute, a government-funded research program formerly based at Tennessee's Oak Ridge National Laboratory and now located at the non-profit Meridian Institute, has spearheaded an attempt to define the parameters of resilience, modeled on the method by which fire and building codes were created and are maintained. Led by Warren Edwards, it has drawn on a steering committee that I was privileged to chair and a network of former governors and former and current mayors, emergency planners, and academics to develop detailed guidelines and comprehensive supporting resources that will allow communities to devise resilience plans tailored to their needs. Other countries, including Australia, Israel, and the United Kingdom, have instituted similar programs. Federal and state governments could provide communities that implement a comprehensive risk-awareness strategy and a broad-based engagement program with tangible financial rewards, such a reduced insurance premiums and improved bond ratings.

U.S. companies compose the third tier of resilience. Resilient companies should make business continuity a top priority in the face of a disaster. They should invest in contingency planning and employee training that allow them to serve and protect their customers under any circumstance. Corporations must also study the capabilities of and partner with their suppliers and surrounding communities. Much like individuals and communities, corporations with resilience would possess the ability to sustain essential functions and quickly resume their operations at full capacity after a disaster. Resilience may also bring financial benefits to companies able to demonstrate their dependability in the wake of a major disruption. Such companies are likely to experience an increase in market share by maintaining regular customers and attracting new ones as well.

Although most large corporations invest in measures that improve resilience, smaller companies—which are the backbone of local economies and yet are constrained by limited resources—generally do not. But small businesses can rectify this in a low-cost manner by creating a buddy system between companies located in different regions. For instance, a furniture store in Gulfport, Mississippi, that may fall victim to an August hurricane could partner with a furniture store in Nashville, Tennessee, that may suffer from spring flooding. These businesses would agree to assist each other in providing backup support for data, personnel, customers, and suppliers in the event of a disaster.

To his credit, President Obama has explicitly identified resilience as a national security imperative in his May 2010 National Security Strategy. Homeland Security Secretary Janet Napolitano did the same in the February 2010 Quadrennial Homeland Security Review. Both have made frequent references to the importance of resilience in their speeches. But much more needs to be done to tangibly advance this agenda, and it will require an all-hands approach. This is why I along with my colleague Peter Boynton feel so privileged to have been appointed the founding co-directors of the George J. Kostas Research Institute for Homeland Security at Northeastern University.

I have long argued that universities and colleges have been a largely overlooked national resource in advancing the homeland security enterprise. Beyond the academic Centers of Excellence established by the Department of Homeland Security, and courses and programs designed to educate homeland security professionals, the higher education community has largely sat on the sidelines as federal, state, and local governments have struggled to find their way in the post-9/11 world. This not the case at Northeastern where President Joseph Aoun has made security one of three areas of strategic emphasis for its growing research enterprise. In addition, thanks to the generous gift of Northeastern alumnus and trustee, George J. Kostas, the university has built a new facility that offers a secure environment for innovative translational research conducted by private-public-academic multidisciplinary research teams.

At the Kostas Institute, our mission is to help advance resilience in the face of 21st Century risks. We have made community resilience and infrastructure and systems resilience our primary area of focus. We are a particularly interested in identifying and advancing ways to "bake-in" to the operations and design of critical systems, especially those involving transportation and information, so as to enhance their security, integrity, and continuity in the face of man-made and naturally occurring disasters. Given the

historic leadership role that Northeastern, our neighboring universities, and the information technology industry that is concentrated in the metro-Boston area have played, we feel a special responsibility to help manage the growing risks to critical systems from cyber threats. To this end, we are committed to bringing together expert researchers and practitioners to identify risks and their potential consequences, to develop next-generation secure applications and computing architecture, and to promote best practices with our counterparts around the U.S. and globally.

Conclusion

For most of the 20th Century, the United States was able to manage our national security as the equivalent to an away game; that is; by confronting threats beyond our shores. That all changed on September 11, 2001. Yet as a nation, we continue to struggle with defining the appropriate role and investment that the federal government should make in managing our ongoing vulnerability to terrorism and other catastrophic risks on U.S. soil. From the standpoint of resources, the investment Washington makes in homeland security remains a fraction of the resources devoted to traditional national security. At times, this can have the perverse outcome of actually making civilian targets potentially more attractive to our adversaries. For instance, the U.S. Navy has invested more in protecting the single port of San Diego that is home to the Pacific Fleet, than the Department of Homeland Security has invested in the ports of Los Angeles, Long Beach, San Francisco, Oakland, Seattle, and Tacoma *combined* upon which the bulk of the U.S. economy relies.

It will take determined leadership to recalibrate our national and homeland security efforts to better managed the evolving and emerging threats that confront us. Mr. Chairman, throughout your long and distinguished career in the U.S. Senate, you have been providing that leadership. I commend you for the instrumental role you have played in advancing the safety and wellbeing of this great nation.

I want to thank you for the opportunity to once again testify before this committee today. I would be happy to answer any questions you may have.

Responses to post hearing questions, "The Future of Homeland Security: Evolving and Future Threats"

Gen. Michael Hayden (USAF, ret.) August 16, 2012

Senator Joseph Lieberman:

1. In your testimony you discuss how key threats that we face, such as terrorism, cyber threats, and transnational organized crime are all becoming increasingly interrelated, noting that they "all merge in a witch's brew of danger."

However, our federal government is still largely stove-piped in facing these threats. Distinct sets of agencies are responsible for addressing each of these threats, using distinct legal authorities, operational procedures, and information systems.

What needs to be done to increase collaboration among agencies across these multiple threat domains in cases where threats overlap or converge? Do we need to consider new organizational approaches within the federal government for addressing the convergence of these different threats?

The answer lies in increasing collaboration, rather than creating new bodies or rearranging existing ones. Mechanisms need to be developed that enhance the free flow of information and the adaptability of authorities. Simultaneously, oversight and accountability must be adjusted in tandem to maintain integrity and security.

The current Congressional oversight model mirrors divisions in the executive branch (if not even more so). As such, Congress has the unique opportunity to lead the way by reducing the intense fractionalization of oversight in the current committee structure. This change would provide the appropriate incentives and support for agencies to break down a certain degree of jurisdictional boundaries between their organizations.

Senator Claire McCaskill:

1. You mentioned that you think the old formula of countering foreign threats through intelligence and domestic threats through law enforcement does not work anymore, but that we have struggled to find a viable alternative model.

a. *What would you recommend as an alternative model?*
   Enabling collaboration is key. As I mentioned previously, collaboration should not occur at the expense of oversight and accountability. A cross-cutting oversight model can give oxygen to information sharing models while keeping excesses in check.
b. Do you thing the criminal justice systems can be used as an effective counterrorism tool? If not, would you suggest changes to the way the current system works in order to make it more effective?
   Of course the criminal justice system is essential for counterrorism. The laws of armed conflict and the U.S. criminal justice system are not mutually exclusive. Under the AUMF, the U.S. government is fully entitled to treat terrorists as enemy combatants while fully preserving our rights to enter them into the criminal justice system. This is important because terrorists apprehended as enemy combatants

often have valuable intelligence that must be gathered in order to prevent harm against citizens and those in uniform. Once that intelligence has been exploited, then the criminal justice system could be the next appropriate step in the process toward justice.

2. The panel discussed how our increasingly interconnected world empowers small groups and continues to shape potential threats, including cyber dangers, terrorism, and transnational crime. On 9/11, there was no Facebook or Twitter, and cell phone use was a fraction of what it is today. Technology changes do not just affect our adversaries; they also affect our vulnerabilities and how we as a nation feel the effects of an attack.

a. *In your view, over the next 5-10 years, how will the same technological and societal forces that transform the threats we face also impact the effects of an attack or other incident?*
The cumulative effect of the changes you describe pushes truly disruptive and destructive power into the hands of increasingly smaller groups, as well as individuals. It will be a consistent challenge to defend ourselves from such threats while maintaining an environment in which the American way of life can thrive.

b. *What new vulnerabilities are we likely to face as a nation over the next 5-10 years?*
Like many, I continue to focus on the potential destructive effects of a sophisticated cyber attack. Such an attack sits at the intersection of high probability and maximum impact. The consequences of such an event would be extremely damaging.

c. *Do such changing technological and societal forces also present new opportunities for resilience?*
Of course they do. But in today's American political culture, we seem to be overly reluctant to discuss resilience and our ability to take a blow and move on. It will require political courage from both executive and legislative branches to inform this dialog in such a way that we take necessary steps to truly be resilient.

3. Generally speaking, how can we create a government that is more flexible, more nimble, and more capable of adapting to the evolving threats you have descried? What general qualities should such an organization have?
Again, I'd like to go back to the concept of improving the way our national security institutions, as well as state and local partners, work together. This is easier said than done, but meaningful change can be led by the way in which congressional oversight committees carry out their responsibilities. Congress has tremendous power to shape the behavior of federal institutions, and this power can be used to incentivize and reward cooperation.

4. Even more important than discussing future threats in the context of this hearing is for government agencies to have the capacity and institutional processes to evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structure we have in place to meet them?
Let me speak to NIEs, with which I am more familiar. These are good products, which are thoughtfully and carefully wrought. But they are infrequent, lengthy and consensus driven. We may be able to learn from the UK's Joint Intelligence Committee, which produces more frequent, shorter and to the point papers for senior government officials.

Brian Michael Jenkins[1]
The RAND Corporation

New Challenges to U.S. Counterterrorism Efforts
An Assessment of the Current Terrorist Threat
Addendum[2]

Before the Committee on Homeland Security and Governmental Affairs
United States Senate

August 24, 2012

The subsequent questions and answers found in this document were received from the Committee for additional information following the hearing on July 11, 2012 and were submitted for the record.

POST-HEARING QUESTIONS FROM SENATOR JOSEPH LIEBERMAN

QUESTION 1:

For the last few years terrorism analysts have focused on a relatively stable model of violent Islamist terrorism threats, involving core al Qaeda, its affiliates and allies, homegrown terrorists inspired by the ideology of violent Islamist extremism, and Iranian-linked threats.

How concerned are you about the possibility of new terrorist groups or actors posing a threat to the homeland and are outside of this model and not on the radar screen of our intelligence agencies today? Are we at risk of "strategic surprise" with respect to new terrorist groups, and if so, what more can the government do to predict and detect such unknown threats?

RESPONSE 1:

Although al Qaeda's global leadership remains dedicated to attacking the United States and therefore represents the most salient threat to the security of Americans abroad and at home, the overall terrorist threat has become more complex. To begin with, al Qaeda itself has become a term of analytical convenience—a label applied to what in actuality is an increasingly complex

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT377z1.html.

array of al Qaeda-linked and al Qaeda-inspired enterprises. Some are creations of al Qaeda; others are recent acquisitions; still others claim or aspire to al Qaeda membership or are unaffiliated jihadists lumped together under al Qaeda.

The tendency of analysts to connect all jihadist terrorism with al Qaeda turns otherwise obscure groups into a cause for concern and reinforces al Qaeda's own propaganda efforts to assert its leadership over a diverse host of organizations. A more complicated order of battle in the turbulent wake of the Arab uprisings will oblige analysts to become more discerning. An al Qaeda connection should not be the sole lens of analysis and criterion for U.S. concern.

As I mentioned in my testimony, the United States also confronts the threat of Iranian-sponsored and Hezbollah terrorism, which growing tensions with Iran and events in Syria could exacerbate. And the violence in northern Mexico, although criminally motivated, includes the use of terrorist tactics.

Beyond these obvious foreign threats, there are two potential sources of terrorist violence in the United States. They receive nowhere near the attention paid to al Qaeda, and because they are domestic in origin (as opposed to homegrown terrorists inspired by al Qaeda's ideology), domestic intelligence operations targeting these groups tend to be more delicate. One threat stream comprises anarchist extremists currently exploiting economic distress and public anger. The other stream, itself an array of groups, includes people with anti-federal-government sentiments, white supremacists, and a variety of hate organizations.

Although they continue dark themes that ebb and flow in American history, these attitudes have recently found only occasional expression in violence. For political reasons, authorities appear reluctant to apply the same scrutiny to these groups that they apply to al Qaeda-linked activity. Moreover, some of the more controversial assertions of federal authority depend upon legislation that is expressly linked to al Qaeda and the Taliban (the Authorization of Use of Military Force of 2001 and the National Defense Authorization Act of 2012) and therefore cannot be applied to the purely domestic groups. Beyond the letter of law, there are greater political risks in confronting these entirely homegrown extremists, which may explain why they receive only a fraction of the attention devoted to al Qaeda-inspired terrorism.

QUESTION 2:

The evolution of the Mexican drug cartels and other transnational criminal networks into conglomerates that no longer specialize in one kind of crime, and the growing evidence of links

between these criminal conglomerates and terrorism organizations, pose a significant threat to national and international security. As we look to the future of homeland security and how to best meet this evolving threat, it is important that we focus on aligning our law enforcement agencies on all levels to achieve a greater unified response.

a. How troubling are these links between organized crime and terrorism, and what do they mean for the future of our homeland security enterprise?

b. What do you believe the Department of Homeland Security and other key federal agencies need to do in order to proactively confront the evolving threat of transnational organized criminal networks?

RESPONSE 2:

As I indicated in my earlier testimony, Mexico's criminal conglomerates pose a threat to the United States. A push to take control of retail drug traffic in the United States could import the horrendous quality of violence seen in Mexico. Clearly, the cartels must be an intelligence-collection priority requiring the same collaboration between national intelligence agencies and local law enforcement that we have seen in the realm of terrorism.

Connections between the criminal conglomerates and terrorist organizations are certainly possible, but I have personally seen very little evidence to indicate an active relationship. Some of the terrorist tactics employed by Mexico's cartels—car bombings, beheadings—resemble Middle Eastern terrorism, but that may be the imitation of tradecraft.

Hezbollah has a presence in Mexico, as it does in the United States, but this appears to be more related to financial crime than to terrorism. And, of course, we have the reported effort by Iranians to enlist the assistance of Mexican criminals in an assassination attempt against the Saudi ambassador in Washington.

There also are prior examples of links between Hezbollah criminal networks and terrorist attacks in Argentina, while Colombia's FARC employed terrorist tactics, engaged in drug trafficking, and had connections with other foreign terrorist organizations. So the idea of links between criminal networks and terrorist organizations is not far-fetched.

Such alliances pose risks to both sides. Organized crime tends to be a conservative provider of illegal goods and services, which, in the case of drugs, provides a continuing cash flow. Alliances

with terrorists bring unwanted heat and additional adversaries, and the rules change from prosecution to destruction. Whatever money terrorists offer must be weighed against the increased risk to continuing profits and organizational survival. Good intelligence about nascent connections will bring opportunities to drive this point home.

For terrorists, allying with criminals increases the risk of betrayal. Large criminal enterprises are more penetrated with informants than are terrorist conspiracies. And lacking the terrorists' organizational zeal, ordinary criminals are more likely to cooperate with authorities.

Again, to deter or preempt any future alliances between criminal conglomerates and terrorist enterprises will require extremely good intelligence and perhaps closer cooperation between those engaged in dealing with organized crime and those engaged in combating terrorism. In addition to overall strategy, there may now be some legal issues worthy of exploring.

POST-HEARING QUESTIONS FROM SENATOR CLAIRE McCASKILL

QUESTION 1:

The panel discussed how our increasingly interconnected world empowers small groups and continues to shape potential threats, including cyber dangers, terrorism, and transnational crime. On 9/11, there was no Facebook or Twitter, and cell phone use was a fraction of what it is today. Technology changes do not just affect our adversaries; they also affect our vulnerabilities and how we as a nation feel the effects of an attack.

a. In your view, over the next 5-10 years, how will the same technological and societal forces that transform the threats we face also impact the effects of an attack or other incident?

b. What new vulnerabilities are we likely to face as a nation over the next 5-10 years?

c. Do such changing technological and societal forces also present new opportunities for resilience?

RESPONSE 1:

This is a fascinating question worthy of lengthy exposition. For now, I can offer only a few observations based on technology's contribution to terrorism in the past.

Technological developments have benefited both terrorists and governments in ways that were not predicted four decades ago when terrorism in its contemporary form emerged as a new mode of conflict. Small arms and bombs, terrorists' primary weapons, however, have changed little since then. Mumbai, a city of 20 million people, was virtually paralyzed for more than two days by ten terrorists armed with essentially a World War II arsenal. The basic chemistry of explosives remains unchanged. There have been incremental developments in miniaturization, less-detectable compounds, and methods of concealment, but an underwear bomb is hardly high-tech.

Shoulder-fired precision-guided missiles have been a concern since the 1970s. They have been used by terrorists, mostly in conflict zones. They remain a concern, especially with large numbers of such weapons missing from Libya's arsenal and perhaps Syria's in the future.

Terrorist use of chemical, biological, or nuclear weapons was a cause for concern 40 years ago. Terrorists in Japan dispersed crude nerve gas, but that turned out to be a one-off event not yet replicated (although al Qaeda reportedly did contemplate the use of poison gas in some of its attacks). Terrorist plots involving very small quantities of ricin continue to surface. None of these have been carried out. But we have the example of the deaths and significant disruption caused by the dispersal of small quantities of anthrax through the mail in 2001.

The deliberate dispersal of contagious diseases remains a health concern. Genetically engineered super pathogens, invulnerable to any treatment, pose a theoretical longer-term threat.

Terrorists have not gone nuclear, although al Qaeda did attempt to acquire fissile material. While nuclear weapons remain a theoretical terrorist ambition, there is no evidence of any current acquisition effort.

Neither have we seen the deliberate dispersal of large quantities of radioactive material. The currently fashionable scenario of terrorists setting off a high-altitude nuclear blast creating an electromagnetic pulse that knocks out all electronics, pushing the country into a post-Apocalyptic stone age, is, in my view, far-fetched.

Doomsday scenarios of terrorists with weapons of mass destruction have remained the property of novelists and Hollywood scriptwriters. Terrorism has escalated over the past 40 years, but not because of technological developments. What terrorists did on September 11, 2001, they could have done (more easily) in 1971.

Because such events have not occurred is no reason to say that they will not occur some time in the future, but it does suggest that they may be either harder to execute than we imagined or less attractive to terrorists than we think.

Modern society is filled with vulnerabilities. Electrical power grids, waterworks, pipelines, air traffic control systems, emergency communications, vital infrastructure managed through the Internet are all seen to be vulnerable to terrorist attack, although we have very few examples of physical sabotage or destruction via the Internet. Again, these targets may be harder to attack than we imagine or terrorists may be more interested in simply racking up high body counts with bombs in easily accessible public places.

Technological developments also have clearly benefited the government side. Thousands of cameras linked to central monitors, including smart cameras that signal suspicious movement or the absence of movement have facilitated remote surveillance. Tracking technologies have greatly improved. Weapons and explosives can be detected at greater distances. Technology enables facial recognition and the detection of subtle physiological indicators of possible malicious intent.

Technological advances have enabled governments to intercept, collect, collate, and analyze vast quantities of data. Information systems serving commercial needs amass tremendous amounts of personal information. In fact, the technology for almost total social control exists, although its implementation is appropriately resisted to preserve civil liberties.

Terrorists have exploited the Internet for purposes of propaganda, recruiting, instruction, and clandestine communications. They have used the Internet to create online communities of like-minded fanatics and to recruit virtual armies. Thus far, however, they have had difficulty in activating these would-be warriors, most of whom seem content to express their convictions vicariously.

The Internet has made instruction in bomb-building more accessible than going to the library or a bookstore, but terrorists in the pre-Internet 1970s built explosive devices that worked, something today's terrorist distance-learners seem to have great difficulty doing. At the same time, the Internet offers authorities insight and investigative leads and has led to the arrest of terrorist plotters. In sum, the Internet is a wash.

VerDate Nov 24 2008 13:06 Dec 04, 2012 Jkt 76059 PO 00000 Frm 000136 Fmt 06601 Sfmt 06601 P:\DOCS\76059.TXT SAFFAIRS PsN: PAT

76059.052

So who is ahead overall? Technology theoretically has put more destructive power into the hands of smaller and smaller groups, while at the same time theoretically increasing the power of the state to monitor the activities of its citizens. Technology has not given the terrorists a strategic advantage, nor has it enabled states to effectively suppress terrorist adversaries.

The one dimension where terrorists have benefited is that of cost. Terrorists are free riders. They exploit existing technology. Protecting society is more costly. Aviation security provides the most obvious example. Terrorists need only to build one small bomb and recruit one determined bomber, while society has to protect hundreds of commercial airports, thousands of daily flights, millions of passengers. It is an unequal exchange, leading to the conclusion that terrorists can bankrupt governments with the burden of security—but that hasn't happened either.

QUESTION 2:

Generally speaking, how can we create a government that is more flexible, more nimble, and more capable of adapting to the evolving threats you have described? What general qualities should such an organization have?

RESPONSE 2:

When discussing government, adjectives like "flexible," "nimble," and "adaptive" are not the first that come to mind. Governments are large, unwieldy human enterprises that must represent and reconcile diverse views and interests. It is not easy to get things done in government, especially in a society that is inherently skeptical of government institutions.

At the same time, America's record isn't too bad. Our political institutions have repeatedly co-opted the potential constituencies of past terrorist movements, left and right, while suppressing the terrorists themselves. America has successfully assimilated immigrant populations that came with built-in quarrels connected to the old country.

As for institutions, the 9/11 attacks brought about fundamental changes in laws, government organization, and deeply ingrained bureaucratic cultures to produce a remarkably successful, albeit controversial, worldwide and domestic counterterrorist effort. Not surprisingly, it took several years to do this, and the system is still not optimally effective. It must be reconciled with a free and open society—frankly, I have some misgivings here.

In an effort to prevent further terrorist attacks, this nation has created a vast internal security apparatus, unprecedented in our history, and conceded extraordinary authority to the Executive branch of government. In the likely absence of a clear end to this undertaking, these institutions may accumulate even further power. And that is a cause for concern.

QUESTION 3

Even more important than discussing future threats in the context of this hearing is for government agencies to have the capacity and institutional processes to evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?

RESPONSE 3

It is a good question, but I can't offer an informed answer here. I have reviewed NIE products in the past, but I believe that the process has changed. And I was not involved in the QHSR. Reflecting the fact that we are dealing with fast-moving subject matter, the number of reports provided by federal agencies to local law enforcement, generally dealing with near-term assessments and immediate trends, has increased enormously.

Post-Hearing Questions for the Record
Submitted to Frank J. Cilluffo
From Senator Joseph I. Lieberman

"The Future of Homeland Security: Evolving and Emerging Threats"
July 11, 2012

1a. What is your assessment of the internal capabilities within DHS today to assess future threats and then take actions (e.g. with respect to budgeting, operational planning, acquisitions) to address them?

DHS continues to mature over time, but the department's internal capabilities to assess future threats and then take actions are not yet evolved to the level that the security ecosystem demands. These capacities generally still remain reactive in nature. The department must be able to respond to a wide range of threats that may materialize quickly. An Office of Net Assessment (ONA) could and should be created in order to better meet that goal. The duties of ONA would include studying existing threats in order to project their evolution into the future; studying trends in the weapons, technologies, modalities, and targets utilized by our adversaries (i.e., the events that can transform the security landscape); reviewing existing U.S. capabilities in order to identify gaps between current capabilities and the requirements of tomorrow's threats; conducting war games and red team scenarios to introduce innovative thinking on possible future threats; assessing how terrorist groups/cells could operate around, and/or marginalize the effectiveness of, policies and protective measures. Admittedly this is a tall order. The alternative however is to walk into the future partly blind and therefore remain more vulnerable than we need to or should be.

In terms of aligning our actions (budgeting, operational planning, acquisitions) with the future threats that we face, there is still a ways to go. While less than perfect, the Quadrennial Homeland Security Review (QHSR) has served as a useful starting point. However as a mechanism and process for helping to bring DHS resources and plans into sync with the threat environment, the QHSR is not as forward-leaning as it could or should be. The country would be better served by a more robust posture and process—one that anticipates threats before they manifest and that allows the Secretary to determine what tools are needed for meeting them, what force structure is needed (at the federal, state and local levels), and what resources are needed from Congress to make that plan a reality.

1b. In your prepared testimony you mention the idea of creating an Office of Net Assessment within DHS headquarters that would be focused on long-range threat and risk analysis for homeland security. Why do you believe that this function would be valuable for DHS?

From a strategic perspective, it would most helpful for the Secretary of Homeland Security to establish an Office of Net Assessment (ONA) within DHS to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats. The ONA should be an independent office that reports directly to the Secretary of Homeland Security. The ONA would fill the much-needed role of producing long-term assessments and strategy, acting as a brain trust of creativity and imagination, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the United States requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable—in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends.

This proposal is not new. To the contrary, it appeared in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served as Vice Chairman together with Chairman Lee Hamilton. Now is the time—indeed it is well past time—to take this recommendation off the page and enact it. Our adversaries are patient and they are long-term thinkers whose horizons extend well beyond weeks and months. To help counter them effectively, we must not lose sight of the long game either.

2. Last year al-Qaeda released a video calling for cyber jihad and the destruction of our infrastructure through cyber attacks. And as recently as April of this year, the head of intelligence at US Cyber Command, Rear Admiral Cox stated publically that al-Qaeda operatives are seeking the capability to stage cyber attacks against U.S. networks.

What is your current assessment of the potential threat of cyber attacks from al Qaeda, its affiliates, and other terrorist groups, both in terms of intent and capability?

The cyber threat is multifaceted and may emanate from individual hackers, hacktivists, criminal or terrorist groups, nation-states or those that they sponsor. The threat spectrum is multifaceted, and affects the public and private sectors, the interface and intersections between them, as well as individual citizens. By and large, from a homeland security perspective, at least in terms of sophistication, foreign states are our principal concerns—specifically those that pose an advanced and persistent threat, namely Russia and China. Their tactics may also be exploited by others.

Although I have said this to you and your predecessor Committee (on Government Reform) before—in fact, less than a month after 9/11: "Bits, bytes, bugs, and gas will never replace bullets and bombs as the terrorist weapon of choice. Al Qaeda in particular chooses vulnerable targets and varies its modus operandi accordingly. They become more lethal and innovative with every attack—the first attempt on the World Trade Center, the

Khobar Tower, the U.S. embassies in Africa, the USS Cole. In light of this demonstrated escalation and flexibility, we must shore up our vulnerabilities, and cyber threats are a gaping hole. While bin Laden may have his finger on the trigger, his grandson may have his finger on the mouse. Moreover, cyber attacks need not originate directly from al Qaeda, but from those with sympathetic views."[1]

Further, as I stated in testimony before you and this Committee in 2007: "Extremists value the Internet so highly that some have adopted the slogan 'keyboard equals Kalashnikov'. Terrorist groups now have their own media production arms (al Qaeda relies on As-Sahab and the Global Islamic Media Front, for example). Terrorists produce their own television programs and stations, websites, chat rooms, online forums, video games, videos, songs, and radio broadcasts."[2]

While I think both assessments are still relevant, there are some nuances that warrant additional concern. As U.S. and allied counterterrorism efforts continue to yield success in the physical world, this may lead al Qaeda and its sympathizers to enter ever more deeply into the cyber domain. Al Qaeda and their jihadi ilk may also be surfing in the wake of Anonymous and other such groups, in order to learn from the latter's actions. Finally, as laid out in my testimony to the Committee last month (as well as in previous testimonies), the government of Iran and its terrorist proxies are serious concerns in the cyber context.

3. How is state and local role in homeland security likely to need to change in response to the future homeland security threat landscape that you and other witnesses discuss in your testimony? How can organizations such as state and local fusion centers be leveraged more effectively to address such growing and evolving threats?

In terms of intelligence, state and local authorities can and should complement what the federal government does not have the capacity or resources to collect (or is simply not best suited to do), and thereby help determine the scope and contours of threat domains in the United States. Further leveraging our decentralized law enforcement infrastructure could also serve to better power our Fusion Centers. Opportunities still exist to tap and apply intelligence and information from the field of organized crime to the field of counterterrorism, and vice versa. Hybrid thinking that marries up the two fields in this way, in order to further build our reservoir of knowledge on the CT side could prove valuable.

To obtain a truly "rich picture" of the threat in this country, we must focus on the field—not the Beltway. As history shows, the intelligence community has come to just such a field bias. For the counterterrorism community to do otherwise is to risk stifling and stymieing the good work being done where the rubber meets the road. Fusion Centers should be given ample opportunity to flourish. The equivalent of Commanders' Intent,

---

[1] "Critical Infrastructure Protection: Who's In Charge" (October 4 2001). http://www.gwumc.edu/hspi/policy/testimony10.4.01_cilluffo.pdf

[2] "The Internet: A Portal to Violent Islamist Extremism" (May 3 2007). http://www.gwumc.edu/hspi/policy/testimony5.3.07_cilluffo.pdf

which gives those in the field the leeway to do what they need to do and which incorporates an honest "hotwash" after the fact to determine what went wrong and how to fix that, is needed in present civilian context for counterterrorism and intelligence purposes.

Simple yet powerful steps remain to be taken. This was revealed starkly in multiple rounds of survey work (first with the major metropolitan intelligence chiefs and later with the fusion centers) that HSPI recently completed in an attempt to bring a little science to the art of intelligence. For example, too few Fusion Centers currently do threat assessments. This is unacceptable, especially in a climate of limited resources in which allocation decisions (regarding human, capital, and financial resources) should be priority-ordered, meaning that scarce resources should be directed to those counter-threat measures, gaps and shortfalls that constitute areas of greatest need. And Fusion Center-specific threat assessments are just a start. Regional threat assessments are also needed. Our adversaries do not respect local, State, or even national boundaries hence our response posture must be similarly nimble and cohesive. Yet according to HSPI survey research published last month, only 29% of Fusion Center respondents reported that their Center conducted a regional threat assessment on at least a yearly basis. Almost half reported that their Centers simply did not conduct regional threat assessments.

Those working in the Fusion Centers have yet to be invested with the analytical skill-craft and training necessary for them to accomplish their mission. Current incentive structures place too much emphasis on information processing and not enough on analytical outcome. Greater resources should be allocated to the professional development of those working in the Centers. Within them lies untapped collection and analysis potential. Realizing and unleashing that potential will further bolster state and local law enforcement efforts, and help develop anticipatory intelligence to prevent terrorist attacks and the proliferation of criminal enterprise operations.[3]

---

[3] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires "Counterterrorism Intelligence: Fusion Center Perspectives" HSPI Counterterrorism Intelligence Survey Research (CTISR) (June 2012). http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf. See also Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing "Counterterrorism Intelligence: Law Enforcement Perspectives" CTISR (September 2011). http://www.gwumc.edu/hspi/policy/HSPI%20Research%20Brief%20-%20Counterterrorism%20Intelligence.pdf

Post-Hearing Questions for the Record
Submitted to Frank J. Cilluffo
From Senator Claire McCaskill

"The Future of Homeland Security: Evolving and Emerging Threats"
July 11, 2012

1. **The panel discussed how our increasingly interconnected world empowers small groups and continues to shape potential threats, including cyber dangers, terrorism, and transnational crime. On 9/11, there was no Facebook or Twitter, and cell phone use was a fraction of what it is today. Technology changes do not just affect our adversaries; they also affect our vulnerabilities and how we as a nation feel the effects of an attack.**

    a. **In your view, over the next 5-10 years, how will the same technological and societal forces that transform the threats we face also impact the effects of an attack or other incident?**

    b. **What new vulnerabilities are we likely to face as a nation over the next 5-10 years?**

    c. **Do such changing technological and societal forces also present new opportunities for resilience?**

The cyber threat (and supporting technology) has markedly outpaced our prevention and response efforts. Use of cyber means as a force multiplier for kinetic activities, which would represent the convergence of the physical and cyber worlds, constitutes probably the area of greatest concern over the next 5 to 10 years. Although much work remains to be done on the counterterrorism side, the country has achieved significant progress in this area. In contrast, the U.S. cybersecurity community's state of development is akin to that of the counterterrorism community as it stood shortly after 9/11. Despite multiple incidents that could have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed, and not just within Government, we have yet to take those necessary steps. Foreign intelligence services are engaging in cyber espionage against us, often combining technical and human intelligence in their exploits. Everything from critical infrastructure to intellectual property is potentially at risk. These exploits permit others to leapfrog many bounds beyond their rightful place in the innovation cycle, by profiting from (theft of) the research and development in which private and public U.S. entities invested heavily. At worst, these exploits hold the potential to bring this country and its means of national defense and national security to a halt, and thereby undermine the trust and confidence of the American people in their Government. What purpose could the mapping of critical U.S. infrastructure by our adversaries serve other than what is known in military terms as intelligence preparation of the battlefield? To my mind, the line between this type of reconnaissance and an act of aggression is very thin, turning only on the matter of intent. Officials in the homeland security community should therefore undertake contingency planning that incorporates attacks on U.S. infrastructure. At

minimum, "red-teaming" and additional threat assessments are needed. The latter should include modalities of attack and potential consequences. The United States should also develop and clearly articulate a cyber-deterrence strategy.

New opportunities for resilience, generated by forces including changing technologies, will assuredly present themselves. Indeed it is this ability to reconstitute, recover, and get back on our feet is in fact perhaps the best deterrent. The storms that recently battered the National Capital Region, leaving close to a million people without power during a week-long heat wave, are instructive in terms of our shortcomings on resilience. Mother Nature may be a formidable adversary, but just imagine the level of damage and destruction that a determined and creative enemy could have wrought. There is no lack of trying, as a recently published DHS report makes clear, noting the spike in attacks (from 9 incidents to 198) against U.S. critical infrastructure from 2009 to 2011.[1] The good news, on the other hand, is that the most serious of these incidents could have been avoided through the adoption of basic security steps and best practices. The bad news, of course, is that these fundamental measures were not yet put into place. Plainly we have not yet made the requisite business case for doing so—which is a fundamental problem, given that the majority of critical infrastructure in this country is owned and operated by the private sector. The urgency for making this case needs no further explanation, but we must take care to strike just the right balance of carrots and sticks and of course measures that ensure both privacy and security.

2. Generally speaking, how can we create a government that is more flexible, more nimble, and more capable of adapting to the evolving threats you have described? What general qualities should such an organization have?

The general qualities needed mirror many of the traits that our adversaries have exhibited over time. They are proactive, innovative, well-networked, flexible, patient, young and enthusiastic, technologically savvy, and learn and adapt continuously based upon both successful and failed operations around the globe. We and our government must be and do likewise. Our institutions must be calibrated and responsive to reflect the changing threat environment. This entails much more than rearranging boxes on an organization chart. The type of nimble organization needed must be supported and reinforced by more than just policy and technology—people are a crucial component of the equation. In other words, cultural change is needed in order to generate organizational change, and cultural change takes time, leadership, and both individual and community commitment.

Cyber threats in particular manifest in nanoseconds, and we need to be able to enact cyber response measures that are almost as quick. This means developing and implementing an "active defense" capability to immediately attribute and counter attacks and future threats in real-time.

---

[1] Suzanne Kelly "Homeland security cites sharp rise in cyber attacks" CNN.com (July 4, 2012). http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/

3. **Even more important than discussing future threats in the context of this hearing is for government agencies to have the capacity and institutional processes to evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?**

We are certainly better off having the current processes to produce the QHSR and NIE than we would be in the absence of such evaluation and planning mechanisms. However we do not yet have a true "rich picture" of the domestic threat landscape because the NIE does not fully elaborate upon that dimension. This ought to be remedied so as to create a fulsome awareness of domestic threats, and this remediation exercise should be placed in the hands of state and local officials who are best placed to undertake the task.

From a strategic perspective, it would also be most helpful for the Secretary of Homeland Security to establish an Office of Net Assessment (ONA) within DHS to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats. The ONA should be an independent office that reports directly to the Secretary of Homeland Security. The ONA would fill the much-needed role of producing long-term assessments and strategy, acting as a brain trust of creativity and imagination, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the United States requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable—in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends.

This proposal is not new. To the contrary, it appeared in the January 2007 Homeland Security Advisory Council Report of the Future of Terrorism Task Force, for which I served as Vice Chairman together with Chairman Lee Hamilton. Now is the time—indeed it is well past time—to take this recommendation off the page and enact it. Our adversaries are patient and they are long-term thinkers whose horizons extend well beyond weeks and months. To help counter them effectively, we must not lose sight of the long game either.

Post-Hearing Questions for the Record
Submitted to Dr. Stephen E. Flynn
From Senator Joseph I. Lieberman

"The Future of Homeland Security: Evolving and Emerging Threats"
July 11, 2012

1. In a recent news article, former CIA Director Jim Woolsey compared the recent power outages in the Washington, DC region to the potential impact of a deliberate cyber attack on our electric grid. He noted that "the right hacker could take the (electrical) grid, or portions of it, down for much longer than that....What we don't have is a decision-making structure or anybody in charge of the grid."

This statement relates to an issue that you discuss in your testimony, with respect to the resilience of our critical infrastructure. To the extent that key parts of our infrastructure are vulnerable to natural hazards, such as the *derecho* that hit the DC region, they are also increasingly vulnerable to deliberate attacks, whose effects could ultimately be much more severe than natural hazards.

What are the implications of this, both in terms of how we should be investing generally with respect to upgrading our critical infrastructure, as well as with respect to our investments in cybersecurity?

In general, as our critical infrastructure becomes more fragile as a result of age, deferred maintenance, and constant use, it becomes more vulnerable to disruption from natural hazards and man-made attacks. For too long Americans have been taking the critical foundations of our society for granted. We are like a generation who has been bequeathed a mansion, but have been unwilling to take on the responsibility of upkeep. The result is to place at risk our national competitiveness, our national security, and our quality of life. Accordingly, it is imperative that we reinvest in infrastructure and concurrently "bake-in" the safeguards that will mitigate the risk of cyber-attacks and other hazards. This require identifying standards that improve infrastrucute resilience and making sure that there are appropriate incentives in place for these standards to be widely adopted.

Jim Woolsey is right to single out the vulnerability of our power grid to cyber attack, but that vulnerability also extends to U.S. critical infrastructure more generally. Over the past decade, more and more Internet Protocol (IP) devices have been replacing proprietary hardware, software, and communications protocols for the nation's physical infrastructure. This translates to industrial control systems (ICS) for the electrical power grid; water and waste management systems; oil pipelines, refineries, and power-generation plants; and transportation systems ranging from mass-transit to maritime port operations, becoming increasingly accessible to the Internet. An attack on these systems by a state or non-state actor, not only places at risk the continuity of service or

the compromise of databases, but the potential for catastrophic loss of life and destruction of property. This is because hackers are not only able to infiltrate systems, but they are increasingly in a position to actually take control of such systems – turning off alarms or sending bad data to create a threat. Unfortunately, bad actors need not be terribly sophisticated in order to accomplish substantial harm. Because of the interconnectivity of our networks, successful disabling of just one critical system can generate cascading consequences across multiple systems.

The U.S. power grid is particularly vulnerable to the risk of cyber attacks and given the reliance on power by all other sectors, it deserves special and urgent attention. As with other large and disbursed infrastructures that make up America's critical industrial landscape, managing the electric grid depends on the operation of supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). SCADA systems make it possible to control geographically dispersed assets remotely by acquiring status data and monitoring alarms. Based on the information received from the remote station control devices, automatic or operator-driven supervisory commands can be provided from a centralized location. These field devices can perform such functions as opening and closing breakers and operating the speed of motors based on the data received from sensor systems. Distributed control systems (DCS) are typically facility-centric and used to control localized industrial processes such as the flow of steam into turbines to support generation of power in an electric plant. DCS and SCADA systems are networked together so that the operation of a power generation facility can be well coordinated with the demand for transmission and distribution.

When most industrial control systems (ICS) were originally installed to help operate components of the power grid, they relied on logic functions that were executed by electrical hardware such as relays, switches, and mechanical timers. Security generally involved physically protecting access to the consoles that controlled the system. But, over time, microprocessors, personal computers, and networking technologies were incorporated into ICS designs. Then in the late 1990's, more and more Internet Protocol (IP) devices were embraced so as to allow managers to gain better access to real-time data on their systems on their corporate networks. These networks are, in turn, often connected to the Internet. The inevitable result of this increased reliance on standard computers and operating systems is to make ICS more vulnerable to computer hackers.

Tampering with DCS and SCADA systems can have serious personal safety consequences since industrial control systems directly control assets in the physical world. According to a June 2011 report by the National Institute of Standards and Technology (NIST), cyber security breeches of industrial control systems could include unauthorized changes to the instructions, commands, or alarm thresholds that result in disabling, damaging, or shutting down key components. Alternatively, false information about the status of systems can be sent that cause human operators to make adjustments or to take emergency actions that inadvertently cause harm. If a cyber attack leads to a power-generating unit being taken offline because of the loss of monitoring and control capabilities, it could result in a loss of power to a transmission substation, triggering failures across the power grid if other substations are not able to carry the added load. The resultant blackouts would affect oil and natural gas production, water treatment

facilities, wastewater collection systems, refinery operations, and pipeline transport systems.

One implication of this is the need for a coordinated R&D strategy that advances the nation's capacity to anticipate threats, map out the associated risks, and devise appropriate responses. A November 2010 JASON Report, Science of Cyber-security, commissioned by the Department of Defense outlines the need to establish cyber security science based centers within universities and other research institutions. Federally funded centers would provide sponsors with access to the innovative ideas by leading academic experts while concurrently facilitating exposure by researchers to agency experience and expertise in managing government cyber networks. Research can support the development of automated approaches to detect and mitigate attacks. Additionally, because security is not only a technical problem, more work needs to be done to understand the human and social aspect contributing to vulnerabilities.

Because information and communications networks are largely owned and operated by the private sector, such centers would bring together industry and academic partners to test data and transition new ideas into the rapid adoption of research and technology development innovations. Regional university-based centers, for example, could develop strategies to improve the security and resilience of information infrastructure and reduce the vulnerability and mitigating the consequences of cyber attacks on critical infrastructure.

Advances in networking and information technology are a key driver of economic competitiveness and are crucial to achieving our major national and global priorities in energy and transportation, education and life-long learning, healthcare, and national and homeland security, including resilience to cyber warfare. They also accelerate the pace of discovery in nearly all other fields. Investing in regional university based cybersecurity centers must be a key component of any cybersecurity strategy for the nation.

VerDate Nov 24 2008 13:06 Dec 04, 2012 Jkt 76059 PO 00000 Frm 000148 Fmt 06601 Sfmt 06601 P:\DOCS\76059.TXT SAFFAIRS PsN: PAT

76059.121

2. On April 26, 2012, the Homeland Security and Governmental Affairs Committee held a hearing to discuss the recent decision to publish the results of two studies showing the ability for H5N1 influenza to mutate and become transmissible between humans. The hearing also discussed new government policy regarding the oversight of dual-use research of concern. Such research has great benefits to the scientific and health communities allowing for surveillance and the development of new countermeasures for example. However, this research also comes with risk of being misused or misapplied and could cause us harm.

What is your assessment of the potential threats and risks posed by this type of research in the future, and what policies do we need with respect to this type of research?

As I general rule, when it comes to homeland security risks, my preference is to err on the side of openness, rather than secrecy. The best tools and safeguards for confronting risks are going to come from researchers and the private sector and they cannot be effectively engaged if they are left in the dark. At the same time, unlimited distribution of detailed technical information that can misused or misapplied is foolhardy. Research communities should put in place a vetting process before this kind of information is shared. In the case of particularly sensitive information, a prospective researcher should be required to provide references before being given permission to access that information.

Responses to Post-Hearing Questions for the Record
Submitted to Dr. Stephen E. Flynn
From Senator Claire McCaskill

"The Future of Homeland Security: Evolving and Emerging Threats"
July 11, 2012

1. The panel discussed how our increasingly interconnected world empowers small groups and continues to shape potential threats, including cyber dangers, terrorism, and transnational crime. On 9/11, there was no Facebook or Twitter, and cell phone use was a fraction of what it is today. Technology changes do not just affect our adversaries; they also affect our vulnerabilities and how we as a nation feel the effects of an attack.

    a. In your view, over the next 5-10 years, how will the same technological and societal forces that transform the threats we face also impact the effects of an attack or other incident?

Attacks by state and non-state actors are going to be easier to conduct—especially in the cyber realm—more difficult to detect and intercept, and more ambiguous as to its source, making it easier for an adversary to have reasonable deniability. There is also the risk that more sophisticated attacks will generate greater cascading consequences given the interconnectedness and interdependencies of critical infrastructure. The bottom-line, is that there will be increasing limits on what can be done to prevent these kinds of attacks, so we need to invest more time, energy, and resources identifying how to mitigate the consequence and rapidly restore critical systems should they be compromised. This should not be seen as act of resignation, but instead as a way to provide deterrence. An attack is far less attractive to our current or future adversaries if they are likely to be inconsequential; i.e., there is no "big bang" for their buck.

    b. What new vulnerabilities are we likely to face as a nation over the next 5-10 years?

While there is no crystal ball that can forecast with precision where future attacks are likely to come, as a general proposition, our current and future adversaries will be drawn to targeting critical infrastructure that holds out the risk of generating the most economic disruption and destruction. Unfortunately, given the tepid investment we have been making in recent year in the upkeep of the physical infrastructure that serve as the critical foundations for our economy and quality of life, that infrastructure will only become all the more attractive to target. To the extent that the electrical power grid; water and waste management systems; oil pipelines, refineries, and power-generation plants; and transportation systems ranging from mass-transit to maritime port operations, becoming increasingly accessible to the Internet, the greatest risk is likely to be from cyber threats.

c. Do such changing technological and societal forces also present new opportunities for resilience?

These changing forces provide opportunities as well as challenges. The key is harnessing the enormous capabilities we possess within our universities and research institutions, the private sector, and civil society more generally. Building resilience requires an open, inclusive, bottom-up process. Social media can be harnessed to support this, as well as investing in an R&D strategy that challenges the best minds and companies to identify ways to back safeguards and resilience into the old and new infrastructure, systems, and networks.

2. Generally speaking, how can we create a government that is more flexible, more nimble, and more capable of adapting to the evolving threats you have described? What general qualities should such an organization have?

We need to fundamentally recalibrate our post-9/11 approach to homeland security. As Alexis de Tocqueville observed in the first half of the 19th century, one of America's most distinctive qualities is its tradition of self-reliance and volunteerism. Clearly those attributes have atrophied in recent years in no small part because much of the responsibility for safety and security has been taken over by professionals with less emphasis on the role of the average citizen. The national security apparatus constructed to deal with the Soviet threat during the Cold War was built around career soldiers and intelligence officials who inhabited a world largely cordoned off from the general public by the imperative of secrecy. At the same time, cities and suburbs are increasingly reliant on full-time emergency responders and sizeable police forces. This has led many people to see public safety as an entitlement instead of as a shared civic obligation. A renewed national emphasis on building individual, community and infrastructure resilience would not only help to be better prepared for 21st Century hazards, but at the same time, it would strengthen our increasingly frayed social fabric since it requires everyone to play a role, not just the professionals.

3. Even more important than discussing future threats in the context of this hearing is for government agencies to have the capacity and institutional processes to evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?

Too little investment has been made in the QHSR process to make it meaningful. Given that the homeland security mission requires the role of multiple federal agencies (DOJ, FBI, HHS, U.S. NORTHCOM, etc.), it should be actively managed out of the White House. When it comes to critical infrastructure protection, I am concerned that there is inadequate expertise within our intelligence community on how those infrastructures are designed and operate to produce adequate threat assessments.

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph I. Lieberman
Homeland Security and Governmental Affairs Committee
"The Future of Homeland Security:
The Evolution of the Homeland Security Department's Roles and Missions"
Washington, DC
July 12, 2012

Good morning, this is the second in a series of hearings the Committee is holding on the past, present, and future of homeland security in our country, coincident with the 10th anniversary of the adoption of the Homeland Security Act in November of 2002 - obviously after 9/11. As I end my service in the Senate I wanted to take a look at homeland security over the past 10 years, but really more importantly, to look forward, discuss the unfinished business, and to anticipate how we can meet evolving threats. I hope thereby to create a record which will be of help to this committee and its new leadership next year.

We had a very good hearing yesterday with a panel that described the evolving homeland security threat. Today we're going to focus on the department itself, how it's done over the almost 10 years now, and what it should be doing in the years ahead.

The Department of Homeland Security doesn't include all of the federal government's majority homeland security agencies. The Departments of State, Defense, Justice, and Health and Human Services, along with key intelligence agencies of our government, all play very important roles in protecting our homeland security.

Our state and local partners, as well as the private sector, and as we discussed yesterday, the American people themselves, all have significant responsibilities.

But really, the center of homeland security was intended to be the Department of Homeland Security. It was intended to be not only the center point, but the coordinating point of the agencies that were brought within it and also to make sure that we were interacting with a lot of other agencies of the federal state and local governments that had both responsibility and some opportunity to contribute to our homeland defense.

As I look back, I would say the Department has come an awful long way in its first decade, but this is a mission that has no final destination point. It has to continue getting better, and there are ways to meet the evolving threat. There are ways in the first decade, there were some things that happened that were not as good as we wanted. But as I go back to 10 years ago, I think the vision that Congress had for the Department of Homeland Security when we created it was to have a department that would be more than the sum of its parts. A department that would integrate key homeland security functions such as border preparedness and infrastructure protection in a department that would help ensure, as we said over and over again after 9/11, that we would never again fail to connect the dots so that we would prevent the next 9/11 from happening.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

As I've said, I think the that the Department has made tremendous strides forward in the nearly ten years since the passage of the Homeland Security Act in achieving some of these broad goals we've talked about and that we had in mind 10 years ago.

Al Qaeda, which we were focused on of course because it claimed credit for 9/11, the attacks against America, and its affiliates have not carried out a successful attack, certainly not one anywhere near the catastrophic dimensions of 9/11, since 9/11 which I think is a credit not only to our offensive forces let by the U.S. military and intelligence communities, but also to the tremendous work the homeland security department has done.

Let me talk about the areas where I think there has been significant progress. We've got a screening system now at points of entry into the U.S. that is integrated with information from the intelligence community and others, and has become very effective at detecting bad actors trying to enter the country.

Our aviation screening system is vastly improved from what we had before 9/11. We now have more robust two-way information sharing on potential threats, not only within the federal government, but with state and local governments, and that's in large measure due to the leadership of DHS and its support for state and local fusion centers. In a different aspect of the DHS responsibilities, our nation's preparedness and response efforts, led by FEMA, have improved significantly in the seven years since Hurricane Katrina, which obviously showed how inadequate FEMA was at that point. Their response to just about every natural disaster that has occurred in our country since then has been significantly better and drawn very positive reviews.

These are important achievements. We shouldn't forget them in the occasional griping from people who don't like to take their shoes off or go through magnetometers or whatever else at airports. But the Department still has a way to go to fully realize what we want it to be.

Let me just mention a few of the areas where I think there is much more to be done. Interestingly, most of these have to do with the administration of the Department, with process if you will. But process is important.

For example, the Department's operational components are still not adequately integrated with its headquarters and with each other, and that causes problems. It causes at least less than optimal use of the Department's resources.

The Department of Homeland Security continues to have workforce morale challenges, as reflected in the annual ratings done in the federal human capital survey. These have improved over the years, but nowhere to the extent needed. The Department of Homeland Security also struggles with setting requirements and effectively carrying them out for major acquisitions and ensuring that these acquisition programs stay on track while they are underway. The Department of Homeland Security is, unfortunately, not unique among federal agencies in this problem, but this is the Department that we helped create and we have oversight responsibility for it. I'll be honest and say their performance in this regard has not been adequate.

In the years ahead, the Department, in a different way, will need to take actions to anticipate and respond to evolving homeland security threats, including continuing to increase its capabilities with respect to cybersecurity in response to cyber attacks on our country.

The greater challenge, of course, is that the Department of Homeland Security, along with every other federal agency, will have to find a way to do this in a period of flat or perhaps, declining budgets. In a budget environment like the one that we are in today, the natural tendency is to focus on preserving and protecting current capabilities. But the risk of doing only that is that we will be under-investing in systems needed to meet evolving and new threats of tomorrow.

I think in a second decade, the Department of Homeland Security will have to be as agile as our enemies. That may mean the Department will have to cut back in some of its now traditional areas of responsibility if they seem less relevant to the threat and take that money and invest it in programs to meet new threats that come along.

The three witnesses that we have, Congresswoman Harman, Admiral Allen and Mr. Skinner are really uniquely prepared by experience and capability to contribute to our discussion and build exactly the type of record I hope this committee will build to hand over to the leadership in the next session. I cannot thank you enough for being with us this morning and I look forward to your testimony.

Opening Statement of
Ranking Member Senator Susan M. Collins
"The Future of Homeland Security:
The Evolution of the Homeland Security Department's Roles and Mission"
Committee on Homeland Security and Governmental Affairs
July 12, 2012

Nearly 10 years ago, the creation of the Department of Homeland Security brought together 22 different agencies into a single Department to focus on protecting our country and its citizens.

Yesterday, we explored the emerging security threats our nation is likely to confront. Today, we will examine whether DHS is well-positioned to address these as well as other, longer-standing threats.

The changing threat landscape at home and abroad requires the Department to be nimble and imaginative, effective and efficient, qualities not often associated with large bureaucracies. Yet the men and women of DHS can take pride in the absence of a successful large-scale attack on our country during the past decade and in the Department's contributions to thwarting numerous terrorist plots.

There have been successes and failures over the last 10 years. Information sharing has improved, but remains a work in progress. Ten years ago, we envisioned that DHS would be a clearinghouse for intelligence. Although incidents like the failed Christmas Day "underwear bomber" make clear that information sharing is still imperfect, numerous public and classified counterterrorism successes since 9/11 demonstrate that information sharing has indeed improved.

This is also true with respect to information sharing between DHS and the private sector - an essential partner in the protection of the homeland, as 85 percent of our critical infrastructure is privately owned.

The growing network of state and local fusion centers also presents opportunities not only for the improved dissemination of information, but also for the collection and analysis of intelligence from the local level. As we discussed yesterday, however, these centers have yet to achieve their full value in aggregating and analyzing local threat information.

TSA, the agency within DHS that is most familiar to the public, has strengthened airline passenger risk analysis, but it troubles many Americans to see TSA screeners putting the very young and the very elderly through intrusive, and in most cases unnecessary, pat downs. TSA is making progress toward implementing more intelligence focused, risk-based screening through such efforts as Pre-Check, but many challenges remain for TSA.

DHS has bolstered the security of our borders and identification documents, but two Iraqi refugees associated with al Qaeda in Iraq were arrested in Kentucky last year. When a bomb

maker, whose fingerprints we had had for some time, is able to enter our country on humanitarian grounds, it is an understatement to say that "work remains" -- as DHS's self assessment report states.

In order to meet and overcome current and future threats, DHS must support its components with stronger management. Since 2003, GAO has designated the Department as "high risk" because of the management and integration challenges inherent with such a large undertaking. DHS must implement changes that will hasten the day when the Department is no longer included on GAO's high-risk list.

The roles of the Department's components have evolved over time. As a positive example, I would note the adaptability and "can do" attitude of the Coast Guard. I don't believe there is another agency within the Department that has done a better job of adapting to new challenges and its expanding post 9-11 mission. This was never more clear then after Hurricane Katrina. As this Committee noted in its report on Katrina, the Coast Guard demonstrated strength, flexibility, and dedication to the mission it was asked to perform, and saved more than half of the 60,000 survivors stranded by the storm.

Many experts have predicted a disaster in the cyber realm that would compare to Katrina or Pearl Harbor. Compared to 10 years ago, the cyber threat has grown exponentially. Clearly, this requires an evolution of the Department's mission to secure critical systems controlling critical infrastructure, a goal we hope to accomplish through the legislation Chairman Lieberman and I have championed.

Despite the fact that DHS has made considerable strides over the past decade, it still has a long way to go. To understand what changes are needed for the future, and to prioritize our limited resources, we must learn from past mistakes and be able to better measure what has worked and what has not. To do so requires metrics and accountability, an area where the Department has been challenged.

I appreciate the outstanding experts who are here today to assist us in evaluating the Department's progress and future.

U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING: "The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"

WASHINGTON – *Today, Sen. Tom Carper (D-Del.) participated in the Homeland Security and Governmental Affairs Committee hearing, "The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions." A copy of his opening statement, as prepared for delivery, is below.*

"Today's security threats are very different than those we faced when the Department of Homeland Security (DHS) was first created. In fact, they continuously evolve. Many terrorist groups, for instance, have changed their strategy over the years, relying more on small-scale attacks, which are often harder to detect. Across our southern border, ruthless drug cartels have become extremely powerful, creating an incredibly dangerous environment for our border security personnel. And, in cyberspace, we are trying to protect our critical infrastructure, government information systems, and business secrets from the daily attacks from hackers and even other nations.

"To respond to these types of dynamic and ever-changing threats, we must take bold action and be ready to adapt when necessary. However, we cannot just throw money at questionable solutions for every new threat that emerges. We can't just create a new office at DHS or pile on a new responsibility for the department whenever we hear about a new threat. Rather, we must be smart with our limited resources and ensure that we're flexible and have strong plans and a strong workforce in place. We also need to make sure that we're measuring the effectiveness of the initiatives we put into place to protect the American people. If a program is not working, we shouldn't just keep throwing good money after bad. We should be willing and able to reassess what's been done and focus our scarce resources on what works.

"As DHS and other federal agencies evolve to address the new security challenges that lie ahead, I will be looking to ensure that our government is making smarter acquisition decisions – decisions that are cost-effective, based on risk, and validated by intelligence and sound science. Moreover, I will keep pushing DHS, the Department of Defense, and other federal agencies to be better stewards of the taxpayer dollars we entrust them with by improving their financial management practices and systems.

"I will also continue to work with my colleagues on both sides of the aisle to pass comprehensive cyber security legislation so that our federal agencies have the tools and resources they need to protect our most sensitive information against new cyber threats that, in many ways, didn't exist in 2001.

"While we have made important strides in improving our security efforts, we know our enemies are always evolving and becoming more sophisticated every day. That is why it is so important that we work even smarter with our limited resources and find ways to get even better results for the money we invest in homeland security. I look forward to hearing from all our witnesses about the future of our homeland security and how we can work smarter as we evolve to meet new threats."

THE HONORABLE JANE HARMAN
TESTIMONY
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITTEE
JULY 12, 2012

Thank you, Senator Lieberman and Senator Collins, for the opportunity to join dear friends and to return to Capitol Hill to testify on a topic I'm passionate about: the security of our homeland.

Our collaboration over many years shows that bipartisanship – indeed tripartisanship – is possible. We had a good gig going and our legislative efforts yielded significant results – and many special times.

As you know, I joined the hardy little band of legislators who thought a homeland security function made sense in the aftermath of 9/11 – something far less ambitious than the plan ultimately sketched out by then White House chief of staff Andy Card.

We envisioned a cross-agency "jointness" similar to the 2004 Intelligence Reform Act structure, which the three of us, and former Rep. Pete Hoekstra, negotiated.

But I clearly recall our decision to embrace a much bigger concept – which the White House proposed – because that would ensure Presidential support.

Though DHS comprised of 22 departments and agencies, Congress legislated four main directorates: Border & Transportation Security, Emergency Preparedness, Science & Technology and Information Analysis & Infrastructure Protection.

The Information Analysis Directorate was supposed to analyze intelligence and information from other agencies (including the CIA, FBI, DIA and NSA) involving threats to the homeland and evaluate vulnerabilities in the nation's infrastructure. Emergency Preparedness would oversee domestic disaster response and training. Border security would streamline all port-of-entry operations and the S&T Directorate would acquire scientific and technological tools to secure the homeland.

The initial strategy has clearly morphed into something different. Merging government functions is difficult, and the threats against us have not been static. DHS has evolved … but so have our enemies.

While DHS has experienced real success, there have also been some hiccups and significant growing pains along the way. It's certainly not the first Department to run into a few problems. To remind: the Department of Defense faced so much inter-service rivalry nearly four decades after its creation that it needed major legislative reform to rework the command structure.

My bottom line is we don't need to rearrange the deck chairs, again. We do need a clear-eyed assessment of what works and what doesn't.

There are homeland functions that execute well:

- Last year, Customs & Border Protection (CBP) stopped more than 3,100 individuals from boarding U.S.-bound aircraft at foreign airports for national security reasons. And CBP was able to process more than 15 million travelers at 15 pre-clearance locations in the same year. That's like picking needles from a haystack!

- The Transportation Security Administration (TSA) now fully implements "Secure Flight," the program screening all passengers on flights from, within, or bound for the US against government terror watch lists. Extending our "borders" by using real-time, threat-based intelligence in addition to multiple layers of security is working to mitigate terror threats.

- The Department expanded the "If You See Something, Say Something" campaign to dozens of states, cities, transit systems, fusion centers, federal buildings, shopping malls, sports arenas, and retail outlets to boost public awareness and reporting of potential threats. Local residents are the first line of defense against terror plots in this country, because they know what is suspicious.

- That's why fusion centers are so important. Last year, the Colorado Fusion center helped identify an attempted bombing suspect. And fusion centers around the country worked together to share tips and leads necessary to arrest and convict Faisal Shahzad, the 2010 Times Square bomber.

- Finally, the Office of Infrastructure Protection conducted more than 1,900 security surveys and 2,500 vulnerability assessments on the nation's most significant critical infrastructure to identify potential gaps and provide recommendations to mitigate vulnerabilities.

But … the homeland security challenges are significant:

First, the Intel function has never fully developed. Part of the reason is that President Bush stood up the Terrorist Threat Integration Center – now the National Counterterrorism Center – that put the mission of fusing intelligence outside of the Department.

Intelligence reports are meant to be consumed by state and local law enforcement, but many of those entities consider DHS reports as "spam," cluttering overflowing inboxes. In many cases, law enforcement still reports that state fusion centers provide better, more timely information than DHS can.

In the new DHS Strategic Plan for FY12-16, intelligence is recognized as an area needing "enhancement." Reinventing the wheel by establishing new "Department Intelligence priorities, policies, processes, standards, guidelines, and procedures" seems to miss the point. Good information is flowing into the components daily – from ports of entry to Suspicious Activity Reports. Can this information be packaged in a way that is helpful for state and local law enforcement?

As you know, this was the point of standing up the Interagency Threat Assessment and Coordination Group (ITACG) at NCTC – to have local law enforcement help shape intelligence products so they are useful. It also creates "ambassadors" at the local level. So I applaud the Chairman's efforts to reverse the funding cuts to ITACG that are in the appropriations bills.

Second, the homeland mission is so large that the Department must assess where it can be most effective and where it can't. For example, DHS will never be the leader in preventing cyber attacks. But the Department can help critical infrastructure owners and operators make their facilities as hardened as possible against attacks. It can also serve as a clearinghouse for reports from the public about "Phishing" scams and other suspicious cyber activities.

Third, Congress has shortchanged the department. By failing to reorganize its committee structure, the homeland jurisdiction remains anemic. So the Department still has to answer to more than 80 committees and subcommittees. And Congress is unable to assert a single, principal point of oversight and review for homeland security issues and problems.

And yet, there remain opportunities for the Homeland Department to shine. Here are three:

First, while the Department should be praised for overhauling its privacy and civil liberties office, DHS shouldn't stop there. It should embrace the Privacy & Civil Liberties Oversight Board – once full membership is confirmed – and urge the board to take on tough issues like analyzing the process for protecting personal information in the event of a cyber attack. As you know, formation of the Board is mandated in the 2004 Intelligence Reform law – and its stand up is eight years overdue.

Second, DHS should do far more to reduce overclassification of intelligence. Your committee worked for a year to help pass the Reducing Overclassification Act of 2010, but little has happened. DHS must be the standard-bearer for pushing the most useful information as possible to state and local law enforcement – and mean it.

Finally, the Secretary must continue to be the face of homeland security. Janet Napolitano is an old friend, and before she took office, I suggested she be the "Everett Koop" of threat warnings – just as he was the Nation's most trusted anti-smoking crusader. That reminds me of the once prominent, color-coded Homeland Security Advisory System, which I would call one of the DHS hiccups. I asked at a hearing, after an advisory was elevated from pale yellow to dark yellow, if Tom Ridge was Homeland Security Secretary or an interior designer. And I got a very funny phone call from him shortly thereafter …

Secretary Napolitano has done a good job with the "See Something, Say Something" campaign – but her mission should be to inspire and inform Americans about how to be prepared and resilient.

In conclusion, no major attack has on U.S. soil occurred since 9/11. DHS deserves real credit – and so does this committee.

Soon, Chairman Lieberman will join the ranks of policy wonks and grandparents (like me) who work outside of the Congress. Just this week, Ranking Member Collins broke Cal Ripken, Jr.'s record for consecutive votes, and next month she will taste married life. Both of you bring such skill and dedication to this work. I strongly doubt that new roles will diminish your passion – and mine remains as strong as ever.

I salute you, dear friends.

Testimony of

Thad W. Allen
Admiral, U.S. Coast Guard (retired)

U.S. Senate
Committee on Homeland Security and Government Affairs

Thursday July 22, 2012
342 Dirksen Senate Office Building

The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions

Mr. Chairman, Ranking Member Senator Collins, and members of the committee, I am pleased to have been invited to testify on this important topic and I thank you for the opportunity.

I am also pleased to be here with my distinguished colleagues, Mr. Richard Skinner, and Congresswoman Jane Harmon.

Mr. Chairman, there are three significant anniversary dates occurring in the next year that frame the discussion of the evolution of the Department of Homeland Security. I am not here to dwell on the past but it is important to understand the circumstances under which the Department was created.

The Past and Present

The dates are:

- The 25th of November, the 10th Anniversary of the signing into law of the Homeland Security Act
- The 24th of January, the date the Department was created pursuant to that law
- The 1st of March, the date on which the operating components of the new Department were transferred from the their respective legacy departments

Mr. Chairman you know these dates all to well, as you were part of the legislative process that created the Department. From the time legislation was submitted by the administration in June 2002 until the Department was formed less than one year elapsed. The time period between enactment of the legislation until the Department was formed there was a little over three months. While this could be considered government at light speed, little time was available for deliberate planning and thoughtful consideration of available alternatives. The situation was complicated by the fact that the law was passed between legislative sessions and in the middle of a fiscal year. Other than Secretary Ridge, early leadership positions were filled by existing senior officials serving in government and did not require confirmation. Funding was provided through the reprogramming of current funds from across government for departmental elements that did not have existing appropriations from their legacy departments.

Operating funds for components that were transferred were identified quickly and shifted to new accounts in the Department to meet the deadline. Because of the wide range of transparency and accuracy of the appropriation structure and funds management systems of the legacy departments some of the new operational components faced a number of immediate challenges. Estimating the cost of salaries

for Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE) required the combination of different work forces, with different grade structures, different career ladders, and different work rules.

Basic mission support functions of the department such as financial accounting, human resource management, real property management, information resource management, procurement, and logistics were retained largely at the component level in legacy systems that varied widely. Funding for those functions was retained at the component level as well. In those cases where new entities were created (i.e. Departmental level management and operations, the Under Secretary for Science and Technology, the Under Secretary for Intelligence and Analysis, the Domestic Nuclear Detection Office) support systems had to be created rapidly to meet immediate demands of mission execution. Finally, components and departmental offices that did not preexist the legislation were located in available space around the Washington DC area and the Secretary and number of new functions were located at the Nebraska Avenue Complex in Northwest Washington.

At the time of this transition I was serving as the Coast Guard Chief of Staff and was assigned as the Coast Guard executive to overseas the Service's relocation from the Department of Transportation to the new Department. We began planning for eventual relocation as soon as the administration submitted legislation to the Congress. I also assigned personnel to the Transition Planning Office (TPO) that was created in the Office of Management and Budget by Executive Order to prepare for the transition. A considerable challenge during this period was the fact that the TPO was part of the Executive Office of the President and there were legal limitations on how much of their work could be shared externally. As a result much of that effort was redone or duplicated when the Department was created.

My intent is not to dwell on the past but to frame the degree of difficulty facing the leaders attempting to stand up the Department from the outset. Many of these issues persist today, ten years later. Despite several attempts to centralize and consolidate functions such as financial accounting and human resource management, most support functions remain located in departmental components and the funding to support those functions remains in their appropriations. Because of dissimilarities between appropriations structures of components transferred from legacy departments there is a lack of uniformity, comparability, and transparency in budget presentations across the department. As a result it is difficult to clearly differentiate, for example, between personnel costs, operations and maintenance costs, information technology costs, and capital investment. Finally, the five-year Future Years Homeland Security Plan (FYHSP) required by the Homeland Security Act has never been effectively implemented as a long rang planning, programming, and budgeting framework inhibiting effective planning and execution of multi-year acquisitions and investments.

In the Washington Area the Department remains a disjointed collection of facilities and the future of the relocation to the St. Elizabeth's campus remains in serious

doubt. One of the great opportunity costs that will occur if this does not happen will be the failure to create a fully functioning National Operations Center for the Department that could serve at the integrating node for departmental wide operations and establish the competency and credibility of the Department to coordinate homeland security related events and responses across government as envisioned by the Homeland Security Act. As with the mission support functions discussed earlier, the Department has struggled to evolve an operational planning and mission execution coordination capability. As a result, the most robust command and control functions and capabilities in the Department reside at the component level with the current NOC serving as a collator of information and reporting conduit for the Secretary.

The combination of these factors, in my view, has severely constrained the ability to the Department of mature as an enterprise. And while there is significant potential for increased efficiencies and effectiveness, the real cause for action remains the creation of unity of effort that enables better mission performance. In this regard there is no higher priority than removing barriers to information sharing within the department and improved operational planning and execution. Effective internal management and effective mission execution require the same commitment to shared services, information systems consolidation, the reduction in proprietary technologies and software, and the employment of emerging cloud technologies.

Mr. Chairman, this summary represents my personal views of the more important factors that influenced the creation and the first ten years of the Department's operations. It is not all-inclusive but is intended to be thematic and provide a basis for discussion regarding the future. Looking to the future the discussion should begin with the Department's mission and the need to create unity of effort internally and across the homeland security enterprise.

The Future

The Quadrennial Homeland Security Review was envisioned as a vehicle to consider the Department's future. The first review completed in 2010 described the following DHS missions

- Preventing Terrorism and Enhancing Security
- Securing and Managing Our Borders
- Enforcing and Administering our Immigration Laws
- Safeguarding and Security Cyberspace
- Insuring Resiliency to Disasters

An additional area of specific focus was the maturation of the homeland security "enterprise" which extends beyond the department itself to all elements of society that participate in and contribute to the security of the homeland.

The QHSR outcomes were consistent with the fiscal year 2010 budget that was submitted in early 2009 following the change of administrations. That request laid out the following mission priorities for the Department

- Guarding Against Terrorism
- Securing Our Borders
- Smart and Tough Enforcement of Immigration Laws and Improving Immigration Services
- Preparing For, Responding To, and Recovering From Natural Disasters
- Unifying and Maturing DHS

The FY 2010 budget priorities and the follow-on QHSR mission priorities have served as the basis for annual appropriations requests for four consecutive fiscal years.

I participated in the first review prior to my retirement and we are approaching the second review mandated by the Homeland Security Act. This review presents an opportunity to assess the past ten years and rethink assumptions related to how the broad spectrum of DHS authorities, jurisdictions, capabilities, and competencies should be applied most effectively and efficiently against the risks we are likely to encounter ... and how to adapt to those that cannot be predicted. This will require a rethinking of what have become traditional concepts associated with homeland security over the last ten years.

Confronting Complexity and Leading Unity of Effort

In the most recent issue of Public Administration Review (PAR) that is the journal of the American Society for Public Administration (ASPA) I wrote an editorial piece entitled "Confronting Complexity and Leading Unity of Effort."(Copy attached) I proposed that the major emerging challenge of public administration and governing is the increased level of complexity we confront in mission operations, execution of government programs, and managing non-routine and crisis events. Driving this complexity are rapid changes in technology, the emergence of global community, and the ever-expanding human-built environment that intersects with the natural environment in new more extreme ways.

The results are more vexing issues or wicked problems we must contend with and a greater frequency of high consequence events. On the other hand advances in computation make it possible to know more and understand more. At the same time structural changes in our economy associated with the transition from a rural agrarian society to a post industrial service/information economy has changed how public programs and services are delivered. No single department, agency, or bureau has the authorizing legislation, appropriation, capability, competency or capacity to address complexity alone. The result is that most government programs or services are "co-produced" by multiple agencies. Many involve the private/non-

governmental sector, and, in some cases, international partners. Collaboration, cooperation, the ability to build networks, and partner are emerging as critical organizational and leadership skills. Homeland Security is a complex "system of systems" that interrelates and interacts with virtually every department of government at all levels and the private sector as well. It is integral to the larger national security system. We need the capabilities, capacities and competency to create unity of effort within the Department and across the homeland security enterprise.

Mission Execution and Mission Support

As we look forward to the next decade I would propose we consider two basic simple concepts: Mission execution and mission support. Mission execution is deciding what do you and how to do it. Mission support enables mission execution.

Mission Execution ... Doing the Right Things Right

As a precursor to the next QHSR there should be a baseline assessment of the current legal authorities, regulatory responsibilities, treaty obligations, and current policy direction (i.e. HSPD/NSPD). I do not believe there has been sufficient visibility provided on the broad spectrum of authorities and responsibilities that moved to the department with the components in 2003, many of which are non discretionary. Given the rush to enact the legislation in 2002 it makes sense to conduct a comprehensive review to validate the current mission sets as established in law.

The next step, in my view, would be to examine the aggregated mission set in the context of the threat environment without regard to current stove piped component activities ... to see the department's mission space as a system of systems. In the case of border security/management, for example, a system of systems approach would allow a more expansive description of the activities required to meet our sovereign responsibilities.

Instead of narrowly focusing on specific activities such as "operational control of the border" we need to shift our thinking to the broader concept of the management of border functions in a global commons. The border has a physical and geographical dimension related to the air, land and sea domains. It also is has a virtual, information based dimension related to the processing of advance notice of arrivals, analysis data related to cargoes, passengers, and conveyances, and the facilitation of trade. These latter functions do not occur at a physical border but are a requirement of managing the border in the current global economic system.

The air and maritime domains are different as well. We prescreen passengers at foreign airports and the maritime domain is a collection of jurisdictional bands that extend from the territorial sea to the limits of the exclusive economic zone and beyond.

The key concept here is to envision the border as an aggregation of functions across physical and virtual domains instead of the isolated and separate authorities, jurisdictions, capabilities, and competencies of individual components. Further, there are other governmental stakeholders who interests are represented at the border by DHS components (i.e. DOT/Federal Motor Carriers regarding trucking regulations, NOAA/National Marine Fisheries Service regarding the regulation of commercial fishing).

A natural outcome of this process is a cause for action to remove organizational barriers to unity of effort, the consolidation of information systems to improve situational awareness and queuing of resources, and integrated/unified operational planning and coordination among components. The additional benefits accrued in increased efficiency and effectiveness become essential in the constrained budget environment. The overarching goal should always be to act with strategic intent through unity of effort.

A similar approach could be taken in considering the other missions described in the QHSR. Instead of focusing on "insuring resiliency to disasters" we should focus on the creation and sustainment of national resiliency that is informed by the collective threat/risks presented by both the natural and human built environments. The latter is a more expansive concept than "infrastructure" and the overall concept subsumes the term "disaster" into larger problem set that we will face. This strategic approach would allow integration of activities and synergies between activities that are currently stove piped within FEMA, NPPD, and other components. It also allows cyber security to be seen as activity that touches virtually every player in the homeland security enterprise.

In regard to terrorism and law enforcement operations we should understand that terrorism is, in effect, political criminality and as a continuing criminal enterprise it requires financial resources generated largely through illicit means. All terrorists have to communicate, travel, and spend money, as do all individuals and groups engaged in criminal activities. To be effective in a rapidly changing threat environment where our adversaries can quickly adapt, we must look at cross cutting capabilities that allow enterprise wide success against transnational organized criminal organizations, illicit trafficking, and the movement of funds gained through these activities. As with the "border" we must challenge our existing paradigm regarding "case-based" investigative activities. In my view, the concept of a law enforcement case has been overtaken by the need to understand criminal and terrorist networks as the target. It takes a network to defeat a network. That in turn demands even greater information sharing and exploitation of advances in computation and cloud-based analytics. The traditional concerns of the law enforcement community regarding confidentiality of sources, attribution, and prosecution can and must be addressed, but these are not technology issues ... they are cultural, leadership, and policy issues.

Mr. Chairman, this is not an exhaustive list of proposed missions or changes to missions for the Department. It is an illustrative way to rethink the missions of the Department given the experience gained in the last ten years. It presumes the first principals of (1) a clear, collective strategic intent communicated through the QHSR, budget, policy decisions, and daily activities and (2) an unyielding commitment to unity of effort that is supported by an integrated planning and execution process based on transparency and exploitation of information to execute the mission.

Mission Support ... Enabling Mission Execution

Mr. Chairman, in my first two years as Commandant I conducted an exhaustive series of visits to my field commands to explain my cause for action to transform our Service. In those field visits I explained that when you go to work in the Coast Guard every day you one of two things: you either execute the mission or you support the mission. I then said if you cannot explain which one of these jobs you are doing, then we have done one of two things wrong ... we haven't explained your job properly or we don't need your job. This obviously got a lot of attention.

In the rush to establish the Department and in the inelegant way the legacy funding and support structures were thrown together in 2003, it was difficult to link mission execution and mission support across the Department. To this day, most resources and program management of support functions rest in the components. As a result normal mission support functions such as shared services, working capital funds, core financial accounting, human resources, property management, and integrated life cycle based capital investment have been vexing challenges.

There has been hesitancy by components to relinquish control and resources to a Department that appears to be still a work in progress. The structure of department and component appropriations does not provide any easy mechanism for departmental integration of support functions. As a result information sharing is not optimized and potential efficiencies and effectiveness in service delivery are not being realized. As I noted earlier, a huge barrier to breaking this deadlock is the lack of uniformity in appropriations structures and budget presentation. This problem has been compounded by the failure to implement a 5-year Future Years Homeland Security Plan and associated Capital Investment Plan to allow predictability and consistency across fiscal years.

Mr. Chairman, having laid out this problem, I see three possible ways forward. The desirable course of action would be build the trust and transparency necessary for the Department and components to collective agree to rationalize the mission support structure and come to agreements on shared services. The existing barriers are considerable but the first principals of mission execution apply here as well ... unambiguous, clearly communicated strategic intent and unity of effort supported by transparency and exploitation of information. A less palatable course of action is top down directed action that is enforced through the budget process. The least desirable course of action is externally mandated change.

A first step that lies within the capability of the Department would be to require standardized budget presentations that can serve as the basis for proposed appropriations restructuring to clearly identify the sources and uses of funds and to separate at a minimum personnel costs, operating and maintenance costs, information technology costs, capital investment, and facility costs.

Conclusion

Mr. Chairman, I have attempted to keep this testimony at a strategic level and focus and thinking about the challenges in terms that transcend individual components, programs, or even the Department itself. I have recently spoken to the Department of Homeland Security Fellows and the first DHS Capstone course for new executives. I have shared many of the thoughts provided today over the last ten years to many similar groups. This year I changed my message. After going over the conditions under which the Department was formed and the many challenges that still remain after ten years, I was very frank with both groups. Regardless of the conditions under which the Department was created and notwithstanding the barriers that have existed for ten years, at some point the public has a right to expect that the Department will act on its own to address these issues. Something has to give. In my view, it is the responsibility of the career employees and leaders in the Department to collective recognize and act to meet the promise the Homeland Security Act. That is done through a shared vision translated into strategic intent that is implemented in daily activities from the NAC to the border through the trust and shared values that undergird unity of effort. It is that simple, it is that complex.

Thad W. Allen
George Washington University

Perspective

Confronting Complexity and Creating Unity of Effort: The Leadership Challenge for Public Administrators

Thad W. Allen is Distinguished Professor of Practice in the Trachtenberg School of Public Policy and Public Administration at George Washington University. He retired as 23rd commandant of the U.S. Coast Guard in 2010 and served as national incident commander for the Deepwater Horizon oil spill. He previously served as principal federal official for the response to Hurricane Katrina. He holds a master of public administration from George Washington University and a master of science from the MIT Sloan School of Management. He is currently senior vice president at Booz Allen Hamilton.
E-mail: thad.w.allen@gmail.com

It was difficult to watch the scenes from Japan last year following the earthquake, tsunami, and reactor meltdowns, just as it was difficult to comprehend the damage created by Hurricane Katrina and the Gulf oil spill. More recently, we have witnessed a cruise ship the size of a small city lying on its side. Speaking to the Annual Conference of the American Society for Public Administration in Baltimore last year, I discussed the increasing complexity of our world and the need to find new ways to address large, complex crises and problems that seem to be increasing.

I am not a scientist or an engineer. I come at this issue as a practitioner of public administration and a military leader. I do believe that advances in technology, the emergence of a global community, and large-scale increases in the "man-built" environment are intersecting with our natural world and its forces to create low-probability, high-consequence events in greater numbers. In fact, there is a significant effort under way at the National Academy of Sciences to understand these extreme events and our ability to assess and communicate risk in both the man-made and natural environments. The ultimate implications of how we view risk, allocate the costs associated with risk, and create and sustain a more resilient world will be important for this and succeeding generations.

That said, we must deal with the issues that face us today and the likelihood of more high-consequence and, in Donald Kettl's terms, "nonroutine events." In the longer term, we must develop the knowledge and capacity to create resiliency: the ability to assess risk, make appropriate preparations against those risks using available resources, respond, recover, mitigate, and reinitiate the cycle repeatedly as we adapt to our environment(s). The advent of virtualization and computation at unimaginable scale just a decade ago offers us the ability to know more and understand what is knowable. But we will continue to face "black swan" events that cannot be predicted by past experience and existing data. The demands of this environment call for us to think differently about public administration, the management of public programs, and the role of leadership in public administration.

Why is that so? Our journey from a geographically agrarian society to a more internationally linked industrial society to the current globally networked information society has, in my mind, sequentially and iteratively changed the nature of the social contract with our citizens as far as what constitutes a "public good." At the same time, our ability to segment and price goods and services has turned the economics that I learned in graduate school in the early 1980s on its ear. (I still remember my professor referring to television as a free good because it could not be segmented or priced just as cable television was born!) More recently in the Gulf oil spill, there was significant concern that the government did not own the "means of production" to cap the well. It had been a long-decided issue that oil production would be a private sector activity in this country, albeit under government supervision.

What we are witnessing is the disaggregation of social, legal, and service provision responsibilities in our society and the joint production or coproduction of what we used to know as public goods. That means that no single person, agency, department, company, nongovernmental organization, or any other entity has the sole means to deal with a black swan event or "wicked problem." Three recent books provide a good context for this challenge: Donald Kettl's *The Next Government of the United States: Why Our Institutions Fail Us and How to Fix Them* (2009); William Bratton and Zachary Tumin's *Collaborate or Perish: Reaching across Boundaries in a Networked World* (2012); and Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly's *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together* (2009).

Public Administration Review, Vol. 72, Iss. 3, pp. 320–321. © 2012 by The American Society for Public Administration.
DOI: 10.1111/j.1540-6210.2012.02585.x.

So whether we are faced with a complex, wicked problem or a disaster of unprecedented proportion, our public leaders and managers must be capable of understanding that complexity and then developing effective responses (planned or not). The central concept in successful adaptation and response in these cases is a focus on working across traditional boundaries (legal, organizational, and cultural) and understanding that trust, networks, collaboration, and cooperation are the building blocks. That is because the primary means to success is unity of effort. I use this term in distinct contrast to the military or law enforcement term "unity of command," in which the action of the organization takes place within a legal framework and compliance with orders is not discretionary.

The concept of unity of command has helped the United States create the greatest and most effective fighting force in the history of the world. However, there are practical and legal limits to the employment of military forces. Accordingly, we must seek to create unity of effort in an atmosphere in which there may be no legal authority to direct participants to act. That is the demand being placed on public administrators today, and it requires the acquisition of new leadership skills to create unity. Warren Bennis said that managers do things right and leaders do the right thing; there is now an imperative for leaders to do the right thing right.

A useful approach to this problem has been developed at the National Preparedness Leadership Initiative, a joint program of the School of Public Health and the John F. Kennedy School of Government at Harvard University. The initiative seeks to bring together leaders who will work in these new nonroutine environments to learn how to create effective unity of effort based on a concept called "metaleadership." The concept involves five dimensions of leadership that foster unity of effort: understanding oneself and one's emotions, understanding the event or the challenge correctly, *leading upward* in space between political leaders and career or subject-matter experts, *leading downward* to support one's people, and *leading across* organizational boundaries. This is a good start, and we need a competition of ideas regarding how to evolve a new model of public leadership.

One additional aspect of this new model is the increasing level of public participation in nonroutine activities. Any response to a black swan event or wicked problem will involve public participation to a greater degree than any time in history. From the 24-hour news cycle to the role of nongovernmental organizations to the social media, the participation of the public is a permanent feature of the social ecology, just as weather will always be a feature of the natural environment.

Our leaders must be capable of speaking with candor to the American people and creating as much transparency as possible. Public participation demands a "government face" for the response, and the credibility of the response often lies in leaders' ability to explain government actions in the context of a whole-of-government or whole-of-nation effort. This demand becomes instantaneous in a digital world, and there is little tolerance for an analog government that the public feels does not "get it." Moreover, elected leaders will not hesitate to create a role if they feel that their leadership and relevancy is being questioned. We should make every effort to minimize those situations.

So what does this mean? It means that Woodrow Wilson's charge to public servants to demonstrate neutral competence in a political environment has been fundamentally changed. To be effective in addressing the challenges that we face, we must learn how to unite those who have a consequential role in the outcomes we seek regardless of their role or affiliation. To rephrase Wilson, we must be effective within a political process without becoming political (as in partisan). So, as we carry out and mature our tradecraft as public administrators, let us also commit to acquiring and integrating leadership skills to work through the tough problems. Let us understand that we will need greater communications skills and political acumen. It is often said that "great leaders are great learners." I believe that. That requires a commitment to lifelong learning. Let us all continue to do that.

STATEMENT OF RICHARD L. SKINNER

FORMER INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

U.S. SENATE

The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions

July 12, 2012

Good afternoon, Chairman Lieberman, Ranking Member Collins, and Members of the Committee. It is truly an honor to be here today to discuss what the Department of Homeland Security needs to do in the years ahead to become a more efficient organization. I thank you for this opportunity.

Since its inception in 2003, the department has worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the missions of protecting the country against another terrorist attack, responding to threats and hazards, ensuring safe and secure borders, welcoming lawful immigrants and visitors, and promoting the free flow of commerce, has presented many challenges. While the department has made progress over the past nine years, it still has much to do to establish a cohesive, efficient, and effective organization.

The OIG's latest major management challenges report, dated November 10, 2011, continues to address a broad range of issues, including both program and administrative challenges. In total, the OIG identified nine categories of challenges: Financial Management, Information Technology Management, Acquisition Management, Grants Management, Emergency Management, Infrastructure Protection, Border Security, Transportation Security, and Trade Operations and Security. These are essentially the same management challenges that the the OIG reported as early as 2005. Today, I would like to talk about four of those management challenges:

- Financial management,
- Information technology management,
- Acquisition management, and
- Grants management.
-

These management support functions constitute the platform upon which the department's programs must operate and are critical to the successful accomplishment of the department's mission. Some of these challenges were inherited by the department from the legacy agencies. Nevertheless, the complexity and urgency of the department's mission have hampered its efforts to make sustainable progress in implementing corrective actions.

Senior officials at the department recognize the significance of these challenges and understand that addressing them will take a sustained and focused effort. They have, in fact, taken actions over the past several years to implement, transform, and strengthen the department's management support functions; albeit, in my opinion, at a snails pace.

FINANCIAL MANAGEMENT

Financial management has been and continues to be a major management challenge for the department since its creation in 2003. In FY 2011, the department was again unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses were again reported. These weaknesses, due to their materiality, are impediments to obtaining a clean opinion and providing positive assurance over internal controls at the department level. The department has made progress from its early days, however. It has reduced the number of material weaknesses in internal controls from 18 to 5. It also received a qualified audit opinion on its consolidated balance sheet and custodial activity for the first time in fiscal year 2011. Unfortunately, unless the department modernizes its financial systems, it is unlikely this progress will continue.

The department twice unsuccessfully attempted to implement an integrated department-wide financial management system, wasting?? millions of dollars. In 2007, the department ended its first attempt, the Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency system after determining it would not provide the expected functionality and performance.In 2011, the department decided to change its strategy for financial system modernization. Rather than implement a department-wide integrated financial management system solution, the department decided to take a decentralized approach to financial management systems modernization at the component level. Specifically, the department reported in its December 2011 strategy that it plans to replace financial management systems at three components it has identified as most in need, e.g., FEMA, USCG, and ICE. However, due to FY 2012 budget reductions, these initiatives have been put on hold indefinitely. It is now not clear when the department will resume its modernization strategy, nor is it clear whether this new, decentralized approach, if and whenever it is implemented, will ensure that components' financial management systems can generate reliable, useful, timely information for day-to-day decision making; enhance the department's ability to comprehensively view financial information across the department; and comply with related federal requirements at the department and its components. In the interim, the department must continue to use archaic, unreliable systems to manage it financial resources, which is unfortunate, particularly in this day and age of budget austerity and the public demand for increased fiscal transparency and accountability.

INFORMATION TECHNOLOGY MANAGEMENT

According to recent OIG and GAO reports, DHS and its components are still struggling to upgrade or transition their respective IT infrastructures, both locally and enterprise wide.

Integrating the IT systems, networks, and capabilities of the various legacy agencies to form a single infrastructure for effective communications and information exchange remains one of the department's biggest challenges.

For example, on October 20, 2011, the Assistant IG for Emergency Management Oversight, Matt Jadacki, testified that FEMA's existing information technology systems do not effectively support disaster response activities . FEMA has not completed its efforts to establish an enterprise architecture, and its IT strategic plan was not comprehensive enough to coordinate and

prioritize its modernization initiatives and IT projects. The plan did not include clearly defined goals and objectives, nor did it address program office IT strategic goals. Without these critical elements, FEMA is challenged to establish an effective approach to modernize its information technology infrastructure and systems.

According to Mr. Jadacki, there is not an adequate understanding of existing information technology resources and needs throughout the agency. Specifically, FEMA's Office of the Chief Information Officer (CIO) does not have a complete, documented inventory of systems to support disasters. Further, program and field offices continue to develop information technology systems independently of the CIO and have been slow to adopt the agency's standard information technology development approach. As a result, systems are not integrated, do not meet user requirements, and do not provide the information technology capabilities agency personnel and its external partners need to carry out disaster response and recovery operations in a timely, effective, and efficient manner.

Furthermore, according to a report issued recently by GAO, FEMA does not have an effective system to manage flood insurance and claims data, although it invested roughly 7 years and $40 million on a new system whose development has been halted because it did not meet users' needs.

Most recently, on June 29, 2012, the Assistant IG for Information Technology Audits, Frank Deffer, reported that the information technology environment and the aging IT infrastructure within CBP does not fully support CBP's mission needs. According to Mr. Deffer, interoperability and functionality of the technology infrastructure have not been sufficient to support CBP mission activities fully. As a result, CBP employees have created workarounds or employed alternative solutions, which may hinder CBP's ability to accomplish its mission and ensure officer safety.

Similar problems also have been reported at the Coast Guard, Citizen and Immigration Services, ICE, and Secret Service. Technical and cost barriers, aging infrastructure that is difficult to support, outdated IT strategic plans to guide investment decisions, and stove-piped system development have impeded the department's efforts to modernize and integrate its IT systems, networks, and capabilities.

Information Sharing

The Homeland Security Act of 2002 makes coordination of homeland security communication with state and local government authorities, the private sector, and the public a key department responsibility. However, due to time pressures, the department did not complete a number of the steps essential to effective planning and implementation of the Homeland Security Information Network (HSIN)—the "sensitive but unclassified" system it instituted to help carry out this mission. For example, the HSIN and the Homeland Security State and Local Community of Interest systems, both developed by DHS, are not integrated. As a result, users must maintain separate accounts, and information cannot easily be shared across the systems. State and local fusion center personnel expressed concern that there were too many federal information sharing systems that were not integrated. As such, effective sharing of the counter-terrorist and emergency management information critical to ensuring homeland security remains an ongoing

challenge for the department. Resources, legislative constraints, privacy, and cultural challenges—often beyond the control of the department—pose obstacles to the success of the department's information sharing initiatives.

On a broader scale, the department is also challenged with incorporating data mining into its overall strategy for sharing information to help detect and prevent terrorism. Data mining aids agents, investigators, and analysts in the discovery of patterns and relationships from vast quantities of data. The Homeland Security Act authorizes the department to use data mining and tools to access, receive, and analyze information. However, the department's data mining activities consist of various stove-piped activities that use limited data mining features. For example, CBP performs matching to target high- risk cargo. The Secret Service automates the evaluation of counterfeit documents. TSA collects tactical information on suspicious activities. ICE detects and links anomalies indicative of criminal activity to discover relationships. Without department-wide planning, coordination, and direction, the potential for integrating advanced data mining functionality and capabilities to address homeland security issues remains untapped.

ACQUISITION MANAGEMENT

DHS has taken notable action to implement, transform, and strengthen its acquisition management capabilities. During my tenure as the IG of the department, the Secretary and Deputy Secretary of Homeland Security, and other senior officials demonstrated a genuine commitment to improve the department's acquisition management function. In its December 2011 strategy for high risk management, the department presented detailed plans to address a number of acquisition management challenges. However, much work remains to fully implement these plans and address these challenges. Most notably, the department needs to identify and acquire the resources needed to implement its acquisition policies.

OIG and GAO audits over the past nine years have identified problems related to acquisition oversight, cost growth, and schedule delays, resulting in performance problems and mission delays, as illustrated by the problems the department experienced with the Coast Guard's Deepwater program, CBP's SBINet program, FEMA's flood map modernization program, and the CFO's financial systems consolidation initiatives. Each of these efforts failed to meet capability, benefit, cost, and schedule expectations. For example, in June 2010 my former office reported that over half of the programs we reviewed awarded contracts to initiate acquisition activities without component or department approval of documents essential to planning acquisitions, such as mission need statements outlining the specific functional capabilities required to accomplish DHS's mission and objectives; operational requirements; and acquisition program baselines. Additionally, the OIG reported that only a small number of DHS's major acquisitions had validated cost estimates.

The urgency and complexity of the department's mission will continue to demand rapid pursuit of major investment programs. Between fiscal years 2003 and 2010, the department spent about 40% of its budget through contracts. Although that figure may have decreased over the past two years, the department will continue to rely heavily on contractors to accomplish its multi-faceted mission and will continue to pursue high-risk, complex acquisition programs.

The department must have an infrastructure in place that enables it to effectively oversee the complex and large dollar procurements critically important to achieving its mission.

Both the OIG and the GAO have reported that the Office of the Chief Procurement Officer needs more staff and authority to carry out its general oversight responsibilities. The GAO recommended that the department provide the Office of the Chief Procurement Officer sufficient resources and enforcement authority to enable effective, department-wide oversight of acquisition policies and procedures. The OIG made a similar recommendation.

Common Themes in Audits of Department Contracts

Over the past several years, the OIG and GAO conducted numerous audits of individual department contracts, such as TSA's information technology services, CBP's SBInet program, the Coast Guard's Deepwater program, and FEMA contracting. Common themes and risks emerged from these audits, primarily poor planning, the dominant influence of expediency, poorly defined requirements, and inadequate oversight that contributed to ineffective or inefficient results and increased costs. To ensure that its acquisition programs are successful, the department must lay the foundation to oversee and assess contractor performance, and control costs and schedules. This requires a sustained commitment, increased resources, and smarter processes to administer and oversee the contractors' work.

FEMA Procurements

The Assistant IG for Emergency Management Oversight, Matt Jadacki, testified on October 20, 2011 that FEMA has developed and strengthened acquisition management policies and processes, but it continues to face challenges. For example, weak internal controls have resulted in multi-million dollar contracts with vague and questionable requirements and no performance measures. Agency employees responsible for managing and monitoring the contractors do not always receive written guidance or training on how to evaluate contractor performance or certify billing invoices. Continued improvements are needed in FEMA's oversight of contracts.

During my tenure as the IG, my office issued several reports recommending improvements to FEMA's acquisition processes. Those recommendations have resulted in policies and procedures on contract closeout, transferring contract files from one contracting officer to another, and labeling and organizing contract files so all contract actions are properly documented.

In fiscal year 2010, FEMA deployed Disaster Assistance Employees to accelerate contract closeout efforts for the Disaster Relief Fund, de-obligating $1.2 billion. These contract closeout efforts continue annually and are in direct response to an OIG recommendation. I was pleased to learn that FEMA has created Disaster Acquisition Response Teams, whose focus on contract administration and oversight of large disaster contracts is much needed. My office also reported FEMA's need for an overarching sourcing strategy. Headquarters, regional, and local FEMA representatives were ordering goods without communicating with their counterparts at other locations. This resulted in goods ordered that were not needed, purchased from the wrong source, or at the wrong time. My former office recommended that FEMA adopt the single-point ordering concept, to coordinate all sourcing decisions through the Logistics Section. As a result

of this recommendation, FEMA piloted the single-point ordering concept during its response to Hurricane Irene .

Strategic Sourcing

The department can improve management of its strategic sourcing. In March 2011, the OIG reported that the department did not have a logistics process in place to facilitate strategic sourcing of detection equipment. Strategic sourcing would require that management standardize equipment purchases for explosive, metal, and radiation detection equipment; identify common mission requirements among components; and develop standard data elements for managing the inventory accounts of detection equipment. Improving its management of detection equipment will offer the department opportunities to streamline the acquisition process and improve efficiencies.

Acquisition Workforce

DHS made progress in the recruitment and retention of a workforce capable of managing a complex acquisition program. At the time of my retirement on March 1, 2011 the number of procurement staff had more than doubled since 2005. In addition, participation in the Acquisition Professional Career Program, which seeks to develop acquisition leaders, increased 62% from 2008 to 2010. Nevertheless, DHS continues to face workforce challenges across the Department. For example, according to GAO, the Coast Guard reduced its acquisition workforce vacancies from approximately 20 percent to 13 percent, and had filled 832 of its 951 acquisition positions as of November 2010. Although acquisition workforce vacancies have decreased, program managers have ongoing concerns about staffing program offices. Also, according to its August 2010 human-capital staffing study, program managers reported concerns with staffing adequacy in program management and technical areas. To make up for shortfalls in hiring systems engineers and other acquisition workforce positions for its major programs, the Coast Guard must use contractors.

Likewise, according to the OIG's Major Management Challenges report, dated November 2011, acquisition staff turnover in FEMA has exacerbated file maintenance problems and resulted in multimillion-dollar contracts not being managed effectively or consistently. One of FEMA's challenges is hiring experienced contracting officers to work disaster operations. The majority of FEMA staff at a disaster site work on an on-call, intermittent basis, and, oftentimes, they lack the training and experience to manage large disaster response and recovery contracts.

FEMA also has made great strides in improving its contracting officer's technical representative (COTR) cadre. FEMA has designated staff to oversee the COTR program; developed a tiered system which ties training requirements to dollar values of contracts a COTR can monitor; and established an intranet site containing tools for COTR use. However, many trained COTRs have never been assigned a contract and are unsure of their ability to be effective. And, although they represent the contracting officer, the COTR's appraisal is completed by his supervisor in the program office for which he works, rather than the applicable contracting officer, thus leading to divided loyalties.

Finally, the department has not fully planned for or acquired the workforce needed to implement its acquisition oversight policies. According to a GAO report issued in February 2011, the department needs to continue its efforts to (1) identify and acquire resources needed to achieve key actions and outcomes; (2) implement a program to independently monitor and validate corrective measures; and (3) show measurable, sustainable progress in implementing corrective actions and achieving key outcomes. The department needs to demonstrate sustained progress in all of these areas to strengthen and integrate the acquisition management functions throughout the department.

Knowledge Management and Information Systems

According to the OIG's annual Major Management Challenges report, the department has made progress in deploying an enterprise acquisition information system and tracking key acquisition data. The department's acquisition reporting system of record, known as nPRS (next-Generation Periodic Reporting System), tracks components' major acquisition investments. It also has capabilities to store key acquisition documents, earned value management information, and risk identification. Component personnel are responsible for entering and updating information, which includes cost, budget, performance, and schedule data. However, components did not complete and report all key information in nPRS. The OIG reported that only 7 of 17 programs (41%) reported Acquisition Program Baseline required milestones. These milestones establish the acquisition cost, schedule, and performance values. Only 13 (76%) programs reviewed contained required key documentation such as mission needs statement, acquisition plan, operational requirements document, and integrated logistics support plans.

In addition, the department reported in its December 2011 strategy for high risk management that senior executives are not confident enough in the data to use the department's Decision Support Tool which was developed to help make acquisition decisions, address problems meeting cost or schedule goals, and prepare for program review meetings.

Although the department continues to make progress in improving its acquisition management, it remains a significant challenge facing DHS, in part because of the magnitude of the number, dollar value, and complexity of its acquisition activity.

GRANTS MANAGEMENT

Disaster Grants Management

FEMA oversees billions of dollars in disaster grant funds each year, and, due to the environment under which these funds are administered, they are highly vulnerable to fraud, waste, and abuse. To illustrate, during FYs 2010 and 2011, the OIG's audits of 105 disaster grants identified $365 million in questionable cost and funds that could be put to better use. The extent of the fraud, waste, and abuse that the OIG uncovers year after year in the disaster relief program, for the past twenty years, is unacceptable, and it needs to be vigorously addressed. Yet FEMA still has not developed a robust program to curtail fraud, waste, and abuse within its disaster relief programs.

Preparedness Grants Management

During fiscal years 2002 through 2011, FEMA distributed over $18 billion through the Homeland Security Grant Program. According to an OIG report released earlier this week, FEMA does not have a system in place to determine the extent that Homeland Security Grant Program funds enhanced the states' capabilities to prevent, deter, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Also, FEMA does not require states to report progress in achieving milestones as part of the annual application process. As a result, when annual application investment justifications for individual continuing projects are being reviewed, FEMA does not know whether prior year milestones for the projects have been completed. FEMA also does not know the amount of funding required to achieve needed preparedness and response capabilities.

Furthermore, according to the OIG's annual Major Management Challenges report, dated November 2011, FEMA continues to face challenges in mitigating redundancy and duplication among preparedness grant programs, including barriers at the legislative, departmental, and state levels. The preparedness grant application process is ineffective because FEMA does not compare and coordinate grant applications across preparedness programs. Since grant programs may have overlapping goals or activities, FEMA risks funding potentially duplicative or redundant projects.

Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, required the OIG to audit individual states' management of State Homeland Security Program and Urban Areas Security Initiatives grants and annually submit to Congress a report summarizing the results of these audits. In the audits completed to date, the OIG concluded that the states have generally done an efficient and effective job of administering the grant management program requirements, distributing grant funds, and ensuring that all the available funds were used.

However, on March 20, 2012, the Assistant Inspector General for Audits testified that FEMA needs to make improvements in strategic management, performance measurement, and oversight. According to Ms. Richards, FEMA needs to improve its guidance on strategic plans for State Homeland Security Grants. While current guidance for state Homeland Security strategic plans encourages revisions every two years, the language is such that it does not require revisions to be made—it is just strongly encouraged. Consequently, many states have outdated strategic plans, and many do not have Homeland Security strategic plans with goals and objectives that are specific, measurable, achievable, results-oriented, and time-limited. Without some form of measurable goal or objective, or a mechanism to objectively gather results-oriented data, states have no assurance of the level of effectiveness of their preparedness and response capabilities. Also, states are less capable of determining progress toward goals and objectives when making funding and management decisions. The OIG reported deficiencies in strategic planning in 15 of the 20 state audits completed as of March 2012.

In regard to performance measurement, Ms. Richards said that FEMA needs to improve its guidance on establishing metrics and measuring performance. OIG audits show that many states continue to lack the proper guidance and documentation to ensure accuracy or track milestones. Providing guidance on the appropriate metrics and requiring those metrics to be documented would provide the states with tools to help them understand the effectiveness of each grant program. FEMA also needs to strengthen its guidance on reporting progress in achieving

milestones as part of the states' annual program justifications. Because of insufficient information on milestones and program accomplishments, FEMA has been annually awarding Homeland Security Grant Program funds to states for ongoing programs without knowing the accomplishments from prior years' funding or the extent to which additional funds are needed to achieve desired capabilities. Tracking accomplishments and milestones are critical elements in making prudent management decisions because of the evolving, dynamic changes that can occur between years or during a grant's period of performance. OIG audits reported problems with performance measurement in 19 of 20 state audits completed as of March 2012.

Finally, Ms. Richards said that FEMA needs to improve its oversight to ensure the states are meeting their reporting obligations in a timely manner to ensure FEMA has the information it needs to make program decisions and oversee program achievements. Further, FEMA needs to improve its oversight to ensure that states are complying with federal regulations in regard to procurements and safeguarding of assets acquired with federal funds. In its annual audits of the State Homeland Security Program, the OIG repeatedly found weaknesses in the states' oversight of grant activities. Those weaknesses include inaccuracies and untimely submissions of financial status reports; untimely allocation and obligation of grant funds; and not following federal procurement, property, and inventory requirements. Delays in the submission of Financial Status Reports hampers FEMA's ability to effectively and efficiently monitor program expenditures and prevents the State from drawing down funds in a timely manner, ultimately affecting the effectiveness of the program.

Strategic planning, performance measurement, and oversight are important management controls for FEMA to ensure that federal funds are used for their intended purpose and that enhancements in preparedness capabilities are being achieved. Without a bona fide performance measurement system, it is impossible to determine whether annual investments are actually improving our Nation's homeland security posture. Furthermore, without clear, meaningful performance standards, FEMA lacks the tools necessary to make informed funding decisions. In today's economic climate, it is critical that FEMA concentrate its limited resources on those threats that pose the greatest risk to the country.

****

While some aspects of the department's management support challenges were inherited from the department's legacy agencies, the complexity and urgency of the department's mission has oftentimes exacerbated the department's ability to address them in a disciplined and effective manner.

It is evident that the department's senior officials are well aware of these challenges and are attempting to remedy them, and they have actually made some headway. The question is, however, does the department have the resolve and wherewithal to sustain those efforts. The ability of the department to do so is fragile, not only because of the early stage of development that the initiatives are in, but also because of the government's budget constraints and the current lack of resources to implement planned corrective actions. In today's environment of large government deficits and pending budget cuts, the new challenge will be to sustain the progress already made and at the same time continue to make the necessary improvements that are critical to the success of the department's management functions.

Unless the department and Congress stay focused on these challenges, it will be harder than ever to facilitate solutions to strengthen the department's management support functions and, ultimately, its homeland security mission.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the Members may have.

****

Post-Hearing Questions for the Record
Submitted to the Honorable Jane Harman
From Senator Joseph I. Lieberman

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. In 2013 the Department will conduct its second Quadrennial Homeland Security Review (QHSR). This is something that Congress mandated in the 2007 Implementing Recommendations of the 9/11 Commission Act, and is a critical strategic initiative for DHS. I believe that the 2009 QHSR was helpful to Secretary Napolitano and the current leadership team in terms of formulating their strategic priorities, and I am hopeful that the review that will take place next year will build on the lessons learned from that review and take the next step in terms of its level of detail and its impact on Departmental planning and operations.

What do you believe are some of the most critical issues for DHS to examine in this next QHSR?

2. In your testimony you highlight the value of state and local fusion centers, which is due both to the federal support that is provided to them – most of it from DHS – but also importantly due to the support of state and local leaders – governors and mayors – which operate them and provide a very large share of funding from their own coffers. What needs to be done to sustain and continue to improve the work of state and local fusion centers?

Responses from Congresswoman Harman:

These responses to questions posed by my former colleague are more general in nature. Given my policy background, I feel most qualified to address three bigger-picture issues.

1. DHS's Intelligence Role:

The DHS intelligence function is not widely respected. Part of this has to do with jurisdiction, but it is also because appointees have lacked certain skills and/or interest.

In my opinion, it makes sense to limit the intelligence function to lanes where DHS can excel. These include 1) securing borders and critical infrastructure and 2) focusing on vertical relationships with state, local, and private sector partners rather than horizontal relationships with other federal agencies.

State and local agencies, as well as different private sectors in the US, should drive requirements for what kind of intelligence would be most helpful to them. Since these

customers require information with limited classification, it is important that DHS concentrate on materials that start at lower-classification levels. At the same time, these clients should also serve as sources of information about what emerging threats they are seeing in their communities or industries. It is vital that intelligence flow both ways.

One good tool is H.R. 553, The Reducing Over-Classification Act, which was considered and reported by your committee. I urge you to conduct oversight on how well it is being implemented.

2. Lone Wolves:

Sadly, the Aurora theater and Sikh temple shootings remind that lone wolves are a growing security threat. As a recent *Washington Post* article pointed out, a technological shift has allowed people to join hate groups (which have increased by 65 percent in number since 2000) anonymously online and become motivated to commit acts of violence.

It is part of DHS's responsibility to protect our country from these lone wolves and small terrorist cells. A DHS-funded video released after the Aurora shooting advised citizens to—in this order—"run, hide, fight." While such counsel is both needed and welcome, the Department should simultaneously be working closely with local law enforcement officials and citizens across the country to prevent a crisis from even getting close to that point of peril. After all, they are the ones who know their communities best and are therefore most likely to identify unusual and suspicious activities.

3. Privacy and Civil Liberties:

I commend DHS for overhauling its privacy and civil liberties office, but there is more work to be done on this front. We established the Privacy and Civil Liberties Board in 2004 as part of the Intelligence Reform and Terrorism Prevention Act, but the board was ineffective in the Bush years and vacant under Obama. (While the Senate just confirmed four nominees before it left for its summer recess, it failed to confirm a chair, who would be the board's only full-time member and have the ability to hire staff.) It should be a high priority after the election either to confirm a chair or to fill the board with new members promptly.

As soon as that happens, DHS should urge the board to take on the tough issues, which range from protecting personal information in the event of a cyber attack to tracking domestic terrorists without infringing on free speech. As the Department hopefully recognizes by now, security and liberty are not—to paraphrase Ben Franklin—a zero-sum game. We either get more or less of both.

Post-Hearing Questions for the Record
Submitted to the Honorable Jane Harman
From Senator Claire McCaskill

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. You mentioned that DHS should narrow some of its functions, particularly intelligence.

    a. What do you suggest the more limited intelligence role should be? How would you define it?

    b. In your opinion, what other functions should be narrowed? Are there any functions that need to be consolidated, but Congress is standing in the way?

2. How do we create an organization that is more flexible, more nimble, and more capable of adapting to the new threats our nation will face in the coming decade? What general qualities should such an organization have?

3. Even more important than discussing the evolution of DHS in the context of this hearing is for the Department to have the capacity and the institutional processes to assess its own operations and evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?

4. We have heard that criminal networks are becoming increasingly sophisticated and diversifying their operations, and that there are growing linkages between these groups.

    a. What is the best way to combat this?

    b. Is it helpful to have the DEA, FBI, ATF, Secret Service, and ICE as separate investigative agencies? Are those divisions between agencies hampering our efforts to combat transnational crime?

Responses from Congresswoman Harman:

These responses to questions posed by my former colleague are more general in nature. Given my policy background, I feel most qualified to address three bigger-picture issues.

1. DHS's Intelligence Role:

The DHS intelligence function is not widely respected. Part of this has to do with jurisdiction, but it is also because appointees have lacked certain skills and/or interest.

In my opinion, it makes sense to limit the intelligence function to lanes where DHS can excel. These include 1) securing borders and critical infrastructure and 2) focusing on vertical relationships with state, local, and private sector partners rather than horizontal relationships with other federal agencies.

State and local agencies, as well as different private sectors in the US, should drive requirements for what kind of intelligence would be most helpful to them. Since these customers require information with limited classification, it is important that DHS concentrate on materials that start at lower-classification levels. At the same time, these clients should also serve as sources of information about what emerging threats they are seeing in their communities or industries. It is vital that intelligence flow both ways.

One good tool is H.R. 553, The Reducing Over-Classification Act, which was considered and reported by your committee. I urge you to conduct oversight on how well it is being implemented.

2. Lone Wolves:

Sadly, the Aurora theater and Sikh temple shootings remind that lone wolves are a growing security threat. As a recent *Washington Post* article pointed out, a technological shift has allowed people to join hate groups (which have increased by 65 percent in number since 2000) anonymously online and become motivated to commit acts of violence.

It is part of DHS's responsibility to protect our country from these lone wolves and small terrorist cells. A DHS-funded video released after the Aurora shooting advised citizens to—in this order—"run, hide, fight." While such counsel is both needed and welcome, the Department should simultaneously be working closely with local law enforcement officials and citizens across the country to prevent a crisis from even getting close to that point of peril. After all, they are the ones who know their communities best and are therefore most likely to identify unusual and suspicious activities.

3. Privacy and Civil Liberties:

I commend DHS for overhauling its privacy and civil liberties office, but there is more work to be done on this front. We established the Privacy and Civil Liberties Board in 2004 as part of the Intelligence Reform and Terrorism Prevention Act, but the board was ineffective in the Bush years and vacant under Obama. (While the Senate just confirmed four nominees before it left for its summer recess, it failed to confirm a chair, who would be the board's only full-time member and have the ability to hire staff.) It should be a high priority after the election either to confirm a chair or to fill the board with new members promptly.

As soon as that happens, DHS should urge the board to take on the tough issues, which range from protecting personal information in the event of a cyber attack to tracking domestic terrorists without infringing on free speech. As the Department hopefully recognizes by now, security and liberty are not—to paraphrase Ben Franklin—a zero-sum game. We either get more or less of both.

Post-Hearing Questions for the Record
Submitted to Admiral Thad W. Allen, USCG, Ret.
From Senator Joseph I. Lieberman

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. In the Committee's hearing on July 11, 2012, several of the witnesses discussed the ways in which our nation's primary homeland security threats – terrorism, cyber threats, drug trafficking organizations, and organized crime – are all increasingly converging with each other. To the extent that you agree that there is such convergence, what are its implications for the operational activities of DHS? How do DHS's major operational components need to adapt to address such hybrid or converging threats?

Response: I agree that the threats are converging. All criminal enterprises share common characteristics that model legal enterprises except those activities are carried out illegally. As globalization has link legal markets it has created the conditions for illicit markets to link as well. I consider terrorism to be political criminality. All criminal enterprises require financing and all criminals must communicate, travel, and spend money. Criminal enterprises are also networks and must be attacked with networks. No single agency or set of authorities and jurisdictions has been designed to address the spectrum of activities that are carried out by criminal networks. Law enforcement agencies must adapt to this new environment and develop better ways to integrate authorities, capabilities, capacities, competencies, and networks to defeat these criminal enterprises. To that end DHS must (1) improve information sharing through the elimination of software or systems that are proprietary or do not allow the exchange of information, (2) integrate existing operational capabilities to reduce redundancies and gain efficiencies, (3) create departmental capability to plan and coordinate multi-agency operations, (4) where possible collocate field operations to improve coordination and unity of effort locally, (5) participate in joint or interagency task forces and private sector partnerships that optimize information sharing and create trust among participants (i.e. JIATF South/West, EPIC, OCDETF Fusion Center), and (6) exploit new advances in high performance computing and cloud based analytics to identify threats earlier.

2. In nearly all of its significant areas of responsibility, DHS needs to carry out its missions in coordination with other Departments and agencies. What is your assessment of how effective DHS has been in terms of its policy-related and operational interactions within the interagency? Where it has been effective, and what needs to be done to improve its ability to lead in areas that involve extensive interagency cooperation?

Response: The Department has matured in these areas but gaps exist. To be effective in the interagency the department needs to demonstrate the capability and competency to

manage events across government. To do that effectively the Department must first create the same capability within the department across components. The challenge in interagency policy or operational coordination is to create unity of effort without legal authority to direct agencies. I use the concept of "unity of effort" in contrast to "unity of command" which exists in the Department of Defense by statute and allows lead/follow relationships to be mandated. The authority of the Secretary in the Homeland Security Act is general and more specific tasking on coordination of interagency operations is contained in HSPD-5 that is a policy document not law. I believe the statutory authority of the Secretary should be strengthened and the Secretary should be a member of the National Security Council. A good example of progress by the Department has been the work carried out by the Council of Governors, a body created by Executive Order in 2009 that is coordinating issue between the federal government and state governors. Significant progress has been made on the harmonization of federal support to states, specifically the employment of the National Guard. The Department was also effective in unifying efforts in support of the Department of State in the response to the Haitian earthquake, most notably in FEMA-USAID cooperation and the DHS led task force in South Florida that managed the personnel evacuations and immigration issues.

3. While serving as Coast Guard Chief of Staff, you chaired the DHS Joint Requirements Council (JRC) from 2003-2006, which was intended to align investments to key missions and operational requirements.

   In 2010, Under Secretary for Management Rafael Borras initiated efforts to establish an "Integrated Investment Life Cycle Model" (IILCM) that would have a similar function as the JRC, and has been strengthening key capabilities (e.g. cost analysis, business intelligence, acquisition risk management) to support such a planning process. What lessons would you offer from your experience leading the JRC that would be helpful to the relevant initiatives at DHS today?

Response: The concept of the IILCM is sound and I support it. The challenges in moving from concept to reality will be (1) the ability to warehouse data and analyze it, (2) the standardization of financial and appropriations structures across the department, (3) the continued migration to a federated and then common financial accounting system, and (4) the willingness of components to accept the process and actively participate (or the Department's ability to direct it).

The JRC enjoyed moderate success because it was a peer review body where every component was represented and trust and collegiality were shared values. JRC development was interrupted by Hurricane Katrina and was never fully restored. The current iteration of the IILCM contemplates a Capabilities and Requirements Council to assume the prior functions of the JRC and a broader portfolio of resource management issues. My lessons from the JRC are contained in the challenges listed above which underscore the need for transparency of financial information as a means to adequately compare investment alternatives.

4. One of the deficiencies frequently identified in the aggregate results of DHS employee surveys relates to professional development and career tracking, particularly for junior and mid-level employees. What do you believe needs to be done to improve professional development and career tracking within DHS?

Response: I would refer the committee to my testimony before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management of 22 March 2012 which is provided below and the following additional comments. Leadership development needs to be a funded program of record with a predictable annual funding level and the direct support and sponsorship of the Secretary.

Professional and career development is hampered by the lack of a standard integrated human resource system for the department. Several attempts have been made and failed. The problem is very complex and stems from the original challenges associated with creating the department. CBP for example is still trying to integrate legacy work force structures from Customs, INS, and Agriculture. The recurring underlying inhibiter that I have referred to in my testimony is the lack of a uniform financial management structure that affects every facet of departmental operations.

ATTACHMENT TO QUESTION 4

Testimony of

Thad W. Allen
Admiral, U.S. Coast Guard (retired)

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Oversight, Investigations, and Management

Thursday March 22, 2012
311 Cannon House Office Building

Introduction

Chairman McCaul, Ranking Member Keating, and members of the subcommittee, thank you for the opportunity to provide testimony today.

Let me first congratulate you Mr. Chairman and the committee for addressing an important issue. I have been involved with the Department since its inception and welcome the opportunity to discuss the linkage between employee morale and and personal and organizational performance.

I am testifying today in my capacity as a private citizen and the views expressed by me are not intended to represent any government agency or private firm. A summary of my work experience and experience related to the missions of the Department of Homeland Security are provided at the conclusion of this statement.

Max Stier, the President of the Partnership for Public Service is a member of the next panel and is best suited to discuss in detail their report *Best Places To Work In The Federal Government.* My perspective today is one of a leader who served in the Department of Homeland Security since its inception and as a coworker and colleague of the men and women who serve or have served in the components that make up the Department for over forty years. My comments also reflect my experience leading large complex responses across the federal government that demand unity of effort to meet our commitment to the American public.

Morale

Let me state at the outset that it is my belief that morale is not an objective to be achieved in an organization. It is rather the natural by product of high performing people and organizations. It is a measure of the collective understanding by employees of the mission and their role in the organization and an acknowledgement that the conditions in which they work enable them to succeed.

When there is a shared vision of the mission, commitment to the shared values of an organization and strong and effective leadership that enables employees to be successful morale "happens." Creating such an environment is not necessarily easy and cannot be accomplished overnight. It is the collective impact of workplace conditions, the quality of front line supervisory leadership, the mission support structure that enables mission execution, and an enduring commitment by senior leaders to the concept that mission performance starts and ends with people.

Organizational Context

It is my opinion that there are three environments that collectively interact with individual performance and therefore impact morale.

The Workplace Environment

At a very basic and personal level, morale is the collective effect and interaction of individual aspirations, interpersonal relationships, workplace conditions, and front line supervisory leadership that that drive employee performance. From this view, to paraphrase your former colleague Tip O'Neill, all "morale is local." At this level the greatest organizational impacts on employee morale in my view are (1) the quality of frontline supervisory leadership and (2) the work environment ... the physical surroundings, support structures, work tools, and co-workers. This applies equally to deployed units, field offices and headquarters staffs.

The Department or Agency Environment

Beyond the immediate work environment factors that impact personal and organizational performance are legislative authorities that define the mission and structure and effectiveness of the organization. Specifically, I am referring to the capability and capacity of the enterprise to execute the mission, the real or perceived competency of the organization (internally and externally), and ultimately the understanding of the individual of their role and their value in that structure. Critical to employee understanding of their role in this larger context is clear, unambiguous communication by leaders on mission and core values.

The Federal Government Environment

Finally, the overall structure of the federal government and its real or perceived competency to meet its social contract with the American public is something that every government employee feels and understands. I have stated repeatedly in various fora that is important to distinguish between the difficult choices that are required to deal with shrinking budgets and the value of public service. We do a great disservice to hundreds of thousands of federal employees when a constrained fiscal environment is interpreted as a referendum on the value of public service.

Pre-existing Organizational Issues Create Complexity And Challenges

It is difficult to discuss employee morale in DHS without first acknowledging the conditions under which the Department was created and the degree of difficulty associated with "retrofitting" basic organizational structure and capabilities. This issue is greatly misunderstood but any discussion regarding departmental performance and morale must acknowledge it. We need to understand that different elements and components of the Department were created and now exist within radically different structures and are in different stages organizational life cycle and maturity, including the departmental headquarters. For example, the highest scoring departmental agencies in the rankings (Coast Guard and Secret Service) were moved intact to DHS in 2003 with minimal disruption to ongoing operations. While TSA was transferred intact, the organization was still being built. CBP and ICE, on the other hand, were created largely from reorganized INS and Customs functions with the attendant challenges of integrating work forces,

different collective bargaining structures, different grade structures, and operating procedures. Still other entities such as the Domestic Nuclear Detection Office, Science and Technology, and Intelligence and Analysis were created from "whole cloth" by legislation and had no precursors.

The process was further complicated by the inelegant redistribution of base funding from legacy departments and agencies due to a lack of historical cost information (the Department was created in the middle of a fiscal year with reprogrammed funds and did not receive an annual appropriation until FHY 2004). OMB has pressed for efficiencies throughout the life of the Department without first acknowledging that capability, competency, and capacity are precursors to cost savings (IT savings were sought in the transition process when new investment was required).

The Department's Fiscal Year 2013 Budget Justifications reveals little consistency in budget presentation or treatment of standard organizational costs such as personnel, operating expenses, capital investment, programs of record, or support costs such as information technology. While progress has been made to standardize budget submissions the basic structure of appropriations remains different in each component and is an indicator of the enduring challenge of functional integration in DHS. While these issues sound bureaucratic and removed from actual work environments, there are few employees in the Department that are not aware of the challenges associated with maturing the enterprise.

Improved Individual and Organizational Performance Positively Impacts Morale

An exhaustive evaluation of every factor that impacts employee morale is well beyond the scope of my testimony today. Accordingly, I would like to focus on a few areas that I believe offer the best opportunities to improve organizational and individual performance and by extension morale. It is not surprising that these recommendations also contribute to a more integrated, functionally aligned department that is more capable of mission execution.

- Develop Leaders That Retain Employees And Create Unity of Effort
- Provide The Tools, Capabilities, And Competencies That Enable Personnel To Succeed In The Work Place
- Create A Mission Support Architecture To Generate and Sustain The Capability and Capacity of the Enterprise to Execute the Mission
- Integrate The Planning and Coordination Of Mission Execution That Reflects Internal Unity Of Effort And External Interagency Leadership

Develop Leaders That Retain Employees And Create Unity of Effort:

The federal government has struggled for decades to create a strategic and comprehensive leadership development framework. The government wide effort has been attenuated by various individual mandates to develop training programs within communities of interest such as the intelligence community, national security organization, Defense Department, State Department and others. The spotty collective performance of these initiatives has less to do with their content than the lack of sustained commitment at the highest levels of the organization that protects, nurtures, and celebrates the process that produces leaders, an earmark of successful and sustained military professional and leadership development.

As a strong supporter of the current DHS Fellows program I can personally attest to the fact that the program is valued and celebrated by the cohort that has received the training and the program is helping to build cohesion within the department. I also strongly support the evolving DHS leadership framework that focuses on employees at all levels. That fact however carries little weight with budget reviewers and examiners and these programs are often the first casualty of internal reviews, OMB passbacks, and budget negotiations that focus on large, high dollar programs and policies at the expense of the basics of organizational success. As a result these programs are often funded from year end "fall out" funds or reprogrammed funds from other programs when available. Mr. Chairman, these are not huge amounts of money but the return on investment is considerable. The leadership development program in Homeland Security should fence off a budget line item that allows multi-year planning, promotes consistency of program execution, and demonstrates senior leader commitment. While current programs begin with senior leader training, I would focus on improving the skills of front line supervisors who have a significant impact on employee performance and morale.

Provide The Tools, Capabilities, And Competencies That Enable Personnel To Succeed In The Work Place:

As noted earlier one facet of employee morale is their sense of the commitment of their organization and leaders to them through the tools they are provided to do their jobs. To that end, physical facilities, information technology, communications, specialized training, access to enterprise information, performance systems, collective bargaining structures, employee benefits, and the opportunity for organizational learning can all positively impact morale. It is well beyond the scope of my testimony to "drill down" in each of these areas regarding Departmental capability and performance. However, there are strong thematic links that can be discussed in the context of stronger component and Departmental performance. Three are discussed here.

Human Resource Systems
First, the current human resource system the Department is an aggregation of pre-existing systems from legacy agencies and departments. Early attempts to create an

all-encompassing HR system and a pay for performance structure across the Department failed and current efforts are focused on smaller incremental changes to integrate the diverse existing systems. Past failures to adequately forecast and budget for adjustments to position grades needed to integrate legacy organizations have resulted in short term emergency fixes. The Department should seek to standardize the forecasting, accounting, budgeting and funding of personnel costs within a departmental framework that is visible and comparable across departmental components and entities in the annual budget. Increased consistency and transparency in managing personnel costs will reduce uncertainty and the need for year-to-year adjustments that, in turn, create concern in the workforce.

Information Systems

Second, whether an employee executes the mission in the field or supports the mission regionally or in a headquarters, the organizational medium of exchange that propels daily operations is information. From automated license plate readers at land ports of entry, to personal radiation detectors, to passenger and cargo screening, to cost accounting information related to logistics support of aircraft, mission execution and mission support is enabled by the information that is generated by or made available to department employees. Information sharing is an enterprise challenge that I will address in the next section but we should remember that employees measure organizational commitment by how much they are empowered to know and then to act on that knowledge. The challenge can be seen in discrete parts.

- Information collection, storage, and access
- Analytical tools that convert data to decision supporting knowledge
- Platforms and devices that allow access, including visualization of knowledge to enable decision making
- Systems security

At present there are numerous efforts to improve information access for employees in the Department but it is generally focused at the component level and within individual stove piped data and communications systems. While progress has been and is being made, every effort must be made to put state of the art information technology tools in the hands of departmental employees and those tools must be integrated across components.

Workplace Integration, Building A Unified Team

Every DHS component and headquarters office has a noble and worthy mission to protect the American public. Some components such as Customs and Border Protection and the Coast Guard have legacies that span two centuries of service. However, the promise of the Homeland Security Act was knit these functions and activities into a unified, cohesive enterprise.

The entering argument for unity of effort at the working level is trust. The formula for trust is (1) a shared vision of the mission, (2) a commitment to share expertise and information, and (3) the ability to represent a parent organization without

allowing parochial policy, budget, or cultural issues to cloud effective participation and the success of the larger "good." When employees see their leaders creating this type of work environment they are motivated to improve their performance as well.

I have seen this demonstrated in countless venues across the Department where effective teams work side-by-side, tirelessly everyday to executive the mission. The challenge is that this model is not present everywhere. Where it exists morale is high, where there is no trust employees revert to governing policies that protect the resources and discretion of their component, regardless of the mission requirement or the demands of the situation. These situations erode the rationale for the Department's creation and inhibit the maturation of the Department as a leader across government.

The ability to integrate effort in the field is affected by (1) facility decisions that restrict, do not allow or fail to facilitate colocation, (2) stove piped data systems that make access to even DHS counterpart's information difficult, and (3) local leadership challenges where supervisors are hesitant or unwilling to partner and collaborate. Similar challenges exist in Washington where components are physically separated from the Departmental headquarters and there is a proliferation of command centers.

Create A Mission Support Architecture To Generate and Sustain The Capability and Capacity of the Enterprise to Execute the Mission:

During my first two years as Commandant of the Coast Guard I initiated a sweeping transformation of our mission support structure to build a more effective organization to enable mission execution. That transformation continues today. To demonstrate my commitment to this change I participated in a number of All Hands meetings throughout the Coast Guard. I explained the mandate for improved mission support in simple terms. If you work for the Coast Guard (or any governmental agency for that matter), you do one of two things: you either execute the mission or you support mission execution. If your daily work cannot be explained by either of these, one of two mistakes has occurred. The task has not been fully explained or the task in not needed.

A significant driver of employee morale is the ability for the employee to connect their daily work to the agency mission. Everyone has heard the classic story of the janitor at a NASA facility who was asked what he did and his response was "I put men on the moon!" As noted earlier, the first decade of the existence of the Department of Homeland Security has been challenging and earmarked by (1) public "zero tolerance" for failure, (2) unrelenting media scrutiny, (3) duplicative oversight, and (3) the inevitable immediate public discourse and referendum on departmental performance while operations are being conducted. In this environment it is easy to become captive to what I call the "tyranny of the present." That said, it is critically important to preserve the time, effort and resources to

unambiguously define the need and create a mission support structure that enables mission execution and allows every employee to say, "I protect the homeland."

While one could argue exactly what constitutes "mission support" I think an acceptable structure would generally include the following:

- Human Resources
- Financial Management
- Information Systems and Communications (and their security)
- Acquisition Planning and Management
- Facilities Management
- Logistics and Maintenance
- Health, Safety, and Environment

The challenge in creating an integrated departmental mission support system is to combine disparate support systems that were transferred from legacy agencies with base funding contained in component appropriations. This requires a shared vision of the end state and a framework to implement needed changes. Repeated attempts at integration and/or consolidation across these functional support lines of business have not been successful. Employees know this. That said, current demand for improved performance and morale are now converging with a constrained budget environment to create a cause for action to refocus on the integration of mission support functions of the Department.

Integrate The Planning and Coordination Of Mission Execution That Reflects Internal Unity Of Effort And External Interagency Leadership:

The Department faces two major challenges in effective mission execution to achieve unity of effort and improve performance (and morale): (1) internal integration of operational planning and execution across components and mission areas and (2) creating the capability, competency, and capacity to eternalize planning and execution across the federal government and vertically with state and local governments. This fundamental process of an operating department is, in my view, is the single most impactful Departmental role that is visible to all employees. Further, it is the basis by which the Department is seen and evaluated by stakeholders, overseers, the public, and the media.

From the outset the Department has been hampered by the Balkanization of facilities and command centers, particularly in the Washington, DC area. The exigencies associated with standing up the Department rapidly and the proliferation of office locations in and around Washington has hampered the development of a central unified command center that is necessary to the effective planning and coordination of operations. The promise of a unified national operations center at the St. Elizabeth's venue appears to be in doubt.

Notwithstanding the need for physical consolidation, the Department should continue to press ahead to develop improved organizational capability to plan and execute operations, including effective information sharing and analysis, risk assessment, and the development of departmental and national doctrine to guide mission execution.

Conclusion

Mr. Chairman, the challenges faced by the Department of Homeland Security are numerous but hundreds of thousands of dedicated employees work tirelessly everyday to serve the American public. Our collective responsibility is to provide them the best leadership and tools that enable them to perform to their greatest potential. The goal should not be to try to affect survey respondents behavior to achieve a better score but to enable and empower employees to do their job and be proud of it. If you enable performance, morale will follow.

PERSONAL BACKGROUND

I am currently employed as a Senior Vice President at Booz Allen Hamilton and prior to that I served for 39 years in the United States Coast Guard. I served as the Commandant from 2006 to 2010. From 2010 to 2011 I was a Senior Fellow at the RAND Corporation. I am a Fellow in the National Academy of Public Administration, and a member of the Council on Foreign Relations. I serve on the Boards for the Partnership for Public Service, the Division of Earth and Life Sciences of the National Research Council, the Coast Guard Foundation, and the Comptroller General's Advisory Board.

Pertinent Homeland Security Experience

1. On 11 September 2001 I was the Commander of the Coast Guard Atlantic Forces.
   a. I directed the overall Coast Guard response to the terrorist attacks. Units under my command closed and secured Boston and New York Harbors and the Potomac River north of the Woodrow Wilson Bridge. The Coast Guard commander in New York City coordinated the evacuation of hundreds of thousands of people from lower Manhattan by employing an ad hoc flotilla of available vessels in the harbor.
   b. From 2001 to 2002 I worked closely with Commander, Joint Forces Command (JFCOM) and Commander, North American Defense Command (NORAD) in the development of the concept for the U.S. Northern Command (NORTHCOM). I later provided a small cell of Coast Guard personnel that became part of the team that stood up NORTHCOM.

2. From 2002 to 2006 I served as the Chief of Staff of the Coast Guard and in that capacity I was responsible for managing Coast Guard Headquarters and coordinating day-to-day activities related to planning, programming, and budgeting.

3. Following the passage of the Homeland Security Act in the Fall of 2002, I was assigned by the Commandant to manage the transfer of the Coast Guard from the Department of Transportation to the newly established Department of Homeland Security.

a. I directed a task force that identified all existing relationships with the Department of Transportation. We then developed a plan to transition these activities to the new Department of Homeland Security, retain them within the Coast Guard or negotiate continued support by the Department of Transportation.

b. I also assigned a senior officer and other personnel to the Transition Planning Office that was created in OMB in the fall of 2002 to prepare for the stand up of the Department.

c. When the Department was created on 24 January 2003, I assigned Coast Guard personnel to work with DHS senior leadership to facilitate the transition, including clerical, contracting, travel, and administrative support to the Secretary and others.

d. On 1 March 2003, the Coast Guard was transferred to DHS. We continued to provide staffing to support DHS Headquarters and I worked with both Deputy Secretary Gordon England and Under Secretary of Management Janet Hale to created the smoothest transition possible.

e. From 2003 to 2006, I worked with Under Secretary Hale to establish a Management Council and a Joint Requirements Council (JRC) for major acquisition oversight. I chaired the JRC from 2003 to 2006.

f. I volunteered to chair the first Combined Federal Campaign for the Department in the fall of 2003. I later served for two years as the Chairman of the National Region Campaign.

g. In advance of the 2008 Presidential election I worked with then Under Secretary George Foresman to create the DHS Fellows Program to develop senior leaders and create a cadre of staff professionals that could be of use during the transition of administrations. That program continues today and is managed by the Partnership For Public Service.

4. From September 2005 to February 2006 I was detailed as the Principal Federal Official for the responses to Hurricane Katrina and Rita.

5. From May 2006 to May 2010 I served as the Commandant of the Coast Guard.

a. As a component head within DHS I participated extensively in a broad spectrum of activities including operations planning and coordination, budgeting, policy development, departmental management, and crisis response and management.

b. I was a participant in the transition of administrations following the 2008 Presidential election.

b. I participated in the initial Quadrennial Homeland Security Review

c. I participated in the response to the Haitian earthquake in January 2010 and represented the Secretary at numerous meetings at the White House.

6. From May 2010 to October 2010 I served as the National Incident Commander for the federal response to the Deepwater Horizon explosion and subsequent oil spill. For a portion of that response (1 July to 1 Oct) I was retired from the Coast Guard and served as a Senior Executive attached to the Secretary's office.

Post-Hearing Questions for the Record
Submitted to Admiral Thad W. Allen, USCG, Ret.
From Senator Claire McCaskill

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. How do we create an organization that is more flexible, more nimble, and more capable of adapting to the new threats our nation will face in the coming decade? What general qualities should such an organization have?

Response: The current DHS organization was conceived and implemented quickly due to the post 9/11 threat environment and tight timelines contained in the Homeland Security Act. There was inadequate time to plan and develop the departmental organizational structure and resource it correctly. As a result here was never a coherent mission execution or support structure developed to conduct the business and operations of the department. Regarding mission support, the resources to support operations reside largely in operating component budgets not the department. I believe the Department needs integrate support services to improve mission performance and create efficiencies. This will be difficult because it will require transparency of operating costs together with a common structure for appropriations and funds execution. This will continue to be a debilitating condition and will inhibit any organizational reforms. Regarding mission execution, the Department needs to develop and implement a more robust command and control structure that can effectively plan and execute operations involving all components. Modest changes in 2008 created an operational planning and coordination function but the department has never been able move beyond the monitoring and reporting of component activities. Failure to create a single integrated national operations center that was envisioned at the St Elizabeth's Complex will perpetuate the current structure with its capability limitations. The qualities that need to exist in the Department and operating components are a commitment to unity of effort, information sharing, the elimination of proprietary software and information systems that do not allow data to be moved and shared, commitment to a robust common operating picture that fuses information in real time to improve operational performance, commitment to common support services (i.e. maintenance, logistics, human resources, financial accounting, real property).

2. Even more important than discussing the evolution of DHS in the context of this hearing is for the Department to have the capacity and the institutional processes to assess its own operations and evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?

Response: I do not believe the current processes that produced the QHSR or NIE are sufficient. As noted in my prior answer the department structure for operational planning and coordination need to be improved. In a similar manner the process to develop policy, create strategies, and make resource allocation decisions needs to mature as well. The Department is currently

developing an Integrated Investment Life Cycle Model (IILCM). The IILCM is intended to create a governance structure and institutionalized processes to support future QHSRs and related strategy and policy development including the capability to conduct evaluations of policies, programs, and operational activities. The first step to insure this effort is successful would be to conduct a baseline review of the authorities, jurisdictions, regulatory responsibilities, treaty obligations, and existing policy guidance that guide departmental and component activities. The Homeland Security Act aggregated existing legal authorities and created new ones for the Department and new entities that were formed. There was never a deliberate process to reconcile these authorities against the threat environment to identify gaps, overlaps, redundancies, and other sources of conflict or inadequate authority. This process should be a requirement before the next QHSR. Finally, there should be a determination as to whether the current policy structure that guides departmental and intergovernmental operations (i.e. Homeland Security Presidential Directive, National Security Presidential Directives) are adequate and whether some of this guidance should be contained in statute. For example, the Homeland Security Act did not amend the National Security Act to make the Secretary a member of the National Security Council and operational coordination across government is carried out under HSPD-5, which is policy not law.

3. We have heard that criminal networks are becoming increasingly sophisticated and diversifying their operations, and that there are growing linkages between these groups.

    a. What is the best way to combat this?

    b. Is it helpful to have the DEA, FBI, ATF, Secret Service, and ICE as separate investigative agencies? Are those divisions between agencies hampering our efforts to combat transnational crime?

Response: This is one of the most important questions facing our Nation as we adapt to a changing threat environment 10 years after the creation of the Department of Homeland Security. A number of factors need to be considered. First, all criminal enterprises rely on illegal sources of financing to conduct operations and generate profits. The most common feature of any enterprise scale criminal activity is the need for operating funds. Second, I believe in this respect that there is no difference between terrorism and transnational organized crime. Terrorism is political criminality. Third, these enterprises are networks and engage in multiple activities that are agnostic to the organizing statutes for federal law enforcement agencies. Fourth, federal law enforcement agencies are organized to address specific threats and activities and were created over time without regard to the commonality of criminal enterprises. They also focus investigations, arrests, indictments, prosecutions, and convictions in response to violations of law within each set of authorities.

A basic question we must confront as we understand the commonality of these networks and the case/defendant focus of law enforcement work is how we can best achieve results. Prosecution is by definition consequence management and it requires public attribution of the sources of information leading to the arrest. Prevention or the creation of a "non event" may be preferable. It is difficult to have that discussion because it requires the reconciliation of authorities that might be brought to bear, the most effective application of resources, and, in some cases,

subordination of one set of authorities to another. Finally, existing organizational boundaries (i.e. authorities, appropriations) result in each agency creating internal case management systems, usually associated with proprietary information systems. This inhibits information sharing and makes it difficult to attack a network with a network that is the only way to deal with transnational organized crime. Generically, criminals need to communicate, travel, and spend money to carry out their activities. Law enforcement efforts should seek to disrupt, debilitate, and destroy these networks. That should be the first priority, not a particular agency arrest and prosecution.

These agencies must adapt to deal with threats that cross organizational boundaries and more openly share information. If they demonstrate they can do this, their performance will answer the question. In my view the jury is out. The Department of Homeland Security can become a leader in addressing this challenge by eliminating proprietary systems and other barriers to the exchange of information within the Department. This does not require new legislative authority. It requires discipline and enforcement of standards that make information "fungible."

Post-Hearing Questions for the Record
Submitted to the Honorable Richard L. Skinner
From Senator Joseph I. Lieberman

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. In your testimony you recommend giving more authority to the DHS Chief Procurement Officer. What specific authorities would you give? And how would you balance the need for strong oversight at the headquarters level with the need for the different DHS components, which are closest to their operational needs, to have control over their procurements?

Response: While serving as the IG, I always asserted that the DHS CPO should have supervisory authority over the component procurement heads, similar to the arrangement the DHS General Counsel has over the component general counsel heads. As it now stands, or at least when I was serving as the IG, the DHS CPO had no say in the component hiring process or in the employee performance evaluation process. Consequently, as OIG audits pointed out year after year, the components were ignoring or consistently failing to meet legislative, White House, and DHS-wide mandates to reduce sole source contracting, increase small business contracting, and improve contract oversight. In my opinion, this is attributable to the DHS CPO's inability to exercise supervisory authority over the component procurement heads. Giving the DHS CPO the authority to hire, manage, and evaluate the performance of the component procurement heads should in no way impede or interfere with the DHS components' ability to satisfy or control their procurement requirements and needs. Rather, it would ensure that those requirements and needs are met in a consistent manner throughout the department and in conformance with applicable legislative, White House, and DHS-wide mandates.

2. DHS has had consistently low rankings as a federal workplace in the annual federal employee surveys – although it should be noted that office that you formerly led, the DHS Office of Inspector General, fared much better than the Departmental averages in these surveys during your leadership tenure. What do you think are the root causes of these low rankings, and what does the Department need to do to improve it? What can Congress do to address deficiencies identified in these surveys?

Response: First, I need to point out that the OIG, at least during my tenure, never performed an assessment of the root causes of the department's low rankings as a federal workplace. Therefore, I have no empirical data to support my opinion on this subject. That said, I believe there are many factors that are contributing to the department's low rankings. Following are a few of my personal observations:

First and foremost was the environment or manner in which the department was created, that is, it was created in haste in response to the 9/11 attacks and without the prerequisite

strategic planning. Consequently, confusion prevailed. The department was stood up without a clear transition plan, operational differences were not fully defined, lines of communications were nonexistent or ineffective, and, most notable, management support functions (financial, acquisitions, human resources, IT, and grants) were short-changed. Congress should require every component within the department to develop a transition plan (it's still not too late), with milestones and performance goals, that clearly articulates what changes are needed in order for the department to operate as a single integrated entity and to ensure that the nuances of disparate policies, procedures, and practices are being addressed.

Second, the numerous congressional committees and subcommittees claiming to have oversight responsibility for the department has had a profound impact on the department and its employees. To meet the oftentimes conflicting demands of more than 88 committees and subcommittees can be demoralizing and counterproductive. Only Congress can address this issue.

Third, the intensive and more often than naught negative media attention the department and its components receive weighs heavily on the morale of the department's employees. The department needs to do a better job of marketing its successes, which are many, and, at the same time, be more proactive and transparent with both the media and the Congress about the many challenges it must overcome each and every day to fulfill its homeland security mission. In the early years, mission demands frequently trumped good business practices, which led to poor decision-making, and, in turn, led to warranted criticism. However, much of the criticism was unwarranted and could have been avoided, in my opinion, had the department been more transparent about its programs and operations and the challenges it faced to successfully administer them.

Fourth, frequent turnover in key leadership positions and the ensuing reorganizations and policy shifts, as well as the lapses in time to fill key leadership positions, is undoubtedly having a profound impact on employee morale and confidence. The White House, the Congress, and the department all have a role to play in ensuring that key leadership positions are filled with "qualified" professionals in a "timely" manner. Those in acting positions, while competent in their prior position, may not be best suited to lead an organization, causing a decay in employee morale and confidence. A case in point is the Office of Inspector General, which was ranked as the number one place to work within the department at the time of my retirement in March 2011. Today, however, I am told it ranks at the bottom. I can only attribute this to the fact that the position of Inspector General has remained vacant for the past 18 months and the Acting IG lacks the leadership skills and qualifications to lead and motivate the OIG's professional staff of auditors, investigators, inspectors, and attorneys.

Finally, some employees within the legacy components, particularly FEMA and Customs, have been reticent to accept the changes that come with a major reorganization and, oftentimes, have a difficult time accepting their new role within the organization. As time passes and legacy employees retire from federal service, this problem should resolve itself. Unfortunately, this can take many years.

Post-Hearing Questions for the Record
Submitted to the Honorable Richard L. Skinner
From Senator Claire McCaskill

"The Future of Homeland Security: The Evolution of the Homeland Security Department's Roles and Missions"
July 12, 2012

1. In the current fiscal climate, Inspectors General (IGs) are being asked to do more with less. In your view, what do you believe should be the top priorities for the Office of the DHS IG? Do you believe the acting DHS IG has made these priorities the focus of his office?

Response:

First, I do not believe that any organization, including the OIG, should be expected "to do more with less." While you may be able to do more, the quality of the work will be adversely affected and, more often than naught, less reliable and useful to both the Congress and the agencies for which the IGs serve. Instead, the IGs need to ensure their priorities: (1) match the priorities and core mission requirements of their respective departments and agencies; (2) focus on those programs that are the most vulnerable to fraud, waste, abuse, and mismanagement; and, (3) provide coverage of the management support functions, (i.e., financial management, acquisition management, information technology management, human resource management, and grants management) upon which their respective agencies' must rely on to successfully meet their mission mandates. IGs simply need to learn to say "NO" when asked to to perform tasks that fall outside these parameters.

I do not believe the acting DHS IG has made these priorities the focus of his office. While it appears that the OIG may be continuing to focus on the department's priorities and management support functions, it most certainly is not focusing its resources on those programs that are most vulnerable to fraud, waste, abuse, and mismanagement. This is most evident in the attention that is being given to FEMA programs and operations, which has a long history of wasting taxpayer dollars. The acting IG has downsized the OIG's Emergency Management Office, which was created, with the full support of Congress, to oversee FEMA's programs and operations. Also, from what I have observed through my review of the IG's annual performance plans, little attention is being given to the programs and operations of TSA, another agency within DHS that has exhibited significant management problems.

2. How do we create an organization that is more flexible, more nimble, and more capable of adapting to the new threats our nation will face in the coming decade? What general qualities should such an organization have?

Response:

I believe the department currently has one of the more flexible and nimble organizations within government capable of adapting to new threats our nation will face in the coming decade, at least more so than it is given credit. Unfortunately, it has not done a good job, at least in my opinion, of marketing or publicizing its successes and capabilities, which has left the mistaken impression that it is not capable of adapting to new threats or, for that matter, current threats. That said, the department is by no means as flexible and nimble as it should or can be in its current stage of development. The general qualities that come to mind, and by no means all-inclusive, that the department should possess in the coming decade would involve, in my opinion, diplomacy, cybersecurity, intelligence, and intergovernmental relations. The department's Office of International Affairs needs to be, in my opinion, elevated within the organization. The department's international affairs office is now buried in the bowels of the organization without the authority to manage or otherwise direct the department's bilateral and multilateral relationships in pursuit of the Nation's homeland security mission. Furthermore, while it has the responsibility, it does not have the authority or tools to effectively manage the ever increasing cybersecurity threats to our Nation's critical infrastructure, which is controlled primary by the private sector. This authority can come only from Congress. Also, the department must do a better job of working with the intelligence community, both domestically and internationally. While the department has a seat at the national intelligence roundtable, its role and value still remains murky. Finally, the department must do a better job of working with its federal, state, local, and tribal counterparts. While progress ha been made over the past nine years, it has been slow and cumbersome. Until the department recognizes these players as equal partners, there will remain an element of mistrust and reticence to share and exchange intelligence information and data.

3. Even more important than discussing the evolution of DHS in the context of this hearing is for the Department to have the capacity and the institutional processes to assess its own operations and evaluate future needs on a recurring basis. Do you believe the current processes to produce the QHSR or NIE are sufficient to examine evolving homeland security threats and the government structures we have in place to meet them?

Response:

Both the QHSR and NIE are important first steps to providing a strategic framework and foundation for national participation in assessing homeland security threats and the government structures in place to meet them. However, these processes are only as

effective as the people and organizations responsible for using them. And, because these processes involve so many people and organizations, it will require persistent leadership, continuing oversight, investment of resources, transparency, and accountability for those responsible for their development and implementation, which, in itself, is an evolving process.

4. We have heard that criminal networks are becoming increasingly sophisticated and diversifying their operations, and that there are growing linkages between these groups.

   a. What is the best way to combat this?

Response:

Staying one step ahead of criminal networks always has and always will be a major challenge for the law enforcement community. To combat this, the law enforcement community needs to maximize the use of its IT capabilities, i.e., forensics; predictive analyses; open source, sensitive law enforcement, and intelligence data matching; and, most importantly, information sharing. All these capabilities are currently available to the community, but they are not always being maximized to their fullest extent, primarily due to development costs and the inability to share information on a real time basis among the myriad of systems that exist today in the law enforcement community.

   b. Is it helpful to have the DEA, FBI, ATF, Secret Service, and ICE as separate investigative agencies? Are those divisions between agencies hampering our efforts to combat transnational crime?

Response:

Each of these agencies have an important role to play to combat transnational crime, and, based on my experiences, it is helpful to have them as separate agencies. Their divisions most certainly do not hamper our efforts to combat crime; instead, they enhance our efforts. Each brings an expertise or specialty to the table that most likely would be diluted or lost if combined under one tent. I do not mean to imply that these agencies can't do a better job of working together, they can. Much more can be done to ensure that they work in a collaborative manner toward a common goal of combatting transnational crime, particularly with regard to information sharing.