

HOMELAND THREATS AND AGENCY RESPONSES

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 19, 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

76-070 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

DANIEL K. AKAKA, Hawaii

THOMAS R. CARPER, Delaware

MARK L. PRYOR, Arkansas

MARY L. LANDRIEU, Louisiana

CLAIRE McCASKILL, Missouri

JON TESTER, Montana

MARK BEGICH, Alaska

SUSAN M. COLLINS, Maine

TOM COBURN, Oklahoma

SCOTT P. BROWN, Massachusetts

JOHN McCain, Arizona

RON JOHNSON, Wisconsin

ROB PORTMAN, Ohio

RAND PAUL, Kentucky

JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*

CHRISTIAN J. BECKNER, *Associate Staff Director for Homeland Security
Prevention and Protection*

NICOLE M. MARTINEZ, *Professional Staff Member*

NICHOLAS A. ROSSI, *Minority Staff Director*

RYAN M. KALDAHL, *Minority Director of Homeland Security Policy*

MARSHALL C. ERWIN, *Minority Professional Staff Member*

TRINA DRIESSNACK TYRER, *Chief Clerk*

PATRICIA R. HOGAN, *Publications Clerk*

LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

| | |
|-------------------------|------|
| Opening statements: | Page |
| Senator Lieberman | 1 |
| Senator Collins | 4 |
| Senator Moran | 19 |
| Senator Akaka | 21 |
| Prepared statements: | |
| Senator Lieberman | 31 |
| Senator Collins | 34 |
| Senator Akaka | 36 |
| Senator Carper | 37 |
| Senator Moran | 38 |

WITNESSES

WEDNESDAY, SEPTEMBER 19, 2012

| | |
|--|----|
| Hon. Janet Napolitano, Secretary, U.S. Department of Homeland Security | 6 |
| Hon. Matthew G. Olsen, Director, National Counterterrorism Center, Office of the Director of National Intelligence | 9 |
| Kevin L. Perkins, Associate Deputy Director, Federal Bureau of Investigation, U.S. Department of Justice, on behalf of the Hon. Robert S. Mueller III, Director, Federal Bureau of Investigation, U.S. Department of Justice | 12 |

ALPHABETICAL LIST OF WITNESSES

| | |
|--------------------------|----|
| Napolitano, Hon. Janet: | |
| Testimony | 6 |
| Prepared statement | 40 |
| Olsen, Hon. Matthew G.: | |
| Testimony | 9 |
| Prepared statement | 61 |
| Perkins, Kevin L.: | |
| Testimony | 12 |
| Prepared statement | 73 |

APPENDIX

| | |
|---|-----|
| Responses to post-hearing questions for the Record: | |
| Secretary Napolitano | 82 |
| Mr. Olsen | 104 |

HOMELAND THREATS AND AGENCY RESPONSES

WEDNESDAY, SEPTEMBER 19, 2012

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

The Committee met, pursuant to notice, at 10:04 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, Pryor, Collins, and Moran.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good morning to all. This is our Committee's annual homeland threat assessment hearing. I want to welcome back Janet Napolitano, Secretary of the Department of Homeland Security (DHS); and Matt Olsen, the Director of the National Counterterrorism Center (NCTC); and welcome the Associate Deputy Director of the Federal Bureau of Investigation (FBI), Kevin Perkins, who is standing in for Director Robert Mueller today. The Director had to undergo an unexpected surgical procedure resulting from complications associated with a recent dental treatment so he is unable to join us today. But we welcome Mr. Perkins in his stead with confidence, and we extend best regards to the Director for a speedy recovery.

This will be the final time that I have the privilege of chairing this annual hearing, so I want to use this opportunity to thank each of you for your leadership in our Nation's homeland security and counterterrorism efforts; to thank those who work with you in each of your departments or agencies; and more narrowly to thank you for the productive relationship that each of you and your predecessors have had with this Committee.

The obvious fact, as I look at the three of you, and then look back, is that on September 11, 2001 (9/11), two of the three organizations testifying today did not exist, and the third, the FBI, was a very different organization than it is today, focused on domestic crime as it had been for quite a while.

Obviously, in the aftermath of the terrorist attacks on America of September 11, 2001, Congress and the Executive Branch created the Department of Homeland Security and then, pursuant to the 9/11 Commission recommendations, created the National Counterterrorism Center. The FBI essentially re-created itself into a first-rate domestic counterterrorism intelligence agency, in addition to

carrying out all of its other responsibilities. And in his absence, we should thank Director Mueller for what I think is the extraordinary job he has done in overseeing this historic transformation and thank the two of you, Secretary Napolitano and Director Olsen, for what you have done.

Together these changes represent the most significant reforms of America's national security organization since the 1940s at the beginning of the Cold War. And it is not coincidental since after 9/11 we understood that we were facing a very different threat to our national security and with an intensity that we had not experienced through most of American history, a very real threat to our homeland security.

So as I look back, I really want to again thank you and your predecessors in each of these roles—although in the FBI, Director Mueller has pretty much been there the whole time—and the thousands of Federal employees who work under you, because I think without question, because of all that the three organizations represented here before us have done, the American people have been much safer here at home than we otherwise would have been if your agency had not existed. So with a lot of gratitude, I thank you for that remarkable transformation. We have made a lot of progress; we have kept the enemy away for most of the last 11 years.

The most lethal threats or attacks on our homeland have actually been carried out, as we know, by homegrown terrorists: Nidal Malik Hasan at Fort Hood and Carlos Bledsoe at the Army recruiting station in Little Rock. But the battle goes on, and it is hard to reach a conclusion other than it will go on for a long time.

Obviously, we hold this hearing today still mourning the deaths of the American Ambassador to Libya, Chris Stevens, and three other State Department personnel, still, speaking personally, infuriated by those attacks that resulted from a movement against—which I believe to be a terrorist act—our consulate in Benghazi on the 11th anniversary of the attacks of September 11, 2001.

These attacks do many things, but they remind us, I think, first of the bravery and commitment of government officials who serve in countries around the world, supporting the struggles of people in those countries to live free and, by doing so, work to improve our own national security.

The attack in Libya also reminds us that even though the core of al-Qaeda has been seriously weakened, we still face threats from an evolving and fractious set of terrorist groups and individuals, united by a common ideology, which is that of violent Islamist extremism. And I will have some questions to ask the three of you about the nature of the terrorist threat today and specifically with regard to the reaction to this film, whether you think it has raised the threat level against any places, institutions, or individuals here in the United States.

In reporting to us on the terrorist threat to the homeland today, I also hope you will address other concerns, such as the effort to counter homegrown violent Islamist groups; the threat to our homeland and people in a different way over the last couple of years posed by Islamic Republic of Iran, its Iranian Guard corps, and the Quds force, part of it, and its proxy groups such as Hezbol-

lah, which certainly seem to be reaching outside of their normal areas of operation in the Middle East and conducting attacks elsewhere. These include an attempted assassination, which was thwarted, of the Saudi ambassador here in Washington, and apparently the attack on a tourist bus in Bulgaria just a short while ago.

I would like to just say a few words about cybersecurity, which has been a significant focus of this Committee this year. We know how serious the problem is. Enormous amounts of cyber espionage and cyber theft are going on, and there is increasing danger of a cyber attack. As you know, the Cybersecurity Act of 2012, which was the compromise bipartisan legislation that made it to the Senate floor, has had problems getting enough votes to get taken up on the Senate floor. We worked for years with partners on both sides of the aisle. We had extensive consultations with private industry, and, of course, we went to substantial lengths to find common ground, including by making the standards voluntary and not mandatory for the private sector owners of cyber infrastructure.

But despite the magnitude of the threat as recognized by national security leaders and experts from the last two Administrations, regardless of party, and the many compromises that were made, the bill was filibustered on the Senate floor last month so it could not come up. Thus was lost the best opportunity we have had to pass comprehensive cybersecurity legislation. And, of course, all of you have said, Director Mueller perhaps most memorably, that, in his opinion, the threat of cyber attack will soon replace the threat of terror attack as a danger for our homeland security.

I believe that it is obvious that we are not going to pass the cybersecurity legislation before the election, and because we are probably leaving here in the next couple of days to return after the election, but I think it is still possible and, I would add, critical for Congress to pass a cybersecurity bill this session. And I certainly will continue to try to do everything in my power to do so. But I must say if the gridlock continues, as I fear it will, then the President and others in the Executive Branch should really do everything within their power, as I know they are considering actively now, to raise our defenses against cyber attack and cyber theft.

The fact is that today, because of the inadequate defenses of America's privately owned critical cyber infrastructure, we are very vulnerable to a major cyber attack, perhaps a catastrophic cyber attack, well beyond in its impact what we suffered on September 11, 2001.

I understand that Executive action cannot do everything legislation can to protect us from cyber attack, but it can do a lot. And as this session of Congress concludes at the end of this year, we have still failed to fix this problem and close some of our vulnerabilities to cyber attack. And I certainly hope the President will step in, along with you, Secretary Napolitano, and act as strongly as you can to protect our country. And I will be asking some questions of you when we get to that point in the testimony.

So I thank you again for being here. I look forward to this hearing every year. It is sometimes unsettling, but it is really important as a report to both Congress and the American people about the status of the current threat to our homeland.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Last week, we observed the 11th anniversary of the horrific attacks of September 11, 2001. We again remembered the victims and the heroes of that day. And we acknowledged the dedicated military, intelligence, law enforcement, and homeland security professionals who have worked together to bring terrorists to justice and to prevent another large-scale attack within the United States. And I want to join the Chairman in thanking each of you for your hard work in that endeavor.

Tragically, however, we have also witnessed violent attacks on the U.S. consulate in Benghazi, Libya, that resulted in the killings of our Ambassador and three other brave Americans. While these attacks remain under investigation, it is difficult not to see shades of the 1998 attacks on our embassies in Kenya and Tanzania, which were among the many precursors to the attacks of September 11, 2001. This tragedy once again underscores the ongoing threat we face, both abroad and at home, from violent Islamist extremists.

In the aftermath of September 11, 2001, we took significant actions to address this threat. When Senator Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), our aim was to improve coordination within the intelligence community and among the key stakeholders at all levels of government. Achieving the goals of this landmark law remains a work in progress.

We know we face a determined enemy. Al-Qaeda in the Arabian Peninsula (AQAP) has tried repeatedly to exploit holes in our security. The failed 2009 Christmas Day bomber used a device specifically designed to avoid detection. The 2010 cargo plot sought to circumvent improvements in passenger screening by targeting cargo. In May of this year, al-Qaeda tried again. The bomb maker apparently sought to avoid the failures of the earlier Christmas Day attack. Through the aggressive efforts of our intelligence community, fortunately this plot was disrupted before it could threaten American lives. Nevertheless, that operation was also plagued by leaks—apparently from within the Executive Branch—that may have undermined future efforts and compromised sources.

Not every threat that we face has been met with sufficient resolve and action. Perhaps the best example, which the Chairman has mentioned, is the ever-increasing cyber threat. Experts have repeatedly warned that the computer systems that run our electric grids, our water plants, financial networks, and transportation systems are vulnerable to a cyber attack that could harm millions of Americans. In fact, rarely has there been such a bipartisan consensus among experts that this threat must be addressed.

Just last week, former Deputy Secretary of Defense John Hamre said that the threats in cyberspace “took a darker turn” this summer, as three very large corporations experienced cyber attacks “designed to damage operations.” Citing government sources, he said that at least two of the attacks may have come from Iran. China and Russia we know have also launched cyber attacks.

To respond to this escalating threat, the Chairman and I have worked during the past 2 years to craft a bipartisan bill that relies

on the expertise of government and the innovation of the private sector. Despite our hard work to find common ground, the Senate has failed to pass cybersecurity legislation. Given the significant damage already done to our economy and our security, as well as our clear vulnerability to even worse attacks, this failure to act is inexcusable.

Former DHS Secretary Michael Chertoff, and former National Security Agency (NSA) and the Central Intelligence Agency (CIA) chief Michael Hayden describe the urgency this way: "We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9/11' hits. It is not a question of 'whether' this will happen; it is a question of 'when.'"

This time all the dots have been connected. This time the warnings are loud and clear, and this time we must heed them.

In contrast to the known threat of cyber attacks, another persistent challenge we face comes from those threats that we fail to even anticipate—what the 9/11 Commission memorably referred to as "a failure of imagination," the so-called black swan events that test our assumptions. These are our most vexing problems because we cannot simply build walls around every potential target. Nevertheless, if we strengthen information sharing and analytic capabilities, our law enforcement and intelligence officers can disrupt even more plots, whether they are ones that we know well are coming or those that we have never before seen.

In my judgment, which is informed by numerous briefings and discussions with experts, the attack in Benghazi was not a "black swan" but, rather, an attack that should have been anticipated based on the previous attacks against western targets, the proliferation of dangerous weapons in Libya, the presence of al-Qaeda in that country, and the overall threat environment.

Whatever the plots hatched by our enemies, I am also concerned about vulnerabilities that stem from our own government's actions or failure to act.

I have already noted what I believe to be the inexplicable lack of security in Benghazi, the grave, self-inflicted wounds from intelligence leaks, and the failure to enact a cybersecurity bill. There is also a genuine danger posed by the automatic, mindless cuts known as sequestration. Absent a commitment by the President and Congress to avoid this disastrous policy, the budget of every Federal agency represented here today—the Department of Homeland Security, the National Counterterrorism Center, and the FBI—the very agencies charged with protecting our Nation from terrorism and other disasters—will be slashed in an indiscriminate way, by 8 percent or more, potentially harming such vital programs as border security, intelligence analysis, and the FBI's work.

At a time when budget constraints require everyone to sacrifice and priorities to be set and waste to be eliminated, we should ask where resources can be spent more effectively and what tradeoffs should be made to balance the risk we face with the security we can afford. What we cannot afford, however, is to weaken a homeland security structure that is helping to protect the citizens of this country.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins. Secretary Napolitano, thank you for being here, and we would welcome your testimony at this time.

TESTIMONY OF HON. JANET NAPOLITANO,¹ SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Thank you, Chairman Lieberman, Senator Collins, and Members of the Committee. And I would also like to thank Associate Deputy Director Perkins and Director Olsen for their partnership.

Mr. Chairman, this is my 17th appearance before you. It is my 44th hearing overall since becoming Secretary of the Department. I am grateful personally for this Committee's tireless advocacy on behalf of DHS, not only during its initial creation but in the time since. Senator, you have been one of our strongest supporters, and our Nation's security has benefited as a direct result. Thank you for all you have done to make the country more secure.

Eleven years after the 9/11 attacks, America is stronger and more secure, thanks to the work of the men and women of DHS; our many Federal, State, local, tribal, territorial, and international partners; and Members of this Committee. And while the United States has made significant progress since the 9/11 attacks, we know that threats from terrorists persist and continually evolve. We face direct threats from al-Qaeda. We face growing threats from other foreign-based terrorist groups which are inspired by al-Qaeda ideology, such as AQAP and al-Shabaab. And we must address threats that are homegrown as well as those that originate abroad.

These threats are not limited to any one individual, group, or ideology. And as we have seen, the tactics employed by terrorists can be as simple as a homemade bomb or as sophisticated as a biological threat or a coordinated cyber attack.

While we deal with a number of threats and threat actors at any given time, three areas merit special sustained attention. The first is aviation. The Christmas Day 2009 plot, the October 2010 air cargo threat, and the AQAP plot earlier this year that would have targeted a U.S.-bound airliner with explosives make clear that commercial aviation remains a target. Terrorists, especially AQAP, continue to seek ways to circumvent existing security measures. Their methods and tactics are sometimes ingenious and increasingly sophisticated.

A second threat area is cybersecurity, as both of you have mentioned. Cyber threats and incidents have increased significantly over the past decade. Our Nation confronts a dangerous combination of known and unknown vulnerabilities in cyberspace: Strong and rapidly expanding adversary capabilities, and limited threat and vulnerability analysis and awareness.

We are committed to working with the Congress to make sure the Department and our Nation have the tools and authorities we need to effectively confront threats to cyberspace, and that includes minimum standards for our Nation's critical infrastructure.

¹The prepared statement of Secretary Napolitano appears in the Appendix on page 40.

We remain hopeful that the Congress can pass strong cybersecurity legislation, and I thank you, Chairman Lieberman and Ranking Member Collins, for your leadership in this area.

The third area of growing concern is homegrown violent extremism. Within the context of U.S.-based violent extremism, we know that foreign terrorists groups affiliate with al-Qaeda and individual extremists are actively seeking to recruit or inspire westerners to carry out attacks against western and United States targets. Importantly, however, as recent events have demonstrated, we also know that violent extremism can be inspired by various religious, political, or other ideological beliefs. Moreover, the attack last week against the U.S. consulate in Libya that took the life of Ambassador Stevens and three other Americans, the terrorist attack in Bulgaria in July, as well as this summer's shootings in Aurora, Colorado, and Oak Creek, Wisconsin, demonstrate that we must remain vigilant and prepared. And certainly our thoughts are with those impacted by these senseless attacks.

How do we mitigate the threat? We mitigate these threats in several ways. First and foremost, we have worked to build a homeland security enterprise that allows DHS and our many partners to detect threats earlier, to share information, to minimize risks, and to maximize our ability to respond and recover from attacks and disasters of all kinds.

With respect to the aviation sector, we have implemented a layered detection system focused on risk-based screening, enhanced targeting, and information sharing, while simultaneously facilitating travel for nearly 2 million domestic air travelers every day.

Following the December 2009 threat, we launched a historic global initiative to strengthen international aviation, which has improved cooperation on passenger and air cargo screening, technology development and deployment, and information collection and sharing, as well as the development of internationally accepted security standards.

As part of this effort, last week, in Montreal, 13 member states of the International Civil Aviation Organization met to reaffirm our commitment to these principles and to continue our progress, including through the development of global air cargo security standards. We have strengthened information sharing with our international partners.

For example, our new and historic passenger name record agreement with the European Union allows us to continue sharing passenger information so that we can better identify travelers who merit our attention before they depart for the United States.

And in addition to our Pre-Departure Targeting Program, Immigration Advisory Program, and enhanced in-bound targeting operations, all of these allow us to more effectively identify high-risk travelers who are likely to be inadmissible to the United States and to make recommendations to commercial air carriers to deny boarding before a plane departs.

And at home, we have continued the deployment of advanced technology at airports, including advanced imaging technology machines, while implementing new programs to make the screening process more efficient for trusted travelers through programs such

as the Transportation Security Administration (TSA) Pre-Check and Global Entry.

Around the cyber domain, we have partnered with sector-specific agencies and the private sector to help secure cyberspace, such as the financial sector, the power grid, water systems, and transportation networks.

We have taken significant action to protect Federal civilian government systems through the deployment of intrusion detection systems like EINSTEIN, greater diagnostic and sharing of threat information, national exercises and incident response planning, public awareness and outreach programs, and a cyber workforce initiative to recruit the next generation of cyber professionals.

And, internationally, we are working with our partners to share expertise, combat cyber crime, and strengthen shared systems and networks.

Finally, we have improved our domestic capabilities to detect and prevent terrorist attacks against our citizens, our communities, and our critical infrastructure. We have increased our ability to analyze and distribute threat information at all levels. Specifically, we have worked to build greater analytic capabilities through 77 designated fusion centers, resulting in unprecedented levels of information sharing and analysis at the State and local level. We have invested in training for local law enforcement and first responders of all types to increase expertise and capacity at the local level.

In partnership with the Department of Justice, we have transformed how we train front-line officers regarding suspicious activities through a nationwide Suspicious Activity Reporting Initiative. And as part of that initiative, we have helped to train over 234,000 law enforcement officials.

We are in the final stages of implementing a Countering Violent Extremism curriculum for Federal, State, local, and correctional law enforcement officers that is focused on community-oriented policing, which will help front-line personnel identify activities that are potential indicators of terrorist activity and violence.

We have also expanded training with respect to active shooter threats, providing a range of information, tools, case studies, and resources to Federal, State, and local partners to help them prepare for and, if necessary, respond to attacks involving active shooters.

And through the nationwide expansion of the "If You See Something, Say Something" campaign, we continue to encourage all Americans to alert local law enforcement if they see something that is potentially dangerous.

In conclusion, DHS has come a long way in the 11 years since September 11, 2001, to enhance protection of the United States and engage our partners in this shared responsibility. Together, we have made significant progress to strengthen the homeland security enterprise, but significant challenges remain. Threats against our Nation, whether by terrorism or otherwise, continue to exist and to evolve, and we must continue to evolve as well. We continue to be ever vigilant to protect against threats while promoting travel and trade and safeguarding our essential rights and liberties.

I thank the Committee for your support in these endeavors and for your attention as we work together to keep the country safe.

Chairman LIEBERMAN. Thanks very much, Secretary Napolitano, for that opening statement, which was a good beginning for us.

Probably most Americans, certainly a large number, know about the Federal Bureau of Investigation and the Department of Homeland Security. Probably very few know about the National Counterterrorism Center, which was created by what I call the 9/11 Commission legislation. But it is really one of the most significant steps forward we have taken in our government. It is the place at which, to go back to language we all used after September 11, 2001, we make sure that the dots are on the same board and can be connected. As a matter of fact, as we have discussed, we have now figured out how to put so many dots on that same board, the challenge now is to see them all and see the patterns and the connections. But I think the folks at NCTC have really taken us a long way, working with the Department of Homeland Security and the FBI. And, Mr. Olsen, I thank you for your leadership and look forward to your testimony now.

TESTIMONY OF HON. MATTHEW G. OLSEN,¹ DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. OLSEN. Thank you, Chairman Lieberman, Senator Collins, and Members of the Committee. I really do appreciate this opportunity to be here this morning.

I also want to express my appreciation to your Committee for its leadership on national security matters and certainly your support of NCTC from its inception. And I thank you for your kind comments this morning about our work, and I accept those on behalf of the men and women at NCTC. And I am also very pleased to be here with Secretary Napolitano and Associate Deputy Director Perkins. We are close partners in the fight against terrorism.

In my brief remarks this morning, I will focus on recent events and highlight a few areas of real key concerns for us, and then I will take a moment to highlight our efforts at NCTC to analyze and share critical threat information.

Certainly the attack on our diplomatic post in Benghazi last week that took the lives of four Americans, including Ambassador Stevens, is proof that acts of terror and violence continue to threaten our citizens and our interests around the world. As the President said of these Americans just this past Friday, they did not simply embrace the American ideal, they lived it.

It is now our responsibility to honor them by fulfilling our mission to combat terrorism and to combat violent extremism. The intelligence community, I can tell you, is working as one to determine what exactly happened in Benghazi, to uncover new threats in the region, and then to identify and bring to justice those who are responsible for this attack.

Last week's attacks I think should be viewed in the context of the evolving threat landscape we face that you have spoken about as well as the ongoing unrest and political transition in the region. More than a decade after the September 11th attacks, we face a dynamic threat from al-Qaeda, from its affiliates, as well as those

¹The prepared statement of Mr. Olsen appears in the Appendix on page 61.

who follow al-Qaeda's ideology. There is no doubt that over the past few years our government, working with our allies, has placed relentless pressure on al-Qaeda's core leadership. We have denied the group safe haven. We have denied the group resources and the ability to plan and train. In short, the intelligence picture shows that al-Qaeda's core in Pakistan is a shadow of its former self.

But even as al-Qaeda's leadership in Pakistan struggles to remain relevant, the terrorist threats we face have become more diverse. Al-Qaeda has turned to other groups to carry out attacks and to advance its ideology. These groups are based in an array of countries, including Yemen, Somalia, Nigeria, and Iraq.

In particular, al-Qaeda in the Arabian Peninsula is the group that is most likely, we think, to attempt attacks against the United States. We saw this in May with the disruption of an AQAP plot to take down an airliner. Other affiliates and related groups, such as al-Qaeda in the Islamic Maghreb, al-Qaeda in Iraq, Boko Haram in Nigeria, as well as militants based in Pakistan, all pose threats to our citizens and interests in those regions of the world.

We are also focused on threats posed by Iran and by Hezbollah. Iran remains the foremost state sponsor of terrorism in the world, and over the past year, the threat from Iranian-sponsored terrorism has increased.

Inside the United States, we remain vigilant to prevent violent extremists from carrying out attacks in the name of al-Qaeda. This past week, the FBI arrested a Chicago man after he allegedly tried to blow up a crowded bar in the city. Also last week, a Federal judge sentenced a Virginia man to 30 years in prison for plotting to bomb the U.S. Capitol. These plots highlight the danger that al-Qaeda inspired extremists pose to our country.

And beyond these threats, we face a period of unrest and a period of transition in the Middle East and in North Africa. The Arab spring or awakening, now in progress for well over a year, has led to fundamental reforms in the region. Al-Qaeda was not part of this change, but the group is seeking to take advantage of the unrest in some areas, seeking to establish safe havens and to recruit extremists where security is diminished.

Now, if I may, turning to the role of the National Counterterrorism Center, Congress and this Committee created NCTC to help lead this effort to combat these threats. Our founding principle is the imperative to integrate all terrorism information and to share that knowledge with those on the front lines of this fight. I will take a few moments to describe the ways in which we are seeking to achieve this goal every day at NCTC.

First, intelligence information and state-of-the-art analysis. NCTC serves as the primary organization in the government for integrating and assessing all intelligence relating to international terrorism. We have a unique responsibility to examine all terrorism issues, spanning geographical boundaries to identify and analyze threat information, regardless of whether that information is collected inside or outside the United States.

At NCTC, our culture is defined by collaboration. Nearly every NCTC analytic product is coordinated throughout the intelligence community. It therefore reflects multiple perspectives for policy-maker and operators alike.

Second, access to data and technological innovation. We are promoting information integration and sharing with the development of a Counterterrorism Data Layer. This approach to data allows our analysts to access terrorist information that we have collected from across the government in a single place, and it allows us to do that without having to manually search multiple networks.

Here, if I may, I would like to make a point about the Foreign Intelligence Surveillance Act (FISA) Amendments Act, a law that is set to expire at the end of this year. As this Committee knows, this law authorizes the government to collect valuable intelligence involving international terrorists and other enemies by targeting non-Americans who are overseas. These provisions were carefully crafted and carefully implemented to protect the privacy and civil liberties of Americans and should remain law.

Third, NCTC has enhanced its focus on tactical intelligence and developing leads involving threats to the United States. We established a Pursuit Group—analysts from across the counterterrorism community who have unparalleled data access and expertise. Their mission is to focus on information that could lead to the discovery of threats, to connect those dots, and to identify actionable leads for agencies such as the FBI, the Department of Homeland Security, and the CIA.

Finally, NCTC provides situational awareness and intelligence support to the broad counterterrorism community. Our Operations Center, which is collocated with the FBI's Watch, provides around-the-clock support to counterterrorism agencies. We also maintain the government's central repository for terrorist identities. This enables us to provide near-real-time watchlisting data to support screening and law enforcement activities across the government.

In addition, the Interagency Threat Assessment and Coordination Group (ITACG), which is located at NCTC and is led by senior DHS and FBI officers, brings Federal and State and local officers together in one place at NCTC. This group is dedicated to providing relevant intelligence on terrorism issues to State, local, tribal, and private sector partners, helping to ensure that information is shared with public safety officials, including police officers and firefighters. Faced with the possible loss of funding, we are working closely with DHS and FBI to retain this capability. Mr. Chairman, you have been a strong supporter of ITACG and have noted its successes, and I am personally committed to working with DHS and FBI to sustain this initiative, to find ways to do so in a cost-effective way, and we are working closely together to chart a way ahead.

I just want to close by identifying our most important assets, and that is our people. NCTC is working to meet the many challenges ahead, but that effort is really dependent on our diverse and dedicated workforce. Maintaining this workforce—through the continued commitment and support of agencies like DHS, the FBI, and other organizations—is a priority for me at the center.

Mr. Chairman, Senator Collins, Members of the Committee, thank you again for the opportunity to speak with you this morning, and thank you for your continued support of NCTC. I look forward to answering your questions.

Chairman LIEBERMAN. Thank you, Director Olsen.

Associate Deputy Director Perkins, thanks again for being here, and we welcome your testimony now.

TESTIMONY OF KEVIN L. PERKINS,¹ ASSOCIATE DEPUTY DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE ON BEHALF OF HON. ROBERT S. MUELLER III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. PERKINS. Good morning, Chairman Lieberman, Senator Collins, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI. I also want to thank Secretary Napolitano and Director Olsen and the men and women they lead in our joint fight against those seeking to do harm against U.S. citizens here and around the world.

As you know, the Bureau has undergone unprecedented transformation in recent years. Since the attacks of September 11, 2001, we have refocused our efforts to address and prevent emerging terrorist threats. The terrorist threat is more diverse than it was 11 years ago, but today, we in the FBI are in a better place to meet that threat.

We also face increasingly complex threats to our Nation's cybersecurity. Nation-state actors, sophisticated organized crime groups, and hackers for hire are stealing trade secrets and valuable research from America's companies, universities, and government agencies. Cyber threats also pose a significant risk to our Nation's critical infrastructure.

As these threats continue to evolve, the FBI must continue to adapt to counter those threats. We must continue to build partnerships with our law enforcement and private sector partners, as well as the communities we serve. Above all, we must remain firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the people we serve.

Counterterrorism remains our number one priority. We face a fluid, dynamic, and complex terrorist threat. We have seen an increase in the sources of terrorism, a wider array of terrorism targets, a greater cooperation among terrorist groups, and an evolution in terrorist tactics and communications methodologies.

In the past decade, al-Qaeda has become decentralized, but the group remains committed to high-profile attacks against the West. Al-Qaeda affiliates and surrogates, especially al-Qaeda in the Arabian Peninsula, now represent the top counterterrorism threat to the Nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009 and the attempted bombing of U.S.-bound cargo planes in October 2010.

We also remain concerned about the threat from homegrown violent extremists. Over the past years, we have seen increased activity among extremist individuals. These individuals have no typical profile; their experiences and motives are often distinct. Lone offenders, some of whom may have some affiliation with known domestic terrorist organizations, present a special challenge. They

¹The prepared statement of Mr. Perkins appears in the Appendix on page 73.

may be self-trained, self-financed, and self-executing. They are sometimes motivated to take action in furtherance of their ideological beliefs, but they stand on the periphery and are hard and difficult to identify.

Unfortunately, we have recently seen a number of lone offender incidents, as we have recently witnessed the shooting at the Sikh Temple in Wisconsin.

Now, as this Committee knows, the cyber threat has evolved and grown significantly over the past decade. Foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property—information that can improve the competitive advantage of state-owned companies.

Unlike state-sponsored intruders, hackers for profit do not seek information for political power; rather, they seek information for sale and trade to the highest bidder. In some cases, these once isolated hackers have joined forces to create criminal syndicates. Organized crime in cyberspace offers a higher profit with a lower probability of being identified and prosecuted. And hackers and hactivist groups such as Anonymous and Lulz-Sec are pioneering their own forms of digital anarchy.

With these diverse threats, we anticipate that cybersecurity may well become our highest priority in the years to come. That is why we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11 attacks.

We are focusing our Cyber Division on computer intrusions and network attacks. We are also hiring additional computer scientists to provide expert technical support to critical investigations ongoing in the field.

As part of these efforts, we are expanding our cyber squads in each field office to become Cyber Task Forces that will be focused on intrusions and network attacks.

We are also working with our partners to improve on the National Cyber Investigative Joint Task Force (NCIJTF)—the FBI-led multi-agency focal point for coordinating and sharing of cyber threat information. The NCIJTF brings together 18 law enforcement, military, and intelligence agencies to stop current and predict future attacks.

As we have in the past, we will be inviting the participation of our Federal, State, and local partners as we move forward with these initiatives. As we evolve and change to keep pace with today's complex threat environment, we must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution. Following the rule of law and upholding civil liberties—these are not burdens. These are what make all of us safer and stronger.

Chairman Lieberman and Senator Collins, I thank you for this opportunity to discuss the FBI's priorities and the state of the Bureau as it stands today. Mr. Chairman, let me again acknowledge the leadership that you and this Committee have provided to the FBI. The transformation of the FBI over the past 11 years would not have been possible without the support of Congress and the

American people. I would be happy to answer any questions you may have at this time, sir.

Chairman LIEBERMAN. Thanks very much, Associate Deputy Director Perkins. It has been a privilege to work with the FBI and the other agencies here.

We will do a 7-minute first round of questions. Let me focus in on the recent wave of protests throughout large parts of the Muslim world, but also the attacks in Benghazi. Director Olsen, let me begin with you and see if you can help us separate this out. It certainly seems to me that there were a series of protests that were set off as a result of this film, and I will get back to that, but what happened in Benghazi looked like a terrorist attack. The NCTC uses the definition of terrorism, which I think is a good one, as "politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents."

So let me begin by asking you whether you would say that Ambassador Stevens and the three other Americans died as a result of a terrorist attack.

Mr. OLSEN. Certainly, on that particular question, I would say yes, they were killed in the course of a terrorist attack on our embassy.

Chairman LIEBERMAN. Right. And do we have reason to believe at this point that the terrorist attack was sort of pre-planned for September 11, or did the terrorists who were obviously planning it—because it certainly seemed to be a coordinated terrorist attack—just seized the moment of the demonstrations or protests against the film to carry out a terrorist attack?

Mr. OLSEN. A more complicated question and one, Mr. Chairman, that we are spending a great deal of time looking at even as we speak, and obviously the investigation here is ongoing and facts are being developed continually.

The facts that we have now indicate that this was an opportunistic attack on our embassy. The attack began and evolved and escalated over several hours. I said "our embassy." It was our diplomatic post in Benghazi. It appears that individuals who were certainly well armed seized on the opportunity presented as the events unfolded that evening and into the morning hours of September 12.

We do know that a number of militants in the area, as I mentioned, are well armed and maintain those arms. What we do not have at this point is specific intelligence that there was a significant advanced planning or coordination for this attack. Again, we are still developing facts and still looking for any indications of substantial advanced planning. We just have not seen that at this point.

So I think that is the most I would say at this point. I do want to emphasize that there is a classified briefing for all of Congress that will take place tomorrow.

Chairman LIEBERMAN. Right. We will be there. Let me come back to what you said, that there was intelligence, as you indicated broadly a moment ago, that in eastern Libya, in the Benghazi area, there were a number of militant or violent Islamist extremist groups. Do we have any idea at this point who was responsible among those groups for the attack on the consulate?

Mr. OLSEN. This is the most important question that we are considering.

Chairman LIEBERMAN. Right.

Mr. OLSEN. We are focused on who was responsible for this attack. At this point, what I would say is that a number of different elements appear to have been involved in the attack, including individuals connected to militant groups that are prevalent in eastern Libya, particularly in the Benghazi area. As well, we are looking at indications that individuals involved in the attack may have had connections to al-Qaeda or al-Qaeda's affiliates, in particular al-Qaeda in the Islamic Maghreb.

Chairman LIEBERMAN. Right. So that question has not been determined yet whether it was a militant Libyan group or a group associated with al-Qaeda and influence from abroad.

Mr. OLSEN. That is right, and I would add that the picture that is emerging is one where a number of different individuals were involved, so it is not necessarily an either/or proposition.

Chairman LIEBERMAN. OK, good.

Mr. OLSEN. Again, as you know, the FBI is leading the investigation, and that is ongoing.

Chairman LIEBERMAN. Yes. I wanted to go to you now, Associate Deputy Director Perkins, and ask you about that. What is the status of the FBI investigation into the attack on our consulate in Benghazi, Libya?

Mr. PERKINS. Yes, Mr. Chairman, as Director Olsen noted, we have an open investigation at this time. We have a significant number of FBI agents, analysts, and various support employees assigned to this matter. We are conducting interviews, gathering evidence, and trying to sort out the facts. We are working with our partners, both from a criminal standpoint as well as in the intelligence community, to try to determine exactly what took place on the ground that evening.

Chairman LIEBERMAN. Secretary Napolitano, let me go to you, I know that last Thursday the Department of Homeland Security and the FBI released a bulletin indicating that this film was the apparent catalyst for these protests and that the fact could increase the risk of violence here in the United States and could motivate homegrown violent extremists, certainly with their recruitment efforts and perhaps with actions.

I wonder if in this setting you could comment on the state of your concern about that and what steps DHS and the FBI are taking, along with other government agencies, to proactively address the potentially higher risk of homegrown terrorist acts as a result of the film?

Secretary NAPOLITANO. Right now, Mr. Chairman, we have no intelligence of impending violent attacks within the United States. There is open source information on some planned demonstrations in, I believe, Los Angeles and Houston, among other places. Those are posted on the Web. But we have no indication of anything that is violent in nature.

Nonetheless, immediately after the attack in Benghazi, we began outreach to a number of groups within the country, faith-based groups and others, who could be the target of a violent attack and provided them with guidance on things they can do to make sure

they are as safe as possible. So we continue that outreach. We continue working with our local partners in terms of what they are seeing on the ground and then monitoring the open-source media.

Chairman LIEBERMAN. Thank you. Let me ask you finally what we as a government can do to counteract the impact of this film. You know, we are a country of almost 310 million people now. This film, hateful really, was done by a handful of people. And yet American embassies and consulates not only are the subject of protests, which is very much in the American spirit of civil protest and right of free speech, but going beyond that to destruction of property and, at its worse, a terrorist attack in Benghazi that kills four people. In one other case, I believe in Yemen, the demonstrators were armed. And, of course, in some cases, including Tunisia, the local police or security forces actually ended up having to fire at crowds to stop them from doing further damage.

I know this is very sensitive, but we have to ask our friends in the Muslim world and ourselves to be willing to say this film does not represent us and, therefore, it is simply unacceptable, even if you are offended by the film, which we understand, to do more than protest, to begin to act violently. It is no more acceptable than it would be in this country if some group seized on the statements of a fringe religious leader or a political leader in some foreign country that attacked Americans, Christians and Jews, and as a result some group in America started to not just protest but to attack the embassy of the country in which that happened. In other words, we have to blow the whistle on this behavior. Fortunately, we have had some help from our allies in countries like in the governments of Libya and Tunisia, and I think we have to be forthright in doing that ourselves. So with apologies for the length of the question and the opportunity I took to get a little bit off my chest, I wonder if any of you could tell us what our government is trying to do now to challenge people in the Muslim world to confront the reality that this film is not representative of America or the American Government?

Secretary NAPOLITANO. Mr. Chairman, the film is absolutely not representative of America or the American Government. It is deplorable. The issue you raise is a difficult one. We are a country where people have rights, and one of the rights they have is to have free speech, and that can include things we find deplorable as well as other things.

So we also recognize that there is a right to assembly, a right to petition the government, so we recognize the right to have a peaceful demonstration against deplorable speech.

What we need to keep communicating is, as deplorable as we find that film to be, it is not, and never will be an excuse for violence and for the senseless killing we saw in Benghazi and other places. And we need that voice to come loud and clear, not just from Washington but from the country as a whole and internationally, and it needs to come from people of all faiths.

Chairman LIEBERMAN. Thank you very much. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. Mr. Olsen, I want to follow up on the series of questions that the Chairman raised

with you about the attack in Benghazi that cost the lives of four Americans.

First, I will tell you that, based on the briefings I have had, I have come to the opposite conclusion and agree with the President of Libya that this was a premeditated, planned attack that was associated with the anniversary of September 11, 2001. I just do not think that people come to protests equipped with rocket-propelled grenades and other heavy weapons. And the reports of complicity—and they are many—with the Libyan guards who were assigned to guard the consulate also suggest to me that this was premeditated.

Nevertheless, I realize that is something you are still looking at, the FBI is still looking at, but I for one believe that the very forthright conclusion by the President of Libya is more likely the correct one.

But putting aside the issue of whether this was an opportunistic attack or a premeditated one, the issue of the security of the consulate in what by any measure has to be considered a dangerous threat environment continues to trouble me. It is clear that the security situation in Benghazi was deteriorating given that there were at least four attacks that I am told about, beginning in June, on diplomatic and western targets. We are also all aware that Libya is awash in heavy weapons. I think there are something like 10,000 man-portable air-defense systems, maybe 20,000, that are still missing.

We also know that it is a bastion for extremist groups, including offshoots of al-Qaeda. We know that the No. 2 person in al-Qaeda was a Libyan who was killed. The Libyan government is having a hard time controlling its borders, getting the militias under control. And even this week, the FBI team investigating the attack had difficulties getting to Libya safely because of the security situation.

So given these facts, how would you personally have assessed the general threat environment prior to the attacks on our diplomats in Benghazi and the former Navy SEALs?

Mr. OLSEN. Well, Senator Collins, I would agree with your characterization of the threat pretty much as you laid it out. So the threat in Libya from armed militant groups, from al-Qaeda-affiliated individuals was high, and that made Libya in some ways very similar to other countries in the region, and certainly similar to parts of Egypt and to northern Mali. We are concerned about Nigeria.

So the region, particularly those countries following the Arab spring, are faced with real challenges from a security perspective. So we are, again, working with our partners, both in the Federal Government here but also with the governments in the region, seeking to increase the security capabilities of those as well as, of course, cooperating with them to look at specific threats or attacks, such as the investigation that is on going in Libya.

Senator COLLINS. Was there any communication between NCTC and the State Department alerting them to the high-threat environment in which Benghazi was located and suggesting that be considered as the State Department evaluated its security?

Mr. OLSEN. So over the course of the last several months, again, you highlighted particularly events in June of this year, we know that there was a small-scale attack on our mission, our post in

Benghazi in June. We also know that there was a more sophisticated attack involving the convoy with the British ambassador in Benghazi. So there were reports detailing those attacks and detailing generally the threat that was faced to U.S. and Western individuals and interests in eastern Libya from, again, armed militants as well as elements connected to al-Qaeda.

There was no specific intelligence regarding an imminent attack prior to September 11 on our post in Benghazi.

Senator COLLINS. Were there any indications that there were communications between extremist elements and the guards, the Libyan guards that were assigned to the consulate?

Mr. OLSEN. In the immediate aftermath—or prior to the—

Senator COLLINS. Prior to the attack.

Mr. OLSEN. That question I think would be better addressed in the session that we are going to have tomorrow.

Senator COLLINS. It just concerns me so gravely that there were not marines present in Benghazi to defend the consulate, and as I have been looking further into this issue, I am learning that the situation is far more common than I would have thought. We are relying on foreign nationals, perhaps on a British security firm that has been told to be unarmed, and other more questionable and less secure means of protecting our American personnel in extremely dangerous parts of the world. And I am just stunned and appalled that there was not better security for all of the American personnel at that consulate given the high-threat environment.

I know you are not in charge of assigning security. You do communicate information to the State Department about the threat. Can you enlighten me at all on why decisions were made to have virtually no security?

Mr. OLSEN. I would say that we do as a community provide as much information as we possibly can in as timely a way as possible with the State Department as well as the rest of the Federal Government. I would say this: We do rely on host countries to help protect our diplomatic personnel in those countries. But I think that the ultimate question that you have asked of the decisions about the security at our post in Benghazi would be better addressed to the Diplomatic Security Service within the State Department.

Senator COLLINS. Mr. Perkins, is your FBI team looking at security as well as trying to better understand how the attack came about and whether or not it was premeditated?

Mr. PERKINS. Yes, Senator. Let me start by saying I share your specific concerns regarding the security. In Libya, as well as on a larger scale, we have FBI employees posted around the world and in many places that have higher-than-usual security concerns. We need to do that to carry out our mission every day in the counter-terrorism environment.

But with regard to the specifics within Benghazi, within Libya itself, we are counting on our investigators on the ground to be able to sort that out, obviously, to gather the facts, go where the facts take us, and then on the back end to be able to work with the State Department, with Diplomatic Security's Regional Security Office, and others to share whatever it is we have found that may be of benefit to providing better security for the people on the ground.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

I do want to say for the record that last Friday, Senator Collins and I addressed a request to the Inspector General at the Department of State to do an investigation of what happened with regard to security at our consulate in Benghazi prior to these deadly attacks, and then to draw conclusions or lessons learned that might relate to provision of security generally, particularly at non-embassy locations throughout the world.

The other thing I would say, although I understand you have a respectful disagreement on the question of whether the attack that resulted in the four American deaths in Benghazi was pre-planned for that day or a spontaneous taking advantage of the protests that were going on, I do appreciate the fact, Director Olsen, that you as the head of the National Counterterrorism Center have told the Committee this morning without hesitation that you believe what happened in Benghazi was a terrorist attack. There seemed to be a little confusion about that over the last few days. And, of course, I could not agree with you more and will await your conclusion of the investigation as to whether you think it was pre-planned for that day or just spontaneous.

My own inclination is to agree with Senator Collins, as I usually do, but I will await the investigation.

In order of importance, we have Senators Moran, Akaka—did I say “importance”? [Laughter.]

I take that back because Senator Akaka is the most important Senator. But in order of appearance, Senators Moran, Akaka, Pryor, and Carper.

Senator MORAN. I very much appreciated your original comment, Mr. Chairman, but have great deference and respect for the Senator from Hawaii and recognize his importance.

Chairman LIEBERMAN. Thank you.

OPENING STATEMENT OF SENATOR MORAN

Senator MORAN. What a difficult hearing with so many topics and how the world changes so often and so rapidly. So I thank the Chairman and the Ranking Member for hosting this hearing, and I appreciate our three witnesses and express my gratitude for the efforts that are being made to make certain that Americans remain safe and secure around the world.

I need to focus my attention, Madam Secretary, as you would expect, on a conversation that we constantly have, and it deals with the threat of biological weapons, either intentional or inadvertent. For a long time, the Department of Homeland Security has been the lead department in developing a bioscience and agrosience facility, and I think all the hurdles that have been placed in making progress in the completion of this facility have now been completed with the National Academy of Sciences report that was released in July.

You and I had a conversation in early August about the Office of Management and Budget. I would like to thank you personally for the graciousness and kindness that you have always demonstrated toward me in our conversations and your interest in this topic and in seeing a good conclusion to this facility being built. Every time you have testified, and every time I have asked you

questions, you have expressed your support not only for the facility but for the location and the process by which that site location was made.

I think we are at the point now, Madam Secretary, at which there is no reason for you, your Department, not to allow the facility to proceed. There is a lot of uncertainty now with the contractors that are on site and when their contracts expire, and all money that has been spent on this facility to date has been from the State of Kansas, and the Congress has appropriated \$40 million for use in the utility plant and another \$50 million to begin construction. It seems clear to me that whether or not those dollars are available for those purposes rests in your hands. It would require also in addition to the money that the land be transferred. I think that also rests at your desk. And my question, I guess, is to be broadly asked: Now what, Madam Secretary? As we know, the construction timetable only becomes more expensive. We know the need for the facility, and I am not certain how long the contractors have a purpose for being on site if you do not release the funds. And I think Kansas has indicated its strong commitment to this process, is willing to continue to provide resources, work with you to accomplish that. But in the absence of a land transfer, I think our confidence that something is going to happen here, that our money is being well spent is greatly diminished.

And so my question is, Madam Secretary, now what?

Secretary NAPOLITANO. Well, you are right, Senator Moran. We have had a number of things to accomplish as predicates to being able to move forward with the National Bio and Agro-Defense Facility (NBAF), the most recent being the National Academy of Sciences' analysis. I think from all the studies, all the analyses, I think they confirm a couple of basic facts.

One is we need a Bio Level 4 laboratory for this there. It is an essential part of our security apparatus, as it were.

Two, the current facility at Plum Island is inadequate as a substitute, although it will have to serve as a bridge and some monies will have to be invested there to allow it to do so while we move forward with the NBAF.

Three, as you say, I think it is time that we begin moving forward with the land exchange and the Central Utility Plant (CUP). Before we do so, I hope to host a meeting with the Kansas delegation and perhaps the governor to talk about out-year funding, cost shares, and some of the things that Kansas has mentioned they are willing to contemplate. But the \$40 million for the CUP has been held in our fiscal year 2012 budget. We have a fiscal year 2012 budget, so we can move ahead. So we will be in touch with your office about when we want to have such a meeting.

But I think it is necessary for the country, and I think it is time to fish or cut bait.

Senator MORAN. Madam Secretary, I always appreciate what you say, and you expressed sentiments that I was pleased to hear. What I would follow up with is you indicate now is the time. What is the definition of "now is the time"? From many of our perspectives, now is the time has been true for a long time. And, again, let me see what your understanding is of what happens on some date, September 30 or October 30, when the contracts have expired

and the contractors leave. We would hate to have to rebid this, so I think when you say the time is now, it is not a matter of many months. It is a matter of a few weeks before this needs to happen.

Secretary NAPOLITANO. That is right.

Senator MORAN. Is that true?

Secretary NAPOLITANO. Yes, that is my understanding as well. I know some of you will be back in your home States, but it could be done by conference call or people can come back here. But I would hope to pull together something in the next couple of weeks.

Senator MORAN. Madam Secretary, I spoke with Governor Brownback last evening and I spoke again with him on the phone this morning during this hearing. His request of me is to tell you that he will be on a plane today or tomorrow, at your earliest convenience, to reach an agreement in which you will sign the transfer—

Secretary NAPOLITANO. Exchange, yes.

Senator MORAN [continuing]. And release the \$40 million.

Secretary NAPOLITANO. We will be in touch with your office over the next few days to schedule such a meeting.

Senator MORAN. I appreciate that. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Moran.

And now, Senator Akaka. If I may on a point of personal privilege before I call on Senator Akaka, this happens to be the day on which Senator Akaka will chair the last hearing of his Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia this afternoon. Senator Akaka has really given extraordinary leadership to this Committee and worked particularly in a way that really is unsung but very important on human capital management in the Federal workforce.

Senator Akaka will be concluding 36 years of service to the people of Hawaii, 22 in the Senate, 13 in the House, and retiring at the end of this year to spend more time with what I take to be the three great loves of his life: His beloved wife, Millie, his family, and the island paradise of Hawaii. Senator Akaka and his wife, Millie, have four sons, one daughter, 15 grandchildren, and 16 great-grandchildren. Not bad. He is much loved here in the Senate and in Hawaii. He has accomplished an enormous amount in his time here. I want to just express to him not only my gratitude for his friendship and what an honor it has been to serve with him, but as the Chairman of the Committee to thank him for his steadfast and principled work on this Committee year in and year out.

And since we are going out together, so to speak, at the end of this term, one of the benefits I hope, Senator Akaka, is that I will have time to visit you in Hawaii more often, and expecting that, I will, just as I turn it over to you, say, "Aloha pumehana." Not bad for a Yankee from New England. [Laughter.]

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. That is terrific. Thank you very much, Mr. Chairman, and thank you for your words. I am glad that we are stepping out of the Senate together, and I have enjoyed working with you very much throughout the years. I want to thank you and Senator Collins for your leadership on this Committee and in the Senate. You continue to do great work, so thank you very much,

Mr. Chairman, for your words. And thank you so much for holding this timely hearing.

I want to join all Americans in mourning the loss of the four brave and dedicated American public servants who died as a result of what we consider senseless attacks in Libya last week. I honor them and the thousands of civilian Federal employees overseas who risk their lives every day in service to this country. We all owe a debt of gratitude to those that have made essential contributions to fighting terrorism. In the face of domestic and international threats, we really rely on these workers to keep us safe, and we will continue to try to help these workers.

Also, I want to commend the Departments of our witnesses for your increased efforts for protecting our Nation against terrorist attacks and for your partnerships that you have been bringing about so that we can have the best kind of efforts made for our country, and also for the training of 230,000 law enforcement officials to help in this effort. And I want to commend you for all of that.

At my request, I want to tell the panel, the Government Accountability Office (GAO) issued a report last week that highlighted troubling vulnerabilities in the security of radiological materials used at medical facilities across the country. Terrorists could steal these materials to build a dirty bomb that would have devastating social and economic consequences.

What is your reaction to this report of GAO? And what are the current threats regarding terrorists' acquisition of radiological materials?

Secretary NAPOLITANO. Senator, I will start and, again, thank you for your years of service to the country.

With respect to that report, it is primarily medical radiological material. The Department of Energy has the responsibility for the security of that material and how it is handled, so we are reaching out to them to see what steps they intend to take with respect to those medical materials. And we will be happy to report back to you.

Senator AKAKA. Any further comments? Mr. Olsen.

Mr. OLSEN. Senator, as well I would like to thank you for your years of service.

In answer to your question, what I would say as a general matter is that we do have at NCTC a significant element within our organization of analysts who are focused solely on radiological, chemical, and biological weapons, and the possibility of terrorists obtaining and using those. And we work closely with the National Counterproliferation Center in that regard, as well as with our domestic partners represented here, and the CIA and other agencies that focus overseas. It is obviously a significant concern for us, and so I will look forward to working, again, with Secretary Napolitano and the FBI on this issue.

Senator AKAKA. Thank you very much, Director. Mr. Perkins.

Mr. PERKINS. Yes, Senator, and I, too, congratulate you on your years of service to the country.

I reflect what Madam Secretary and Director Olsen both stated. We have a Weapons of Mass Destruction Directorate that works closely with the Department of Energy, with components of DHS, as well as NCTC, in tracking, following, and in trying to be in a

mode where we are able to detect any thefts along those lines. We will have to have some time to review the actual aspects of the GAO report and could get back to you on that. But we work closely with our counterparts in these agencies as well as the Department of Energy to mitigate those threats.

Senator AKAKA. Well, thank you again for your partnerships. It really shows. As you know, Secretary Napolitano, the Senate failed to pass comprehensive cybersecurity legislation prior to the August recess. Because the prospects of enacting legislation this year are dim, I support the President's use of his authorities to improve cybersecurity of the Nation's critical infrastructure such as the power grid.

What are the contours of the Executive Order currently under consideration? And when do you expect it to be issued?

Secretary NAPOLITANO. Senator Akaka, there is an Executive Order that is being considered. It is still being drafted in the inter-agency process, but I would say that it is close to completion pending a few issues that need to be resolved at the highest levels. And, of course, the President will need to be involved. It is perhaps easier to say what cannot be in an Executive Order as opposed to what can be in an Executive Order.

We still need cyber legislation. We still need the congressional action and appreciate the efforts everyone has made in this regard. This is something that the Congress should enact in a comprehensive fashion. We have come close, but we have not been able to get across the goal line here. But it remains an urgent need.

There are at least three things I can think of just off the top of my head that an Executive Order cannot solve. One is it cannot solve some of the limitations we have on personnel, personnel hiring and salaries, and how that works. It cannot solve issues about liability protections, which are often viewed as a mechanism to foster timely and effective information sharing. And we cannot without legislation increase criminal penalties for the bad actors that we find or the FBI finds. So those are at least three important areas that even a robust Executive Order would not be able to cover.

Senator AKAKA. Well, thank you very much. My time has expired, Mr. Chairman. Thank you.

Chairman LIEBERMAN. Thanks, Senator Akaka.

Let me pick up on the last round of questioning by Senator Akaka. I appreciate that report, Secretary Napolitano, and I am glad that the Administration is going forward with a sense of urgency about this because it is possible that we will be able for a variety of reasons to adopt cybersecurity legislation in the lame-duck session. But I agree with Senator Akaka. Based on what we have been through up until now, I would not count on it. I will be, obviously, quite pleasantly surprised if we are able to find common ground. And we are still working on it. We still have bipartisan discussions going on.

But with that probability of the failure of Congress to adopt the Cybersecurity Act of 2012 or something like it, I think the sooner the Executive Branch is ready to try to fill whatever gaps it can, the safer the country will be. So I appreciate that, and I certainly take this to be what the pace of work in the Administration is, so

I am not saying anything that is at odds with it. But I certainly would not wait to see how the lame-duck session works out. In other words, if we get something passed, then it will presumably overcome the Executive Order. And as you said, there are at least those three matters that are in legislation that the President cannot adopt by Executive Order.

I assume, but I look for reassurance now, that you and the Department of Homeland Security are quite actively involved since you are charged with the unique responsibility for cybersecurity in the construction of a possible Executive Order or orders regarding cybersecurity.

Secretary NAPOLITANO. Mr. Chairman, yes, we have been very actively involved, as have some of the other agencies who have primary responsibility in this area. One of the benefits of the legislation, even though it did not pass, is it helped to begin educating people as to the really considerable civilian cyber responsibilities and capabilities that are already being exercised by the Department of Homeland Security. And I think that any Executive Order will reflect that as well.

Chairman LIEBERMAN. That is good. Even though we ended up with a proposal that would have made compliance with the standards voluntary—and I understand the President by Executive Order cannot make them mandatory—but we looked at the possibility that under existing statutory authority, various regulatory agencies might have the existing authority to make whatever standards emerged mandatory on the sector of the economy that they oversee. Do you know whether the Executive Order is considering that possibility?

Secretary NAPOLITANO. Mr. Chairman, without talking in detail because things are still in draft.

Chairman LIEBERMAN. Sure.

Secretary NAPOLITANO. But I can tell you that there has been a deep dive into sector-specific analysis as to where there may already exist some powers.

Chairman LIEBERMAN. That is good to hear. I am encouraged by that.

Let me give you an opportunity one more time to rebut what seems to be driving a lot of the opposition to the bill, which is that this would be the heavy hand of government over the private sector that controls critical cyber infrastructure. Even though in the non-cyber infrastructure or primarily non-cyber, the 18 areas that are designated now which DHS has authority over, you are working really quite constructively and collaboratively, I gather, with the private sector in each of those areas. So what more do you think you and we can do to reassure the private sector that this is intended to be collaborative, not coercive.

Secretary NAPOLITANO. Well, I think, Mr. Chairman, we need to continue to remind them that past is prologue to the future; that we have worked collaboratively on a number of areas outside of cyber affecting critical infrastructure; and that they themselves benefit if there are shared standards. And, quite frankly, with respect to core critical infrastructure, many businesses, communities, and families rely on that core infrastructure to be safe and secure. So that in and of itself I think elevates this to a different plane.

We want to be collaborative. We think that is the way to go. It is truly public-private in contemplation and in current activity. But, again, a significant gap anywhere respecting core critical infrastructure can have ripple effects far beyond the individual entity that is the controller.

Chairman LIEBERMAN. Agreed. Associate Deputy Director Perkins, do you want to add anything? The FBI has developed really impressive cybersecurity capacities, obviously particularly with regard to domestic law enforcement. I take it you two are involved in the construction of a possible Executive Order?

Mr. PERKINS. Yes, Mr. Chairman, that is correct. We are working with our partners at DHS to effect that end, and I echo to some degree what Secretary Napolitano was talking about as far as the efficiency. We have to have the partnerships to make things work. In many of the things the FBI does, partnerships make our work efficient. In the world of cyber crime and cyber threat, partnerships are essential, more than efficient. They have to be there in order for us to carry out our mission.

So looking at the past, looking at the success we have had with the partnerships with the private sector, we hope to play on that going forward to win the confidence and to get this type of partnerships, whether it be through legislation or Executive Order, in place that could benefit our ability to carry out our mission.

Chairman LIEBERMAN. My staff just handed me a note that said that Reuters news service is just reporting that the Bank of America's Web site has suffered intermittent problems amid threats on the Internet that a group was planning to launch cyber attacks on the bank and the New York Stock Exchange, again, in retaliation for this film. Do any of you know anything about that at this point?

Secretary NAPOLITANO. Mr. Chairman, there has been some ongoing activity, and whether it is retaliatory I do not think has been determined. Without going into more, I will just simply say that this is an example of where working public to private and private to public benefits everybody.

Chairman LIEBERMAN. Yes. Director Olsen or Associate Deputy Director Perkins, do you want to add anything?

Mr. OLSEN. I would just add, we were familiar with these reports as of last night, and so there have been ongoing efforts in this regard.

Mr. PERKINS. Yes, sir, that is accurate. We are working with DHS on that matter, but beyond that point right now I really cannot share a great deal of detail on it as we look into it.

Chairman LIEBERMAN. Good enough. It does make the point. Again, this is a news story that I am going from, but you have given some legitimacy to parts of it, although not clearly to whether it is related to the film. But it does make the point that we have been trying to make in the cybersecurity legislation that we are in an unusual circumstance now where the target of an attack by an enemy, whether a nation-state or a terrorist group, would just as likely, in some senses more likely, be privately owned cyber infrastructure that controls some significant part of life in America as opposed to attacking a military target or a government Web site or something of that kind.

I want to move to another area, and that is, the extent to which over the last year or so the Iranian Revolutionary Guard Corps (IRGC) and Quds Force from Iran and its clients, including particularly Hezbollah, have attempted to perpetrate a number of terrorist attacks in countries around the world, again, most recently the successful terrorist attack on a tourist bus in Bulgaria. But, obviously, again, we know that last year the government of Iran apparently attempted to carry out an attack here in Washington against the Saudi ambassador to the United States using someone they believed to be a member of a Mexican drug cartel.

I wanted to ask the three of you—first, to put this into context—my impression is that the Iranian Revolutionary Guard Corps and the Quds Force have made a strategic decision to move out of their immediate neighborhood and to begin to operate internationally. Am I correct on that, Director Olsen?

Mr. OLSEN. What I would say, Mr. Chairman, is that we have seen an uptick in operational activity by the Iranian Revolutionary Guards Force and the Quds Force over the last year or so. And certainly to your point, the plot against the Saudi ambassador here in Washington last fall highlighted a willingness of Iran and its terrorist elements to actually carry out or seek to carry out an attack inside the United States.

Chairman LIEBERMAN. Right. And what I am wondering is am I right—my impression certainly is that whereas traditionally the IRGC and the Quds Force have operated within the Middle East through Hezbollah—perhaps sometimes Hamas, certainly Hezbollah—and Iraqi Shia militias in, obviously, Iraq, that now they seem to be spreading out more broadly. The two cases we know are the United States and Bulgaria.

Mr. OLSEN. I would say that your impression is consistent with my own insofar as certainly we have seen Iranian influence in Iraq and in Afghanistan. But we have also seen links between Iran and terrorist operations in India, Thailand, and Georgia. So it is a threat that is posed beyond the immediate region of Iran.

Chairman LIEBERMAN. So let me ask any of you to what extent now this expansion of terrorist activity sponsored by the Iranian government rises as a threat to our homeland among the other terrorist threats to our homeland?

Mr. OLSEN. I will take that, at first at least. Again, you mentioned and I discussed briefly the planned attack last fall. I would consider it to be a significant source of concern for us, both Iran and, again, its terrorist element, the Quds Force, as well as the group that it coordinates with, Lebanese Hezbollah.

Chairman LIEBERMAN. Right. Associate Deputy Director Perkins.

Mr. PERKINS. Yes, I agree with Director Olsen in that Quds Force, Hezbollah, and others have shown they both have the capability and the willingness to extend beyond that region of the world and likely here into the homeland itself. We look at it as a very serious problem. We look at it as a serious threat and that we are focusing intelligence analysts and other resources on that on a daily basis to monitor that threat, to make determinations, is it increasing, is it dropping off, and the like. But I agree with Director Olsen that they have the capability and they have the willingness to do that, which are two very important steps.

Chairman LIEBERMAN. Yes. And obviously you are coordinating with other parts of our intelligence community that have unique responsibility for intelligence outside of the United States.

Mr. PERKINS. That is correct, Senator, and that is a key point there, that this is a whole-of-government approach to dealing with this. This is very key across the entire intelligence community, both outside of the United States, as well as here in the homeland.

Chairman LIEBERMAN. Let me go to aviation security which, overall post-September 11, 2001, has been an area where we have put tremendous resources into the battle, and overall we have successfully defended our country and the enormous number of people, Americans and non-Americans, who travel by air. You offered testimony that al-Qaeda in the Arabian Peninsula nonetheless continues to show an intention to attack American and international aviation systems.

I wonder, and I will begin, Secretary Napolitano, with you, apart from your statement in your prepared remarks, are there additional steps that you would like to highlight at this point which you think we can or should take to deter or detect future attacks via our aviation systems?

Secretary NAPOLITANO. Well, I think the whole aviation sector demonstrates the necessity to have a layered approach so that if someone or some group is able to evade one layer, another layer can pick them up. And it begins fundamentally with good intelligence, good intelligence sharing with our international partners, good intelligence sharing within the aviation sector, and good intelligence sharing among the Federal family. It goes to the standards that we require for planes bound for the United States, both for passengers and for cargo, and how we inspect those standards.

It goes to what we ourselves require of airports and airport authorities that control, say, the perimeter of the airport. We have had one or two instances of breaches this last year. We have jumped on both of those to see why and what corrective measures needed to be taken.

It goes to when you get into the airport, what you see in the area before you get to the gate, what you may not see in the area before you get to the gate, and the construction of the gate itself with the new technology. Then there are things that we are doing in the so-called sterile area where, even though we call it a sterile area, there is still a lot of work underway and different things that TSA does on different days at different times and different places to increase security. So it is an entire layered approach.

One of the things I think has really helped and I think American passengers will begin seeing the benefits, if they have not already, is moving to a risk-based approach where, if we have pre-knowledge of a traveler and we have their biometrics, they are able to go through the airport and go through customs or whatever more quickly. So we are really encouraging that. That takes pressure off of the lines.

The second thing that is going on is a lot of technology research to see if in this country, where we have the world's best scientists and engineers, we can devise a system that is even more efficient for travelers and yet deals with the evolving threat. Research cy-

cles take time, but there is some very interesting work underway in that regard.

Chairman LIEBERMAN. Director Olsen, Associate Deputy Director Perkins, do you want to add to that?

Mr. OLSEN. Just a couple of quick points.

First, in terms of the threat, and I know we have touched on this briefly, but we do see from al-Qaeda in the Arabian Peninsula that it has demonstrated its desire to carry out an attack involving the aviation sector, really three failed attempts since December 2009, including one just this past May. I concur completely with Secretary Napolitano in terms of developing a layered approach, in terms of NCTC's contribution to that effort. We maintain the identities database of known and suspected terrorists, which becomes the basis for watchlisting and screening, at least in part the types of screening that can take place at airports. And then, finally, I would highlight again the point that Secretary Napolitano made about the value of intelligence and developing at the earliest possible stages the signs, indications, and information about individuals who may be seeking to carry out such an attack so that we can disrupt that type of plot before that person ever seeks to board an airplane or go to an airport.

Chairman LIEBERMAN. Mr. Perkins.

Mr. PERKINS. Yes, Mr. Chairman, I echo their comments. I agree that AQAP is one of the top if not the top threat we face right now simply because of their active willingness to continue coming at us in that way.

I echo Director Olsen's comments as far as intelligence goes. One of the things we have done recently to enhance and build our intelligence capabilities, especially within our Counterterrorism Division, is a better integration of our intelligence analysts into operations. Recently, we have named three deputy assistant directors who are all non-agent personnel, intelligence analysts, to lead those efforts within the Counterterrorism and Criminal Investigative Divisions. So the focus on intelligence ahead of time as well as the layered approach to thwart these attempts is vital.

Chairman LIEBERMAN. So you said something just now that anticipated the following question I was going to ask, which we are in a context, as we have said, where core al-Qaeda, which was responsible for the September 11, 2001, attacks on America, has been greatly weakened. Bin Laden is dead. A series of people who have worked their way up to replace others are gone. Abu Laith al-Libi, the Libyan who was close to the top, is now gone. Ayman al-Zawahiri unfortunately remains at liberty, but I am sure that he is in our sights nonetheless.

So if I asked you to give me what you would rank as the top two or three Islamist terrorist threats to the homeland, what would you say? Associate Deputy Director Perkins, you said you might even put AQAP now at the top. What else? Other groups? Iran, Quds Force? Which?

Mr. PERKINS. Obviously, Quds Force, Hezbollah. A lot depends on future world events as to where exactly that goes. But as we echoed, they have the capability and the willingness so that puts them near the top of that list as well. Other emerging threats in other parts of the world that we look at in addition to AQAP, are

some of the West Africa, East Africa threats in those regions, as far as their actual extent and threat to the homeland, there is debate in those areas. But, nonetheless, those are things that are near the top of our list to follow as they emerge.

Chairman LIEBERMAN. Director Olsen, how about you? What are your major concerns about sources of threats to our homeland?

Mr. OLSEN. In terms of the threat to the U.S. homeland, I would put AQAP at the top of the list. But I would also put, again, al-Qaeda core. Notwithstanding its greatly diminished capability, it does retain the intent—and we have seen this—to carry out an attack, even if it is a smaller-scale, less sophisticated attack than we have seen in the past, against the U.S. homeland. And then, third—and, again, these are not in any particular order—but I would also include on that list Iran and Hezbollah, echoing the comment that the likelihood of an attack inside the United States depends largely on events in the Middle East and what we see.

Chairman LIEBERMAN. Understood. Secretary Napolitano.

Secretary NAPOLITANO. I would add to what was said the nature of homegrown Islamist terrorists or terrorism, what we saw, for example, the arrest in Chicago last Saturday of an individual. We have seen a pattern of this or several of these instances over the last year. I think the Internet serves as a facilitator for that, and I think the so-called lone wolf can also be a lone Islamist in that regard, driven by motivations that may be behind, for example, what occurred in Benghazi.

Chairman LIEBERMAN. Well, I thank you, the three of you, very much. Again, we have made great progress. I think the American people have reason not only to be grateful to you and all the work with you for our increased security in the face of a really unusual, unprecedented threat to our homeland security, unique really in American history—and we are not only improving our defenses, we are on the offense in a very real way. But the threat goes on, and so will the work that you and this Committee will continue to do, so I thank you very much.

The record of the hearing will stay open for 15 days for any additional statements or questions that you or Members of the Committee have. Associate Deputy Director Perkins, you can tell Director Mueller that he does not have to appear anymore, that you have done very well. [Laughter.]

With that, thank you. The hearing is adjourned.

[Whereupon, at 11:55 p.m., the Committee was adjourned.]

A P P E N D I X

**Opening Statement for Chairman Joseph Lieberman
Homeland Security and Governmental Affairs Committee
“Homeland Threats and Agency Responses”
Wednesday, September 19, 2012**

Good morning and welcome to this hearing, focusing on threats to our homeland and what our key homeland security and counterterrorism agencies are doing to address those threats.

I'm pleased to welcome back Secretary Napolitano, Director Olsen, and welcome the Associate Deputy Director of the FBI, Kevin Perkins, standing in for Director Mueller today. The director had to undergo an unexpected surgical procedure resulting from complications associated with a recent dental treatment so he is unable to join us today. But we welcome Mr. Perkins in his stead with confidence, and we extend the best for the Director's speedy recovery.

This will be the final time that I chair a hearing with each of you as witnesses, and I'd like to publicly thank each of you for your leadership in our nation's homeland security and counterterrorism efforts, and for the productive relationship that each of you and officials at your agencies have had with this Committee.

The obvious fact is, as I look at the three of you, and then look back to September 11, 2001, two of the three of these organizations did not exist, and the FBI was a very different organization that focused on domestic crime. In the aftermath of the attacks, Congress and the executive created the Department of Homeland Security and, pursuant to the 9/11 Commission recommendations, the National Counter Terrorism Center. The FBI essentially recreated itself into a first-rate domestic counterterrorist intelligence agency, in addition to carrying out its other responsibilities. In his absence, I think we should thank Director Mueller for overseeing this historic transformation and thank you Secretary Napolitano and Director Olsen for what you've done.

Together these changes represent the most significant reforms of America's national security organization since the 1940s at the beginning of the Cold War. It's not coincidental since after 9/11 we understood that we were facing a very different threat to our national security and with an intensity that we had not yet faced to our homeland security.

So as I look back I want to thank you and your predecessors and the thousands of federal employees who work under you. Without question, because of what these three organizations have done, the American people have been much safer here at home than if you had not existed. So I want to extend my gratitude for what you have done. We've made a lot of progress and we've kept the enemy away for most of the last 11 years.

The most lethal threats attacks have been carried out by homegrown terrorists: Hasan at Fort Hood and Bledsoe at the Army recruiting station in Little Rock. The battle goes on, and its hard to reach a conclusion other than it'll go on for a long time.

We hold this hearing today still in mourning over the deaths of the American Ambassador to Libya, Chris Stevens, and three other State Department personnel. Speaking personally, I am infuriated by these attacks that resulted from a terrorist act against our consulate in Benghazi on the anniversary of the September 11th attacks.

This recent terrorist attack reminds us of the bravery of government officials who serve in countries such as Iraq, Afghanistan, Libya, and Egypt, working to support the struggles for freedom in these nations and by doing so, to improve our own national security.

The attack also reminds us that even though the core of Al Qaeda has been seriously weakened in the last few years, we still face threats from an evolving and fractious set of terrorist groups and individuals, united by a common ideology – that of violent Islamist extremism. And I'll have some questions to ask of you about the nature of the ter threat today specifically with reg to the reation to this film, whether tou think it has raised the threat level against any place ind or inst here in the US.

In examining the terrorist threat to the homeland today, I look forward to hearing from you on topics such as the status of efforts to counter homegrown violent Islamist extremism; the significance of the emergence of new jihadist groups in countries such as Egypt, Libya and Syria; and the threat to our homeland posed by Iran, the Quds force, and its proxy group Hezbollah, which seems to be reaching out of its normal area of operation, including the attempted assassination, which was thwarted, of the Saudi ambassador here in Washington and the recent bombing in Bulgaria.

I'd like to say a few words about cyber security, which has been a significant focus of the Committee this year. We know how serious the problem is. Enormous amounts of cyber espionage and cyber theft are going on, and there is increasing danger of a cyber attack. As you know the Cybersecurity Act of 2012, which was the compromise bipartisan legislation that made it to the Senate floor, has had problems getting enough votes to get taken up on the Senate floor. We worked for years with partners on both sides of the aisle. We had extensive consultations with private industry and of course we went to substantial lengths to find comond ground - including by making the standards voluntary and not mandartoy for private sector owners of cyber infrastructure.

But despite the magnitude of the threat as recognized by national security leaders from the past two administrations and both parties, the bill was filibustered on the Senate floor. Thus passed the best opportunity we've had to pass comprehensive cybersecurity legislation. And of course all of you have said, perhaps Director Mueller most notatbly, that the threat of cyber attack will surpass the threat of terror attack.

I think it is obvious that we are not going to pass cybersecurity legislation before the election because we're leaving here in the next couple days but I think its possible and critical for Congress to pass such leglislation. But if the gridlock continues, as I fear it will, then the President and others in the Executive Branch should do everything within their power, as they are doing, to raise our defenses against cyber attack and cyber theft.

The fact is that today because of the inadequate defenses of America's privately owned critical cyber infrastructure, we are very vulnerable to a major cyber attack, perhaps a catastrophic cyber attack, well beyond what we suffered on 9/11.

I understand that executive action cannot do everything legislation can to protect us from cyber attack but it can do a lot. So far, we have failed to fix this problem and close our vulnerabilitie to cyber attack, and I hope the President will step in along with you, Secretary Napolitano, and act as strongly as you can to protect our country from these attacks.

So I want to thank you for being here. I look forward to this hearing every year. It's sometimes unsettling but it's important as a report to Congress and the people on the status of the threat to our homeland.

**Opening Statement of
Senator Susan M. Collins
“Homeland Threats and Agency Responses”
Committee on Homeland Security and Governmental Affairs
September 19, 2012**

Last week, we observed the eleventh anniversary of the horrific attacks of September 11th, 2001. We again remembered the victims and heroes of that day. And we acknowledged the dedicated military, intelligence, law enforcement, and homeland security professionals who have worked together to bring terrorists to justice and to prevent another large-scale attack inside the United States.

Tragically, however, we have also witnessed violent attacks on the U.S. Consulate in Benghazi, Libya, the resulted in the killings of our Ambassador and three other brave Americans. While these attacks remain under investigation, it is difficult not to see shades of the 1998 attacks on our embassies in Kenya and Tanzania, which were among the many precursors to the attacks of 9/11. This tragedy underscores the ongoing threat we face, both abroad and at home, from violent Islamist extremists.

In the aftermath of 9/11, we took significant actions to address this threat. When Senator Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our aim was to improve coordination within the Intelligence Community and among the key stakeholders at all levels of government. Achieving the goals of this landmark law remains a work in progress.

We know we face a determined enemy. Al-Qaeda in the Arabian Peninsula (AQAP) has tried repeatedly to exploit holes in our security. The failed 2009 Christmas Day bomber used a device specifically designed to avoid detection. The 2010 cargo plot sought to circumvent improvements in passenger screening by targeting cargo. In May of this year, al-Qaeda tried again. The bomb-maker apparently sought to avoid the failures of the earlier Christmas Day attack. Through the aggressive efforts of our intelligence community, this plot was disrupted before it could threaten American lives. Nevertheless, that operation was also plagued by leaks – apparently from within the Executive branch – that may have undermined future efforts.

Not every threat that we face has been met with sufficient resolve and action. Perhaps the best example is the ever-increasing cyber threat. Experts have repeatedly warned that the computer systems that run our electric grids, water plants, financial networks, and transportation systems are vulnerable to a cyber attack that could harm millions of Americans.

Just last week, former Deputy Secretary of Defense John Hamre said that the threats in cyberspace “took a darker turn” this summer, as three very large corporations experienced cyber attacks “designed to damage operations.” Citing government sources, he said that at least two of the attacks may have come from Iran. China and Russia have also launched cyber attacks.

To respond to this escalating threat, the Chairman and I have worked during the past two years to craft a bipartisan bill that relies on the expertise of government and the innovation of the

private sector. Despite our hard work to find common ground, the Senate has failed to pass cybersecurity legislation. Given the significant damage already done to our economy and our security, as well as our clear vulnerability to even worse attacks, this failure to act is inexcusable.

Former DHS Secretary Michael Chertoff and former NSA and CIA chief Michael Hayden describe the urgency this way: "We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9/11' hits - it is not a question of 'whether' this will happen; it is a question of 'when.'"

This time all the dots have been connected. This time the warnings are loud and clear, and we must heed them.

In contrast to the known threat of cyber attacks, another persistent challenge we face comes from those threats we fail to even anticipate—the so-called “black swan” events that test our assumptions. These are our most vexing problem because we cannot simply build walls around every potential target. Nonetheless, if we strengthen information sharing and analytic capabilities, our law enforcement and intelligence officers can disrupt more plots, whether they are those we know well or ones we have never before seen.

In my judgment, which is informed by numerous discussions with experts, the attack in Benghazi was not a “black swan” event but rather an attack that should have been anticipated based on previous attacks against Western targets, the plentiful, dangerous weapons in Libya, the presence of al-Qaeda, and the overall threat environment.

Whatever the plots hatched by our enemies, I am also concerned about vulnerabilities that stem from our own the government’s actions or failure to act.

I’ve already noted the lack of security in Benghazi, the grave, self-inflicted wounds from intelligence leaks, and the failure to enact a cybersecurity bill. There is also the genuine danger posed by the automatic, mindless cuts known as sequestration. Absent a commitment by the President and Congress to avoid this disastrous policy, the budget of every federal agency represented here today – agencies charged with protecting our nation from terrorism and other disasters – will be slashed in an indiscriminate way, by eight percent or more, potentially affecting vital programs such as border security, intelligence analysis, and the FBI’s work.

At a time when budget constraints require everyone to sacrifice, we should ask where resources can be spent more effectively and what tradeoffs should be made—to balance the risk we face with the security we can afford. What we cannot afford, however, is to weaken a homeland security structure that is helping to protect our country.

Prepared Statement of Senator Daniel K. Akaka
Committee on Homeland Security and Governmental Affairs
September 19, 2012

Thank you, Mr. Chairman, for holding this hearing.

I join all Americans in mourning the loss of the four brave and dedicated American public servants who died as a result of the senseless attacks in Libya last week. I honor them and the thousands of civilian federal employees overseas, as well as members of the military, who risk their lives every day in service to this country.

I am troubled by the recent violence that has targeted U.S. facilities across the Muslim world. These incidents raise concerns about the protection of Americans working abroad, including questions about U.S. efforts to secure our 270 posts around the world. I applaud President Obama's action sending Marines to secure diplomatic posts in Libya and Yemen, and I recognize the important work the State Department's Diplomatic Security Bureau is doing to protect American posts overseas. In the wake of these violent protests, I hope our witnesses today will address the current threats to Americans both at home and abroad, how those threats are being countered, and how the Departments represented today are working with the State Department to ensure the security of all Americans serving overseas.

We owe a debt of gratitude to the government workers who have made essential contributions to thwarting terrorism. I want to particularly applaud the leadership of our witnesses today and thank them for collaborating in this important effort. In the face of domestic and international threats, we rely on them and the many men and women of our military, law enforcement, homeland security, and intelligence communities to keep us safe.

**Prepared Statement of Senator Thomas R. Carper
September 19, 2012**

Last week, as Americans were commemorating the 11th Anniversary of 9/11, our nation lost four American heroes, including Ambassador Chris Stevens, who dedicated his life to advancing the ideals of democracy, liberty and justice across the globe. These senseless acts are another stark reminder that the values that make us a great country are still a target across the world and that we must remain ever vigilant to new and evolving threats.

As the tragic events in Libya and the turmoil across North Africa and the Middle East make clear, our country and people still face a very real threat from terrorism. While we have made important strides in taking out top Al Qaeda leaders, the group's violent anti-American message continues to resonate with many around the world. We must also maintain a clear-eyed assessment of the dangers posed by the nuclear ambitions of Iran. All of these dangers pose real threats not only abroad but here at home too. That is why we must continue to find innovative ways to protect our borders and ports, enhance our aviation and transportation security, and secure our critical infrastructure. However, if a program is not working, we shouldn't just keep throwing good money after bad; we must work smarter across the federal government and look to get better results with our limited resources.

One threat that continues to grow and, in the words of FBI Director Robert Mueller, may "equal or surpass the threat of counter terrorism in the foreseeable future" is the threat from hackers, terrorists, and nation states in cyberspace. Every day, hackers are stealing the hard work and innovation of our American companies, putting our economic security at risk. But, it's not just valuable information that we are losing. To put it bluntly, it's also American jobs and our competitive edge. Of course, the same vulnerabilities being exploited to steal our intellectual property can also be used by those who want to do us physical harm. With a few clicks of a mouse, cyber terrorists or nation states could shut down our electric grid, release dangerous chemicals into the air we breathe, or disrupt our financial markets.

If we don't become more vigilant – and soon – a sophisticated hacker might just find a way to carry out a cyber 9/11. That is why I joined Chairman Lieberman, Ranking Member Collins and others in introducing the Cybersecurity Act of 2012. The bill takes a number of bold and necessary steps to better secure our critical infrastructure and share cyber threat information and will go a long way toward bringing our cyber capabilities into the 21st century. Unfortunately, the bill has become mired in partisan politics despite our best efforts to address the concerns of Senators on both sides of the aisle. While I am disappointed that the Senate has not been able to come together and pass a cybersecurity bill, I remain committed to working with my colleagues to pass legislation as soon as possible.

I would like to thank Secretary Napolitano, Associate Deputy Director Perkins, and Director Olson for being with us today to discuss all of these threats and the steps we are taking to better secure our country. I would also like to thank them for their years of dedicated public service. Your efforts, along with those many others across our government, including the bravery of our armed forces, intelligence community, and diplomatic corps, are why we are a safer nation today. I would also like to recognize all the first responders and law enforcement officials throughout the country who continue to work so hard for our safety and security.

The challenges before us are vast, but if we can rekindle that spirit of unity that helped us get through those difficult days after 9/11, I know we will be able to overcome any challenge and continue to accomplish great things.

Statement of Senator Jerry Moran
Homeland Security and Governmental Affairs Committee
“Homeland Threats and Agency Responses”
Washington, DC
September 19, 2012

I thank the Chairman and the Ranking Member for holding this hearing, and I appreciate our three witnesses being here to testify. I want to express my gratitude to them for their efforts in making certain that Americans remain safe and secure around the world.

Today I want to focus my attention on our pressing need to address the threat of a biological attack against the United States. As Secretary Napolitano mentioned, there is real danger of a “sophisticated biological threat” against the United States. Such an attack could have a very detrimental impact on our citizenry, our supply chain, and the U.S. and international economies. An attack could be something like Anthrax or Ricin, or an animal disease like foot and mouth disease. According to the FBI’s Law enforcement bulletin, many believe foot and mouth disease to be the greatest threat due to its highly contagious nature, stability, and survivability. A foot and mouth disease outbreak could spread to as many as 25 states in as little as 5 days, and could cost taxpayers up to \$60 billion in damage. There is no doubt that an act of agroterrorism would deliver a major blow to the US agricultural industry, which is the largest single sector in the US economy. Such an attack could unravel the health, wealth, and economic fiber of our nation. In fact, DHS’s own website says that an attack against our food and agricultural industry “would have dire economic and potentially human health consequences.”

Current and previous Administrations have affirmed these threats and the need to prepare and respond. For example, the Bush Administration addressed this issue in the Homeland Security Presidential Directive 9 (HSPD 9: Defense of United States Agriculture and Food (January 2004)), and the Obama Administration did so in the National Security Strategy for Countering Biological Threats (NSSCBT) (November 2009). Despite the widespread attention this issue has received, currently no facility meets the requirements identified in HSPD 9, and we are not taking the appropriate measures based on the NSSCBT – the Graham-Talent WMD Commission gives the U.S. an “F” grade for bioterrorism readiness. The Congressional report, *The Clock Is Ticking*, pointed to the prospect of biological threats and stated that “it is essential that the US government move more aggressively to address the threat of Bioterrorism.”

A critical component to addressing these threats is actively researching biological and zoonotic diseases and developing the capability to rapidly and inexpensively produce vaccines and other remedies for such diseases. For a long time, the Department of Homeland Security has been the lead Department in developing a new facility where this research can take place, the National

Bio and Agro-Defense Facility (NBAF), in Manhattan, Kansas. I thank Secretary Napolitano for her support of the facility, the location, and the process by which Manhattan was chosen. She has repeatedly stated there is a definitive need for NBAF and research on biological and zoonotic diseases to protect our national security and economic stability. She has stated that "Plum Island does not meet the Nation's needs in this area," and she "believes in NBAF, and it should be in Kansas, and we need to get on with it." I agree with the Secretary. We need to move forward, and the time to do so is now.

All of the hurdles with regard to proceeding with NBAF have been cleared, the most recent being the National Academy of Science (NAS) report, which was released in July. We are now at the point where there is no reason for the Department of Homeland Security not to allow the facility to proceed. All of the funds spent on the project thus far have been from the state of Kansas – the appropriated \$40 million for use on the central utility plant and \$50 million to begin general construction are being held back. It is clear to me that the release of these appropriated funds now rests in the Secretary's hands. The ability to proceed depends on releasing those funds and authorizing the land to be transferred. The time is now and the decision should be made to move forward.

As we know, with the passage of time, the more costly the NBAF project becomes; not only in dollar amount, but also costly in terms of risking American lives and our national and economic security. Whether manmade or natural, biological and zoonotic threats are imminent and we need to be actively engaged in research to find vaccines and other appropriate response mechanisms. We should not wait any longer; enough has been said and it is time to act. In the absence of a land transfer and the release of the already appropriated funds, the confidence of many Kansans who believe that our money is being well spent is diminishing. Now is the time and it is a matter of a few weeks that this transfer needs to happen. The entire Kansas delegation stands ready to work with you on this, and we thank you in advance for your continued hard work.



Statement for the Record
“Homeland Threats and Agency Responses”
Secretary Janet Napolitano
U.S. Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
September 19, 2012

Page 1 of 21

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee.

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS), not only over the past three and a half years, but indeed, since the Department's founding. I look forward to continuing our work together to protect the American people as we advance our many shared goals.

I also thank Director Mueller and Director Olsen. DHS collaborates very closely and effectively with the Federal Bureau of Investigation (FBI) and National Counterterrorism Center (NCTC), and together we have forged a strong partnership to meet the shared responsibility of protecting the American people from foreign terrorist plots to acts of homegrown extremists.

Eleven years after the terrorist attacks of September 11th, America is stronger and more secure, thanks to the support of the Congress, the work of the men and women of DHS, and our Federal, state, local, tribal, and territorial partners across the homeland security enterprise. I thank them all for their service.

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the Federal government, public and private sectors, and communities throughout the country have strengthened homeland security to better mitigate and defend against evolving threats.

Additionally, within the Federal government, many departments and agencies contribute to the homeland security mission. The Nation's armed forces serve on the frontlines of homeland security by degrading al-Qaeda's capabilities to attack the United States and targets throughout the world. The Office of the Director of National Intelligence, the Central Intelligence Agency, and the entire Intelligence Community, of which DHS is a member, are producing better streams of intelligence than at any time in history.

The Federal homeland security enterprise also includes the strong presence of the Department of Justice (DOJ) and the FBI, whose role in leading terrorism investigations has led to the arrest of numerous individuals on terrorism-related charges.

But despite considerable progress, the recent attacks in Oak Creek, Wisconsin, and Aurora, Colorado—and the terrorist attack in Bulgaria—serve as a reminder that our work to detect and prevent attacks is never done.

As I have said many times, homeland security begins with hometown security. As part of our commitment to strengthening hometown security, we have worked to get information, tools, and resources out of Washington, D.C., and into the hands of state, local, tribal, and territorial officials and first responders.

This has led to significant advances. We have made great progress in improving our domestic capabilities to detect and prevent terrorist attacks against our citizens, our communities, and our critical infrastructure. We have increased our ability to analyze and distribute threat information

at all levels. We have invested in training for local law enforcement and first responders of all types in order to increase expertise and capacity at the local level. We have also supported and sustained preparedness and response capabilities across the country through more than \$36 billion in homeland security grants since 2002.

As we look ahead, and in order to address evolving threats and make the most of limited resources, the Administration proposed a new vision for homeland security grants in the Fiscal Year (FY) 2013 President's budget. The Administration's proposal focuses on building and sustaining core capabilities associated with the five mission areas within the National Preparedness Goal (NPG), helping to elevate nationwide preparedness.

This proposal reflects the many lessons we have learned in grants management and execution over the past ten years. Using a competitive, risk-based model, the proposal envisions a comprehensive process to assess gaps, identify and prioritize deployable capabilities, limit periods of performance to put funding to work quickly, and require grantees to regularly report progress in the acquisition and development of these capabilities. The Administration looks forward to working with Congress and stakeholders on this proposal to enable all levels of government to build and sustain, in a collaborative way, the core capabilities necessary to prepare for incidents that pose the greatest risk to the security of the Nation.

Our experience over the past several years has also made us smarter about the terrorist threats we face and how best to deal with them. We continue to expand our risk-based, intelligence-driven security efforts. By sharing and leveraging information, we can make informed decisions about how to best mitigate risk, and provide security that is seamless and efficient.

We also free up more time and resources, giving us the ability to focus resources on those threats or individuals we know the least about. This approach not only makes us safer, it also creates efficiencies within the system for travelers and for businesses. In other words, our homeland security and our economic security go hand-in-hand.

Strengthening homeland security includes a significant international dimension. To most effectively carry out our core missions – including preventing terrorism, securing our borders, enforcing immigration laws, and protecting cyberspace – we partner with countries around the world. This work ranges from strengthening cargo, aviation, and supply chain security to joint investigations, information sharing, and science and technology cooperation.

Through collaborations with the State Department and other Federal agencies and our foreign counterparts, we not only enhance our ability to prevent terrorism and transnational crime; we also leverage the resources of our international partners to more efficiently and cost-effectively secure global trade and travel, to help ensure that dangerous people and goods do not enter our country.

In my time today, I would like to provide an update on the key areas of the DHS mission that fall within the Committee's jurisdiction, our priorities, and our vision for working with Congress to build on the substantial progress we have achieved to date and must continue to sustain in the months and years ahead.

Preventing Terrorism and Enhancing Security

While the United States has made significant progress, threats from terrorists—including, but not limited to al-Qaeda and al-Qaeda affiliated groups—persist and continually evolve, and the demands on DHS continue to grow. Today's threats are not limited to any one individual, group or ideology and are not defined or contained by international borders. Terrorist tactics can be as simple as a homemade bomb and as sophisticated as a biological threat or a coordinated cyber attack.

DHS and our partners at the Federal, state, tribal, and local levels have had success in thwarting numerous terrorist plots, including the attempted bombings of the New York City subway, foiled attacks against air cargo, and other attempts across the country. Nonetheless, recent attacks overseas, and the continued threat of homegrown terrorism in the United States, demonstrate how we must remain vigilant and prepared.

To address these evolving threats, DHS employs risk-based, intelligence-driven operations to prevent terrorist attacks. Through a multi-layered detection system focusing on enhanced targeting and information sharing, we work to interdict threats and dangerous people at the earliest point possible. We also work closely with Federal, state, and local law enforcement partners on a wide range of critical homeland security issues in order to provide those on the frontlines with the information and tools they need to address threats in their communities.

Likewise, countering biological, chemical, nuclear, and radiological threats requires a coordinated, whole-of-government approach. DHS, through the Domestic Nuclear Detection Office, works in partnership with agencies across Federal, state, and local governments to prevent and deter attacks using nuclear and radiological weapons through nuclear detection and forensics programs. The Office of Health Affairs (OHA), the Science and Technology Directorate (S&T), and the Federal Emergency Management Agency (FEMA) also provide medical, scientific, and other technical expertise to support chemical, biological, nuclear, and radiological preparedness and response efforts.

Sharing Information, Expanding Training, and Raising Public Awareness

The effective sharing of information in a way that is timely, actionable whenever possible, and that adds value to the homeland security enterprise is essential to protecting the United States. As part of our approach, we have changed the way DHS provides information to our partners by replacing the outdated color-coded alert system with the National Terrorism Advisory System, or NTAS, which provides timely, detailed information about credible terrorist threats and recommended security measures.

We also have continued to enhance the Nation's analytic capability through the 77 designated fusion centers, resulting in unprecedented information sharing capabilities at the state and local levels. DHS has supported the development of fusion centers through deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to Federal systems, technology, and grant funding. We currently have more than 90 DHS intelligence

officers deployed to fusion centers, working side by side with their Federal, state, and local counterparts. DHS also has provided hundreds of personnel, including U.S. Immigration and Customs Enforcement (ICE) special agents, U.S. Secret Service (USSS) agents, Federal Air Marshals, U.S. Customs and Border Protection (CBP) officers, U.S. Citizenship and Immigration Services (USCIS) officers, and representatives from FEMA and the U.S. Coast Guard (USCG) to support FBI-led Joint Terrorism Task Forces (JTTFs) across the country.

We are working to ensure that every fusion center supported by DHS maintains a set of core capabilities that includes the ability to assess local implications of national intelligence, share information with Federal authorities so we can identify emerging national threats, and ensure the protection of civil rights, civil liberties and privacy.

Specifically, we are encouraging fusion centers to develop and strengthen their grassroots analytic capabilities so that national intelligence can be placed into local context, and the domestic threat picture can be enhanced based on an understanding of the threats in local communities. We are partnering with fusion centers to establish more rigorous analytic processes and analytic production plans, increase opportunities for training and professional development for state and local analysts, and encourage the development of joint products between fusion centers and Federal partners.

Over the past three years, we have transformed how we train our Nation's frontline officers regarding suspicious activities, through the Nationwide Suspicious Activity Reporting Initiative (NSI). This initiative, which we conduct in partnership with the DOJ, is an Administration effort to train state and local law enforcement to recognize behaviors and indicators potentially related to terrorism and terrorism-related crime; standardize how those observations are documented and analyzed; and ensure the sharing of those reports with fusion centers for further analysis and with the JTTFs for further analysis and investigation.

As of August 2012, more than 234,000 law enforcement officers have now received training under this initiative, and more are getting trained every week. The training was created in collaboration with numerous law enforcement agencies, and with privacy, civil rights and civil liberties officials. DHS also has expanded the Nationwide Suspicious Activity Reporting Initiative to include our Nation's 18 critical infrastructure sectors. Infrastructure owners and operators from the 18 sectors are now contributing information, vetted by law enforcement through the same screening process otherwise used to provide information to the JTTFs.

Because an engaged and vigilant public is vital to our efforts to protect our communities, we have also continued our nationwide expansion of the "If You See Something, Say Something™" public awareness campaign. This campaign encourages Americans to contact law enforcement if they see something suspicious or potentially dangerous. To date, we have expanded the campaign to Federal buildings, transportation systems, universities, professional and amateur sports leagues and teams, entertainment venues, some of our Nation's largest retailers, as well as local law enforcement. Most recently DHS has partnered with sports leagues such as the National Football League, Major League Soccer, Major League Baseball, the National Basketball Association, National Collegiate Athletic Association, National Hockey League,

U.S. Golf, and the U.S. Tennis Association, to promote public awareness of potential indicators of terrorism at sporting events.

Countering Violent Extremism

At DHS, we believe that local authorities and community members are often best able to identify individuals or groups residing within their communities exhibiting dangerous behaviors—and intervene—before they commit an act of violence. Countering violent extremism (CVE) is a shared responsibility, and DHS continues to work with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to terrorist activity, and the best ways to mitigate or prevent that activity.

The Department's efforts to counter violent extremism are three-fold. We are working to better understand the phenomenon of violent extremism through extensive analysis and research on the behaviors and indicators of violent extremism. We are bolstering efforts to address the dynamics of violent extremism by strengthening partnerships with state, local, and international partners. And, we are expanding support for information-driven, community-oriented policing efforts through training and grants.

All of this work is consistent with the Administration's CVE Strategy released in August 2011 and the *CVE Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States* released in December 2011.

As part of our CVE approach, DHS has conducted extensive analysis and research to better understand the threat of violent extremism in order to support state and local law enforcement, fusion centers, and community partners with the knowledge needed to identify behaviors and indicators associated with acts of violent extremism.

In addition, over the past year, DHS has worked closely with state and local partners, including the State and Provincial Police Academy Directors (SPPADS), the International Association of Chiefs of Police (IACP), the Major City Chiefs Association (MCC), the Major City Sheriff's Association (MCSA), as well as NCTC, DOJ, and the FBI to develop training for frontline law enforcement officers on behaviors potentially indicative of violent extremist activity.

DHS has also created a new CVE Webportal, launched on August 31, 2012, for a select group of law enforcement through the Homeland Security Information Network (HSIN). The purpose of this portal is to provide law enforcement with CVE training resources and materials, as well as a central portal for communication and information sharing on CVE. DHS aims to make the Webportal available to law enforcement nationwide by the end of September 2012.

Finally, DHS has supported State and Local CVE activities through grants. DHS publicly released the *CVE Training Guidance and Best Practices*, which was sent to all state and local partner grantors and grantees thereby tying CVE to grant guidance policy on October 7, 2011. DHS also incorporated language into FY 2012 grant guidance that prioritizes CVE and allows funds to be used in support of state and local CVE efforts.

Active Shooter Threats

There have been a series of international and domestic violent extremist incidents over the past several years that have involved active shooters, including the 2008 Mumbai attacks; shootings in 2009 at the U.S. Holocaust Memorial Museum, Fort Hood, and a military recruiting station in Little Rock, Arkansas; and the 2011 attacks in Utoya, Norway. The recent shooting at a Sikh temple in Oak Creek, Wisconsin, was carried out by an individual with a history of involvement in the white supremacist extremist movement, although his motives remain unknown. Attacks by active shooters with no known ties to extremist movements also have caused significant loss of life and injury, including most recently in Aurora, Colorado.

Preventing and responding to active shooter threats is a priority for state and local law enforcement authorities, regardless of the motivation behind the attack. Where there is any active shooter scenario, prevention is a priority, response efforts will be the same, and the impact on the community is significant. This is an area in which DHS, in partnership with the FBI, has been very active. DHS is working to better understand the behaviors and indicators that lead to these acts of violence, the tactics used, and the actions that can be taken to help prevent them in the future. A central goal of our efforts is to build capabilities within state and local law enforcement communities to effectively respond to active shooter threats.

As part of this effort, we have worked with the FBI to produce both classified and unclassified case studies about past active shooter events and have made them available to state and local law enforcement. These case studies include behaviors and indicators, so that front line personnel will be better able to recognize pre-incident indicators of an emerging active shooter threat. We have incorporated this information in the training materials pertaining to CVE.

Additionally, the DHS Office of Infrastructure Protection and FEMA conduct active shooter trainings for state and local law enforcement and for the private sector. DHS's Active Shooter Awareness Program provides resources to help public and private-sector security managers train their workforce and enhance their facilities' preparedness and response to an active shooter scenario. Since the program's inception in December 2008, more than 5,000 law enforcement officers and other partners have participated.

FEMA, through Louisiana State University, a member of the National Domestic Preparedness consortium, also offers the Law Enforcement Active Shooter Emergency Response (LASER) course which addresses the technical aspects of planning and implementing a rapid law enforcement deployment to an active shooter incident.

In addition, the Federal Law Enforcement Training Center (FLETC) has been instrumental in preparing our Nation's state, local, and Federal law enforcement officers to respond effectively to an active shooter incident should one occur. FLETC has trained over 4,000 U.S. law enforcement officers in active shooter response and active shooter response instructor training. These newly trained instructors have gone on to train thousands more. FLETC also has reached out to its law enforcement partners that have experienced active shooter incidents to develop "lessons learned/lesson anticipated" that help to continually update and improve the tactics for active shooter response programs.

DHS also has developed an online Independent Study Course titled "Active Shooter: What You Can Do" through FEMA's Emergency Management Institute. This course provides guidance to individuals, including managers and employees, to prepare to respond to an active shooter situation. Nearly 134,000 government and private-sector participants have completed this training since it was released in March 2011.

In collaboration with the FBI and NCTC, DHS and FEMA have organized a two-day Joint Counterterrorism Awareness Workshop Series (JCTAWS) to review and improve operational capabilities, response resources, and information sharing among Federal, state, local, and private sector partners. This nationwide initiative is designed to increase the ability of local jurisdictions to prepare for, protect against, and respond to coordinated terrorist attacks against multiple targets. Since 2011, workshops have been conducted in Boston, Philadelphia, Honolulu, Indianapolis, Sacramento, Houston, Nashville, Denver, and Los Angeles. Modified workshops were also conducted in Tampa and Charlotte in support of the Republican and Democratic National Conventions. The next scheduled workshop is in Las Vegas this October.

Because faith-based communities have been the targets of violence, DHS continues to maintain regular contact with faith-based communities and helps coordinate rapid incident communications efforts. One recent example includes the DHS Office for Civil Rights and Civil Liberties' (CRCL) activation of the Incident Community Coordination Team (ICCT) on August 6, 2012, following the shooting in Oak Creek, Wisconsin.

During the call, leaders from Sikh, Hindu, Jewish, Muslim, and interfaith communities and organizations discussed the shooting with senior Government officials from the White House, DOJ, FBI, and DHS. More than 100 participants from across the country joined the ICCT call to share information about response activities and resources available, and to address community concerns.

Through the Office of Infrastructure Protection, DHS also has made the Active Shooter Awareness Program available to faith-based communities, as well as provided resources to ensure that their facilities are safe and secure through site assessments, threat briefings, and trainings.

Protecting Our Aviation System

Threats to our aviation system remain active and continue to evolve. Consequently, the Transportation Security Administration (TSA) is working internationally and with the private sector to continue to improve security screening, while simultaneously facilitating lawful travel and trade. We are continuing to strengthen protection of our aviation sector through a layered detection system focusing on risk-based screening, enhanced targeting, and information-sharing efforts to interdict threats and dangerous people at the earliest point possible.

The Department is focused on measures to shift aviation security from a "one size fits all" approach for passenger screening to a risk-based approach. In doing so, TSA utilizes a range of measures, both seen and unseen, as part of its layered security system - from state of the art

explosives detection, to using Advanced Imaging Technology (AIT) units and canine teams to screen passengers and cargo, to expediting screening for known travelers. Through Secure Flight, TSA is now pre-screening 100 percent of all travelers flying within, to, or from the United States against terrorist watchlists before passengers receive their boarding passes.

In our increasingly interconnected world, we also work beyond our own airports, partnering with our Federal agencies and countries to protect both national and economic security.

For example, through the Pre-Departure Targeting Program, Immigration Advisory Program and enhanced in-bound targeting operations, Customs and Border Protection (CBP) has improved its ability to identify high-risk travelers who are likely to be inadmissible into the United States and make recommendations to commercial carriers to deny boarding before a plane departs.

Through the Visa Security Program, U.S. Immigration and Customs Enforcement (ICE) has deployed trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States.

Through preclearance agreements, CBP Officers deployed overseas inspect passengers abroad through the same process a traveler would undergo upon arrival at a U.S. port of entry, allowing us to extend our borders outward while facilitating a more efficient passenger experience.

Finally, our continued use, analysis, and sharing of Passenger Name Record (PNR) data has allowed us to better identify passengers who merit our attention before they depart for the U.S. On July 1, 2012, a new agreement with the European Union on the transfer of PNR data entered into force, marking an important milestone in our collective efforts to protect the international aviation system from terrorism and other threats.

As we have taken these actions to strengthen security, we also have focused on expediting lawful trade and travel for the millions of people who rely on our aviation system every day. One key way we have done this is through expansion of trusted traveler programs.

For instance, the Global Entry program, which is managed by CBP, is allowing us to expedite entry into the United States for pre-approved, low-risk air travelers. More than one million trusted traveler program members are able to use the Global Entry kiosks, and we are expanding the program both domestically and internationally as part of the Administration's efforts to foster increased travel and tourism.

In addition to U.S. citizens and lawful permanent residents, Mexican nationals can now enroll in Global Entry, and Global Entry's benefits are also available to Dutch citizens enrolled in the Primum program; South Korean citizens enrolled in the Smart Entry Service program; Canadian citizens and residents through the NEXUS program; and citizens of the United Kingdom, Germany, and Qatar through limited pilot programs. In addition, we have signed agreements with Australia, New Zealand, Panama, and Israel to allow their qualifying citizens to participate in Global Entry. We are continuing to expand the program both domestically and internationally as part of the Administration's efforts to foster travel and tourism, which supports the President's Executive Order 13597 on Travel and Tourism.

U.S. citizen participants in Global Entry are also eligible for TSA Pre✓™ – a passenger prescreening initiative. TSA Pre✓™ is part of the agency's ongoing effort to implement risk-based security concepts that enhance security by focusing on travelers the agency knows least about. More than 2 million passengers have received expedited screening through TSA Pre✓™ security lanes since the initiative began last fall. TSA Pre✓™ is now available in 25 airports for select U.S. citizens traveling on Alaska Airlines, American Airlines, Delta Air Lines, United Airlines and US Airways and members of CBP Trusted Traveler programs. TSA has expanded TSA Pre✓™ benefits to U.S. military active duty members traveling through Ronald Reagan Washington National and Seattle-Tacoma international airports. In addition to TSA Pre✓™, TSA has implemented other risk-based security measures including modified screening procedures for passengers 12 and younger and 75 and older.

Visa Waiver Program

With our partners overseas, we have acted to strengthen the Visa Waiver Program (VWP), a program that boosts our economy by facilitating legitimate travel for individuals traveling to the United States for tourism or business. According to the Commerce Department, tourism alone supported 7.6 million U.S. jobs last year, and tourism revenue in early 2012 was up 14 percent from the previous year.

The VWP is an essential driver of international tourism because it allows eligible nationals of 36 countries to travel to the United States without a visa and remain in our country for up to 90 days. Almost two-thirds of international travelers come to the U.S. from VWP countries. Additionally, since its inception in the mid-1980s, VWP has also become an essential tool for increasing security standards, advancing information sharing, strengthening international relationships, and promoting legitimate travel to the United States.

Over the last several years, DHS has focused on bringing VWP countries into compliance with information sharing agreement requirements of The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. No. 110-53. As of January 2012, all VWP countries have completed an exchange of diplomatic notes or an equivalent mechanism for the requirement to enter into an agreement to share information on lost and stolen passports with the United States through INTERPOL or other designated means.

DHS, in collaboration with the DOJ, has concluded Preventing and Combating Serious Crime (PCSC) agreements, or their equivalent, with 35 VWP countries and two VWP aspirants. DHS, along with the Departments of Justice and State, continues to work closely with the remaining country to sign a PCSC agreement. These agreements facilitate the sharing of information about terrorists and serious criminals. The U.S. government has also concluded negotiations on arrangements with all VWP countries for the exchange of terrorism screening information.

Additionally, DHS developed the Electronic System for Travel Authorization (ESTA) as a proactive online system to determine whether an individual is eligible to travel to the United States under the VWP, and whether such travel poses any law enforcement or national security risks.

We support carefully managed expansion of the VWP to countries that meet the statutory requirements, and are willing and able to enter into a close security relationship with the United States. To this end, we support current bi-partisan efforts by the Congress, such as the proposed JOLT Act of 2012, to expand VWP participation and to promote international travel and tourism to the United States while maintaining our strong commitment to security. Additionally, as part of the President's recent Executive Order, we are working with international partners to meet existing requirements and prepare for further expansion of the VWP.

Overstays and Exit Capabilities

Over the past year, we have worked to better detect and deter those who overstay their lawful period of admission through the enhanced biographic program. The ability to identify and sanction overstays is linked to our ability to determine who has arrived and departed from the United States. By matching arrival and departure records, and using additional data collected by DHS, we can better determine who has overstayed their lawful period of admission.

In May 2011, as part of Phase 1 of the enhanced biographic effort, DHS began a coordinated effort to vet all potential overstay records against Intelligence Community and DHS holdings for national security and public safety concerns. Using those parameters, we reviewed the backlog of 1.6 million overstay leads within the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program and referred leads based on national security and public safety priorities to ICE for further investigation.

Through limited automated means, DHS cross-referenced additional overstay leads with DHS location and immigration holdings, closing additional records by confirming changes in immigration information or travel history that had not yet been recorded. Previously, these records would not have been examined, except in instances when resources allowed it. Now, we are vetting all overstays for public safety and national security concerns, and DHS is also conducting automated reviews for changes in immigration status or travel history. This is performed on a recurrent basis.

In July, Congress approved DHS's plan to continue building its enhanced biographic capability. DHS is implementing Phase 2 of this effort, and expects to have these enhancements in place by early 2013. Once completed, this initiative will significantly strengthen our existing capability to identify and target for enforcement action those who have overstayed their authorized period of admission, and who represent a public safety and/or national security threat by incorporating data contained within law enforcement, military, and intelligence repositories.

This strategy also will also enhance our ability to identify individual overstays; provide the State Department with information to support visa revocation, prohibit future VWP travel for those who overstay, and place "lookouts" for individuals, in accordance with existing Federal laws; establish greater efficiencies to our Visa Security Program; and enhance the core components of an entry-exit and overstay program.

Concurrently, S&T is working to establish criteria and promote research for emerging technologies that would provide the ability to capture biometrics and develop a biometric exit capability at a significantly lower operational cost than is currently available. S&T is collaborating with the National Institute of Standards and Technology (NIST) on this initiative.

Lastly, as part of the *Beyond the Border Action Plan* signed by President Obama and Canadian Prime Minister Harper in December 2011, we are creating an exit program on the United States northern border. Under the plan, the United States and Canada will exchange entry records, so that an entry to one country essentially becomes an exit record from the other.

Protecting Surface Transportation

Beyond aviation, we have worked with Federal agencies and other government partners, transportation sector entities, and companies across the United States to enhance security of surface transportation infrastructure through risk-based security assessments, critical infrastructure hardening, and close partnerships with state and local law enforcement partners.

Because of its open access architecture, surface transportation has a fundamentally different operational environment than aviation. As a result, our approach must be different. To protect surface transportation, we have conducted compliance inspections throughout the freight rail and mass transit domains; critical facility security reviews for pipeline facilities; comprehensive mass transit assessments that focus on high-risk transit agencies; and Baseline Assessments for Security Enhancement conducted in multiple modes of transportation on a continuous basis to elevate standards and identify security gaps.

We continue to support surface transportation security through the deployment of 37 Visible Intermodal Prevention and Response (VIPR) teams, which include 12 multi-modal teams added in FY 2012. VIPR teams are composed of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to detect, deter, and prevent potential terrorist acts and disrupt pre-operational surveillance or planning activities.

These efforts have been supported by grant funding to harden assets, improve situational awareness, and build national capabilities to prevent and respond to threats and incidents across the transportation sector.

Global Supply Chain Security

Securing the global supply chain system is integral to securing both the lives of people around the world, and maintaining the stability of the global economy. We must work to strengthen the security, efficiency, and resilience of this critical system. Supply chains must be able to operate effectively, in a secure and efficient fashion, in a time of crisis, recover quickly from disruptions, and continue to facilitate international trade and travel.

We know that a crisis or vulnerability in any part of the world has the ability to impact the flow of goods and people thousands of miles away. Beyond loss of life and physical damage, these

events can cause large economic consequences. Therefore, our economy is dependent on our ability to secure and facilitate the flow of people and goods to and from our shores.

Within the American economy, trade with our international partners accounts for roughly one quarter of our GDP. This year alone, DHS will help facilitate about \$2 trillion in legitimate trade, while enforcing U.S. trade laws that protect the economy, the health, and the safety of the American people.

Earlier this year, the Administration announced the U.S. National Strategy for Global Supply Chain Security to set a Government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system. The National Strategy establishes two explicit goals: promoting the efficient and secure movement of goods and fostering resilient supply chain systems. As we work to achieve these goals, we will be guided by the overarching principles of risk management and collaborative engagement with key stakeholders who also have key supply chain roles and responsibilities.

DHS is now working in close partnership with other Federal departments and agencies to translate the high-level guidance contained in the Strategy into concrete actions. We are focusing our immediate efforts on the priority action areas identified in the Strategy.

In addition to the National Strategy for Global Supply Chain Security, DHS continues to advance a range of other measures and programs to strengthen different components of this vital system in partnership with multilateral organizations such as the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), the World Customs Organization (WCO), Universal Postal Union (UPU), and the Asia-Pacific Economic Cooperation (APEC) forum as well as bilaterally with trading partners.

Just last week in Montreal, I attended ICAO's ministerial conference on aviation security, where I met again with the Secretary General and counterpart ministers and reached an agreement regarding global air cargo security standards.

We are also working closely with industry and foreign government partners to identify and address high-risk shipments as early in the shipping process as possible by collecting and analyzing advance electronic commercial data. This allows DHS to make risk informed decisions about what cargo is safe to be loaded onto vessels and aircraft prior to their departure from a foreign port and facilitates the clearance of those shipments upon their arrival in the United States.

Through the Container Security Initiative (CSI), CBP works with host government customs services to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States. CSI currently operates at a total of 58 ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America—covering approximately 80 percent of all maritime containerized cargo imported into the United States. In addition, cargo that does not pass through a CSI port is screened at the National Targeting Center-Cargo and scanned by specialized CBP units located at the first port of arrival within the United States. Currently, CBP has 398 Radiation Portal Monitors (RPMs) at

priority seaports in the United States, through which approximately 99 percent of all containerized cargo volume passes.

S&T is also pursuing a number of innovative approaches to supply chain and cargo security, including maintaining maritime cargo and container integrity; tracking containers and conveyances; and, detecting and interdicting dangerous and illicit goods. Currently, S&T is piloting a land-based container and conveyance security pilot with our trading partners in Canada and Mexico. In FY 2013 we plan to expand the pilot program by conducting a maritime cargo and container security pilot with our EU colleagues.

In the aviation environment, we are working with leaders from global shipping companies and the International Air Transport Association (IATA) to develop preventive measures, including terrorism awareness training for employees and vetting personnel with access to cargo. We are reviewing our foreign partners' cargo screening to determine whether their programs provide a level of security commensurate with U.S. air cargo security standards. Those who meet these requirements are officially recognized to conduct screening for cargo traveling to the U.S. We are also building partnerships, through mutual recognition arrangements, with foreign governments maintaining industry partnership programs compatible with CBP's Customs-Trade Partnership against Terrorism. We signed a Mutual Recognition Decision with the European Union in May which will strengthen international supply chain security and facilitate trade with the EU.

DHS is also focused on preventing the exploitation of the global supply chain by those seeking to use the system to transport dangerous, illicit cargo, contraband, contaminated or counterfeit products. For example, under Program Global Shield, we are working with more than 90 countries to prevent the illegal theft or diversion of precursor chemicals that can be used to make Improvised Explosive Devices, or IEDs. Through these efforts, we have already seized more than 127 metric tons of these deadly materials.

DHS, through ICE and CBP, also continues to investigate U.S. export control law violations, including those related to military items, controlled "dual-use" commodities, and sanctioned or embargoed countries. We are committed to ensuring that foreign adversaries do not illegally obtain U.S. military products and sensitive technology, including weapons of mass destruction and their components, or attempt to move these items through the global supply chain. In FY 2011, ICE initiated 1,780 new investigations into illicit procurement activities, made 583 criminal arrests, and accounted for 2,332 seizures valued at \$18.9 million. ICE also manages and operates the Export Enforcement Coordination Center (E2C2), an interagency hub for streamlining and coordinating export enforcement activities and exchanging information and intelligence.

Securing and Managing Our Borders

DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and

streamlining lawful trade and travel; and disrupting and, in coordination with other Federal agencies, dismantling transnational criminal and terrorist organizations.

Southwest Border

To secure our Nation's Southwest border, we have continued to deploy unprecedented amounts of manpower, resources, and technology, while expanding partnerships with Federal, state, tribal, territorial, and local partners, as well as the Government of Mexico.

We have increased the number of Border Patrol agents nationwide from approximately 10,000 in 2004 to more than 21,000 today with nearly 18,500 "boots on the ground" along the Southwest border. Working in coordination with state and other Federal agencies, we have deployed a quarter of all ICE operational personnel to the Southwest border region –the most ever – to dismantle criminal organizations along the border.

We have doubled the number of ICE personnel assigned to Border Enforcement Security Task Forces (BEST), which work to dismantle criminal organizations along the border. We have tripled deployments of Border Liaison Officers, who facilitate cooperation between U.S. and Mexican law enforcement authorities on investigations and enforcement operations, including drug trafficking, in coordination with the Drug Enforcement Administration. We also have increased the number of intelligence analysts working along the U.S.-Mexico border.

In addition, we have deployed dual detection canine teams as well as non-intrusive inspection systems, Mobile Surveillance Systems, Remote Video Surveillance Systems, thermal imaging systems, radiation portal monitors, and license plate readers to the Southwest border. These technologies, combined with increased manpower and infrastructure, give our personnel better awareness of the border environment so they can more quickly act to resolve potential threats or illegal activity. We also are screening southbound rail and vehicle traffic, looking for the illegal weapons and cash that are helping fuel the cartel violence in Mexico.

We also have completed 651 miles of fencing out of nearly 652 miles mandated by Congress as identified by Border Patrol field commanders, including 299 miles of vehicle barriers and 352 miles of pedestrian fence.

To enhance cooperation among local, tribal, territorial, state and Federal law enforcement agencies, we have provided more than \$202 million in Operation Stonegarden funding to Southwest border law enforcement agencies over the past four years.

Our work along the border has included effective support from the Department of Defense (DOD). In addition to continuing support from DOD's Joint Interagency Task Force (JIATF)-North, in 2010, President Obama authorized the temporary deployment of up to 1,200 National Guard troops to the Southwest Border to contribute additional capabilities and capacity to assist law enforcement agencies as a bridge to longer-term deployment of border surveillance technology and equipment that will strengthen our ability to identify and interdict the smuggling of people, drugs, illegal weapons, and money.

Beginning in March 2012, DOD's National Guard support to CBP began to transition from ground support to air support, essentially moving from boots on the ground to boots in the air with state of the art aerial assets equipped with the latest detection and monitoring capabilities.

These aerial assets supplement the CBP Office of Air and Marine aerial assets and support the Border Patrol's ability to operate in diverse environments, expand our field of vision in places with challenging terrain, and help us establish a greater visible presence from a distance, which increases deterrence. And this year, CBP introduced an extremely effective new aviation surveillance technology to monitor the border. The U.S. Army has loaned CBP a new electronic sensor system. CBP flies Predator B unmanned aircraft systems (UASs) with this new system on the Southwest border. This system provides DHS with the first broad area, electronic sensor system, with capabilities that far exceed those of the ground based fixed or mobile systems.

The results of these comprehensive and coordinated efforts have been significant. Border Patrol apprehensions—a key indicator of illegal immigration—have decreased 53 percent in the last three years and have decreased 80 percent from what they were at their peak. Indeed, illegal immigration attempts have not been this low since 1971. Violent crime in U.S. border communities has also remained flat or fallen over the past decade according to FBI Uniform Crime Report data, and statistics have shown that some of the safest communities in America are along the border. From FYs 2009 to 2011, DHS seized 74 percent more currency, 41 percent more drugs, and 159 percent more weapons along the Southwest border as compared to FYs 2006 to 2008.

To further deter individuals from illegally crossing our Southwest border, we also directed ICE to prioritize the apprehension of recent border crossers and repeat immigration violators, and to support and supplement Border Patrol operations. Between FYs 2009 and 2011, ICE made over 30,936 criminal arrests along the Southwest border, including 19,563 arrests of drug smugglers and 4,151 arrests of human smugglers.

In addition to our efforts to strengthen border security, we made great strides in expediting legal trade and travel, working with local leaders to update infrastructure and reduce wait times at our Southwest border ports of entry. Along the Southwest border, new initiatives have included outbound infrastructure improvements and port hardening, which when completed, will expand our outbound inspection capabilities, enhance port security, and increase officer safety. We also have implemented Active Lane Management, which leverages Ready Lanes, Dedicated Commuter Lanes, and LED signage to dynamically monitor primary vehicle lanes and re-designate lanes as traffic conditions and infrastructure limitations warrant.

These efforts are not only expediting legitimate trade, they are also stopping contraband from entering and leaving the country. In FY 2011, DHS interdicted goods representing more than \$1.1 billion in Manufacturer's Suggested Retail Price. Further, the value of consumer safety seizures including pharmaceuticals totaled more than \$60 million, representing a 41 percent increase over FY 2010.

Northern Border

To protect the Northern border, we have continued to deploy technology and resources, invest in port of entry improvements to enhance security, and deepen our strong partnership with Canada.

For instance, CBP expanded unmanned aerial surveillance coverage along the Northern border into eastern Washington, now covering 950 miles of the Northern border. In 2011, CBP Office of Air and Marine provided nearly 1,500 hours of unmanned aerial surveillance along the Northern Border.

In 2011, CBP opened the Operations Integration Center in Detroit—a multi-agency communications center for DHS, and other Federal, state, local, and Canadian law enforcement agencies. The Operations Integration Center increases information sharing capabilities leading to seizures of drugs, money, and illegal contraband along the northern border within the Detroit Sector.

ICE has four BEST units along the northern border. These units, including representatives from the Royal Canadian Mounted Police, Canadian Border Services Agency and numerous other provincial Canadian police departments, enhance coordination of U.S.-Canada joint interdictions and investigations, resulting in increased security for both countries.

Recognizing the continued importance of the U.S.-Canada partnership, President Barack Obama and Canadian Prime Minister Stephen Harper released the joint declaration, *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness*, on February 4, 2011. This declaration committed the United States and Canada to pursue a perimeter approach to security, working together within, at, and away from the borders of our two countries to enhance our security and accelerate the legitimate flow of people, goods, and services between our two countries. *Beyond the Border* includes multiple Cabinet-level departments, reflecting a true interagency effort within each government and in a bi-national capacity.

Our countries have committed to improving information sharing while respecting each country's respective constitutional and legal frameworks. Specific examples of information sharing initiatives under the *Beyond the Border Action Plan* include efforts to:

- Share risk assessment/targeting scenarios, and enhance real time notifications regarding the arrival of individuals on U.S. security watchlists;
- Provide access to information on persons who have been removed or who have been refused admission or a visa from either country, as well as those who have been removed from their respective countries for criminal reasons; and
- Implement a systematic and automated biographic information sharing capability by 2013 and biometric information sharing capability by 2014 to reduce identity fraud and enhance screening decisions, and in support of other administrative and enforcement actions.

Together, these initiatives will help improve immigration and border processes and decision making, establish and verify the identities of travelers, and permit screening to be conducted at the earliest point possible.

To support the *Beyond the Border Action Plan*, in June we released the DHS Northern Border Strategy, the first unified strategy to guide the department's policies and operations along the U.S.-Canada border. Through this strategy, we will continue to work to improve information sharing and analysis within DHS, as well as with our partners. We will enhance coordination of U.S.-Canada joint interdictions and investigations, deploy technologies to aid joint security efforts along the border, and continue to update infrastructure to facilitate travel and trade. We also look forward to continuing to deepen partnerships with Federal, state, local, tribal, private sector, and Canadian partners that are so critical to the security, resiliency, and management of our Northern border.

Maritime

With more than 350 ports and 95,000 miles of coastline, the U.S. maritime domain is unique in its scope and diversity.

The Coast Guard provides maritime security using a major cutter and patrol boat fleet to respond to threats, and launch boats and aircraft to maintain a vigilant presence over the seas. Closer to shore, Coast Guard helicopters small cutters and boats monitor, track, interdict, and board vessels. In the Nation's ports, the Coast Guard and CBP, along with our Federal, state, local, and tribal partners, working in concert with other port stakeholders, monitor critical infrastructure, conduct vessel escorts and patrols, and inspects vessels and facilities.

The U.S. Coast Guard plays an integral role in DHS's border enforcement strategy through its maritime operations as part of JIATF-South, the U.S. Southern Command entity that coordinates integrated interagency counter drug operations in the Caribbean Sea, Gulf of Mexico, and the eastern Pacific. In FY 2011, Coast Guard major cutters and other assets removed over 75 metric tons of cocaine, more than 17 metric tons of marijuana, detained 191 suspected smugglers, and seized 40 vessels. Additionally, Coast Guard Law Enforcement Detachments are deployed aboard U.S. Navy and Allied assets to support detection, monitoring, interdiction and apprehension operations. CBP Office of Air and Marine P-3 and Coast Guard fixed-wing aircraft have also been an integral part of successful counter-narcotic missions operating in the Source and Transit Zones in coordination with JIATF-South. Collectively the efforts to interdict drugs in the Source and Transit Zones helped to control the flow of drugs to the Southwest border.

Robust interagency cooperation and strong international partnerships also helped the Coast Guard interdict 2,474 migrants at sea in FY 2011.

Safeguarding and Securing Cyberspace

Our daily life, economic vitality, and national security depend on a safe, secure, and resilient cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse.

Cyber incidents have increased significantly over the last decade and the United States continues to confront a dangerous combination of known and unknown vulnerabilities in cyberspace, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. There have been instances of theft and compromise of sensitive information from both government and private sector networks. Last year, the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

DHS is the Federal government's lead agency for securing civilian government computer systems and works with our industry and Federal, state, local, tribal, and territorial government partners to secure critical infrastructure and information systems. DHS analyzes and mitigates cyber threats and vulnerabilities; distributes threat warnings; provides solutions to critical research and development needs; and coordinates the vulnerability, mitigation, and consequence management response to cyber incidents to ensure that our computers, networks, and information systems remain safe. DHS also works with Federal agencies to secure unclassified Federal civilian government networks and works with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities.

With respect to critical infrastructure, DHS and the sector specific agencies work together with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. Protecting critical infrastructure requires taking an integrated approach toward physical and cyber security and ensuring that we can utilize our established partnerships with the private sector to address cyber security concerns. We do this by sharing actionable cyber threat information with the private sector, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

In addition, DHS S&T works collaboratively across Federal agencies, private industry, academic networks and institutions, and global information technology owners and operators to research, develop, test, and transition deployable solutions to secure the Nation's current and future cyber and critical infrastructures. DHS, in collaboration with the Department of State and other departments/agencies, also works with international partners on cyber threats and other cybersecurity issues, as appropriate.

To combat cyber crime, DHS leverages the skills and resources of the U.S. Secret Service (USSS) and ICE, who investigate cyber criminals and work with the Department of Justice, which prosecutes them. Within DHS, cyber crime investigations are directly led by the USSS

and involve numerous partners at the Federal, state and local level as well as the private sector. In FY 2011 alone, USSS prevented \$1.6 billion in potential losses through cyber crime investigations. Additionally, ICE HSI cyber crime investigations relating to child exploitation in FY 2011 resulted in 1,460 criminal arrests, 1,104 indictments and 928 convictions. One significant child exploitation investigation conducted by ICE HSI was Operation Delego, which resulted in prosecutors bringing charges against 72 individuals for their alleged participation in an international criminal network that sought the sexual abuse of children and the creation and dissemination of child pornography. To date, 43 of these individuals have been convicted.

DHS recognizes that partnership and collaboration are crucial to ensuring that all Americans take responsibility for their actions online. To that end, we are continuing to grow the Department's Stop.Think.Connect.™ Campaign, which is a year-round national public awareness effort designed to engage and challenge Americans to join the effort to practice and promote safe online practices.

The Department of Defense is a key partner in our cybersecurity mission. In 2010, I signed a Memorandum of Understanding with then-Secretary of Defense Robert Gates to formalize the interaction between DHS and DOD, and to protect against threats to our critical civilian and military computer systems and networks. Congress mirrored this division of responsibilities in the National Defense Authorization Act for FY 2012. We are currently working with the Defense Industrial Base to exchange actionable information about malicious activity.

As much as we are doing, we must do even more. All sides agree that Federal and private networks must be better protected, and information about cybersecurity threats must be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. DHS is committed to ensuring cyberspace supports a secure and resilient infrastructure, enables innovation and prosperity, and protects privacy and other civil liberties by design.

The Administration sent Congress a legislative package in May 2011 that included the new tools needed by homeland security, law enforcement, intelligence, military and private sector professionals to secure the Nation, while including essential safeguards to preserve the privacy rights and civil liberties of citizens. Since that time, Administration officials have testified at 17 hearings on cybersecurity legislation and presented over 100 briefings, including two all-Member Senate briefings and one all-Member House briefing.

The *Cybersecurity Act of 2012* would have begun to address vulnerabilities in the Nation's critical infrastructure systems. This legislation was the result of years of work. It reflected input from the Administration, the private sector, privacy experts, and Members of Congress from both sides of the aisle. Numerous current and former homeland and national security officials had also expressed the importance and urgency of this legislation.

The American people expect us to secure the country from the growing danger of cyber threats and ensure the Nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent. We will continue to work with the Congress – and this Committee – to pass strong cybersecurity legislation to give DHS and our partners the tools

and authorities we need to continue to protect cyberspace while also protecting privacy and civil rights.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

The Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

The DHS Privacy Office – the first statutorily required privacy office of any Federal agency – partners with every DHS component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information. To further integrate privacy and reinforce the headquarters privacy office, a team of privacy officers are embedded into the operational components throughout the Department.

DHS's Office for Civil Rights and Civil Liberties plays a key role in the Department's mission to secure the Nation while preserving individual freedoms and represents the Department's commitment to the idea that core civil rights values—liberty, fairness, and equality under the law—are a vital part of America, and that these values provide a bulwark against those who threaten our safety and security.

Since its inception, CRCL has expanded its participation in programs and activities throughout the Department and continued its efforts to promote civil rights and civil liberties. For example, CRCL collaborates with ICE on detention reform and other immigration-related efforts, and works with TSA to ensure that evolving aviation security measures are respectful of civil rights and civil liberties.

CRCL's community engagement efforts include a wide variety of stakeholders and organizations through regular roundtables and other tools across the country. CRCL has also expanded its training capacity and worked closely with the DHS Privacy Office and the Office of Intelligence and Analysis to offer civil rights and civil liberties training for fusion centers, as well as training to a number of the Department's Federal, state, and local partners.

Conclusion

While America is stronger and more resilient as a result of these efforts, threats from terrorism persist and continue to evolve. Today's threats do not come from any one individual or group. They may originate in distant lands or local neighborhoods. They may be as simple as a homemade bomb or as sophisticated as a biological threat or coordinated cyber attack.

As threats to our Nation evolve, DHS must also evolve. Thus, we continue to remain vigilant, protecting our communities from terrorist threats, while promoting the movement of goods and people and maintaining our commitment to civil rights and civil liberties.

I thank the Committee for your continued partnership and guidance as together we work to keep our Nation safe. I look forward to your questions.

Hearing before the Senate Committee on Homeland Security and Government Affairs
The Homeland Threat Landscape and U.S. Response
September 19, 2012

The Honorable Matthew G. Olsen
Director
National Counterterrorism Center

Thank you Chairman Lieberman, Ranking Member Collins, members of the Committee. I appreciate this opportunity to be here today to discuss the terrorist threat against the United States and our efforts to counter it.

I also want to express my appreciation to the Committee for your steadfast leadership and your support of the National Counterterrorism Center (NCTC). I am particularly pleased to be here today with Secretary Napolitano and Director Mueller. We are close partners in the fight against terrorism.

I have now served as the Director of the National Counterterrorism Center for just over a year. During this year—with the support and guidance of Congress—our nation has made significant progress in the fight against terrorism. Our nation has placed relentless pressure on al-Qa'ida core's senior leadership. We have denied the group safe havens, resources, and the ability to plan and train. Following the death last year of Usama bin Ladin, several of his top lieutenants have been eliminated. Leaders who remain lack the same experience and are under siege. They have limited ability to recruit and communicate with other operatives. In short, the intelligence picture shows that al-Qa'ida core is a shadow of its former self, and the overall threat from al-Qa'ida in Pakistan is diminished.

Further, the government has disrupted terrorist attacks in the United States and abroad. Our intelligence, military, and law enforcement officers have worked to identify and stop terrorist plots before they are executed. And we have investigated and prosecuted individuals who have sought to carry out and have supported terrorist operations.

In addition, we have continued to build an enduring counterterrorism framework. NCTC—along with the FBI and DHS—is dedicated to analyzing and sharing terrorism information across the government and to the mission of detecting and preventing terrorist attacks against our citizens and interests around the world.

While these gains are real and enduring, al-Qa'ida, its affiliates and adherents around the world—as well as other terrorist organizations—continue to pose a significant threat to our country. This threat is resilient, adaptive, and persistent.

Now more than a decade after the September 11th attacks, we remain at war with al-Qa'ida, and we face an evolving threat from its affiliates and adherents, who rally around the al-Qa'ida brand. Indeed, the threats we face have become more diverse. As al-Qa'ida's core leadership struggles to remain relevant, the group has turned to its affiliates and adherents to carry out attacks and to advance its ideology. These groups are based in an array of countries, including Yemen, Somalia, Nigeria, and Iraq. To varying degrees, these groups coordinate their activities and follow the direction of al-Qa'ida leaders in the Afghanistan-Pakistan border region.

UNCLASSIFIED

Many of the extremist groups themselves are multidimensional, blurring the lines between terrorist group, insurgency, and criminal gang. Unrest and political uncertainty from Northern Mali to the Sinai can present opportunities terrorists can exploit and areas from which they can operate.

Confronting this threat and working with resolve to prevent another terrorist attack is NCTC's overriding mission. We continue to monitor threat information, develop leads, work closely with domestic and international partners, and develop strategic plans to combat our terrorist adversaries. While we have taken important steps against al-Qa'ida and other terrorist groups, much work remains. The dedicated professionals at NCTC, along with our partners across the government and overseas, remain steadfast and committed to sustaining and enhancing the effort to protect the nation.

In my statement, I will begin by examining the terrorist threats to the homeland and to U.S. interests. I will then describe NCTC's role in addressing these threats and some of the key reforms and initiatives we have adopted.

The Terrorist Threat in Transition

Pakistan-Based Al-Qa'ida Core

Over the past several years, sustained counterterrorism pressure has systematically degraded Pakistan-based al-Qa'ida's leadership and operational capabilities. These efforts have left the group at its weakest point in the last ten years. Although core al-Qa'ida remains committed to its overarching goals, it is clearly a group in decline.

The death of Usama bin Ladin on May 2, 2011 removed al-Qa'ida's founder and leader and its staunchest proponent of spectacular attacks against the U.S. . The subsequent losses of several of Bin Ladin's top lieutenants and senior operational planners—including general manager 'Atiyah 'Abd al-Rahman in August 2011 and his replacement Abu Yahya al-Libi this June—have eroded the group's bench of potential leaders and have shaken al-Qa'ida's sense of security in Pakistan's tribal areas. Remaining leaders have been driven underground to varying degrees and the group has shifted a substantial portion of its attention from terrorist plotting to security and survival.

Operationally, core al-Qa'ida has not conducted a successful operation in the West since the 2005 London bombings. The group, however, remains committed to striking Western targets, including the United States. Its degraded capabilities almost certainly will compel operational planners to place a greater emphasis on smaller, simpler plots that are easier to carry out against soft targets.

Since Bin Ladin's death, multiple al-Qa'ida leaders have publicly endorsed the concept of individual acts of violence. We remain concerned that individuals such as alleged Fort Hood shooter Nidal Hassan and Toulouse shooter Mohammed Merah may inspire other like-minded individuals to conduct attacks in al-Qa'ida's name.

Despite its shrinking leadership cadre, al-Qa'ida continues to issue propaganda and media statements specifically focused on the Arab unrest. Persistent unrest in places such as Yemen, Libya, Egypt, and Syria may also provide core al-Qa'ida a propaganda opportunity to claim victories over the United States and reinvigorate its image as the leader of the global movement.

Al-Qa'ida's Affiliates: A Persistent and Diversifying Threat to the U.S. and Overseas Interests

AQAP. Al-Qa'ida in the Arabian Peninsula (AQAP) remains the affiliate most likely to attempt transnational attacks, including against the United States. Despite Anwar al-Aulaqi's death, the group maintains the intent and capability to conduct anti-U.S. attacks with little to no warning.

In its three attempted attacks against the U.S. Homeland—the airliner plot of December 2009, an attempted attack against U.S.-bound cargo planes in October 2010, and an airliner plot this May—AQAP has shown an awareness of Western security procedures and demonstrated its efforts to adapt. The death of al-Aulaqi probably temporarily slowed AQAP's external plotting efforts but did not deter the group from attempting another aviation attack in May. We are also concerned by AQAP's efforts to exploit the security vacuum associated with the Arab Spring, although the group has suffered recent setbacks in these efforts.

AQAP also remains intent on publishing the English-language *Inspire* magazine—previously spearheaded by al-Aulaqi and now-deceased Samir Khan—in order to mobilize Western-based individuals for violent action. While the deaths of al-Aulaqi and Khan have affected the quality of the magazine, the publication endures and continues to reach a wide global audience of extremists.

AQIM and Boko Haram. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) and Boko Haram remain focused on local and regional attack plotting, including targeting Western interests in Nigeria. The groups have shown minimal interest in targeting the U.S. Homeland.

AQIM is actively working with local extremists in northern Mali to establish a safe haven from which to advance future operational activities. We are watching developments closely including the presence of militants in Niger; AQIM's ability to operate from a safe haven could eventually threaten U.S. and allied interests. While Boko Haram is primarily focused on plotting against targets in Nigeria, in April a spokesman for the group publicly threatened to find a way to attack a U.S.-based news outlet if its coverage of Islam did not change.

Al-Qa'ida in Iraq. Since the withdrawal of U.S. forces from Iraq late last year, Al-Qa'ida in Iraq (AQI) has conducted near-monthly country-wide attacks against government, security, and Shia civilian targets. During the past two years AQI has continued to release media statements supporting global extremism.

AQI's propaganda statements have cited its support for uprisings against secular governments in the Middle East and North Africa and, in a June statement, the group expressed solidarity with the Syrian Sunni population. In January 2011, it published an explosives training

video that called for lone wolf attacks in the West and against so-called apostate regimes in the Middle East.

During the past two years, American and Canadian authorities have arrested several North America-based AQI operatives, highlighting the potential threat posed to the United States. The FBI in May 2011 arrested Kentucky-based Iraqi refugees Waad Alwan and Shareef Hamadi for attempting to send weapons and explosives from Kentucky to Iraq and conspiring to commit terrorism while in Iraq. Alwan pled guilty to supporting terrorism in December 2011; Hamadi pled guilty just last month. In January 2011, Canadian authorities arrested dual Iraqi-Canadian citizen Faruq 'Isa who is accused of vetting individuals on the internet for suicide operations in Iraq.

Al-Shabaab. We continue to monitor al-Shabaab and its foreign fighter cadre as a potential threat to the U.S. homeland, although the group is mainly focused on combating the ongoing African Mission in Somalia (AMISOM) and regional military incursions which have eroded the group's territorial safe haven since late last year.

The group, which formally merged with al-Qa'ida in February, also remains intent on conducting attacks against regional and Western targets in East Africa, especially in countries supporting the Somali Government and allied forces in Somalia. Probable al-Shabaab sympathizers conducted several low-level attacks in Kenya earlier this year. Some al-Shabaab leaders in the past have publicly called for transnational attacks, including threatening to avenge the January death of British national and al-Shabaab senior foreign fighter Bilal Berjawi.

Al-Shabaab has attracted foreign fighters from across the globe, including more than 20 U.S. persons – mostly ethnic Somalis – who have traveled to Somalia since 2006.

Other Terrorist Threats

Lebanese Hizballah. Lebanese Hizballah has intensified its terrorist activities around the world and we remain concerned the group's activities endanger U.S. interests and citizens, as well as our allies.

Since May 2008, Hizballah plots against Israeli targets in Azerbaijan, Egypt, and Israel have been disrupted, and additional operational activity in Turkey has reportedly been uncovered. The mid-July attack on an Israeli tourist bus in Burgas, Bulgaria that killed six, the early July arrest of an operative in Cyprus, and the January plotting against tourists in Bangkok all bear the hallmarks of Hizballah. The group has engaged in an increasingly aggressive terrorist campaign since the end of its 2006 war with Israel and probably accelerated by the death of its operations chief 'Imad Mughniyah in Syria in 2008.

Since the start of unrest in Syria in early 2011, Hizballah has also provided training and extensive logistical support to the Government of Syria. The Treasury Department recently designated Hizballah for providing support to the Government of Syria.

Syria. We are monitoring the activities of several groups in Syria, including the development there of a terrorist group known as al-Nusra Front, which announced its existence in a January video posted on extremist-affiliated web forums. The group has styled itself as the defender of Syrian Sunnis in propaganda statements. Al-Nusra has openly claimed suicide, car bomb, coordinated assault, and small arms attacks against Syrian regime targets.

Multiple actors are now present in Syria and we are focused on any non-state actors inside or outside of Syria who may seek to acquire Syria's now-acknowledged chemical weapons stockpile. The U.S. is monitoring the weapons sites and remains concerned about the security of these weapons especially with the escalation of violence in Syria. We're working closely with the National Counterproliferation Center (NCPC), through our joint WMD-Terrorism Office, stood up this year, to monitor and help counter those who may seek to acquire Syria's weapons.

Additionally, unaccounted for conventional Libyan weapons pose a regional threat if they proliferate to non-state actors and make their way onto the Syrian battlefield. The Libyan regime stored conventional weapons in hundreds of unsecured locations throughout the country which included at least 20,000 MANPADS, not all of which have been recovered.

Iranian Threat. Iran is still the foremost state sponsor of terrorism, and since 9/11 the regime has expanded its involvement with terrorist and insurgent groups—primarily in Iraq and Afghanistan—that target U.S. and Israeli interests. The threat to U.S. interests from Iranian or Iranian-sponsored terrorist attacks has increased in the past year.

The disrupted Iranian plot to assassinate the Saudi Ambassador to the United States in late 2011 demonstrates that Iran is more willing to conduct terrorist operations inside the United States than was previously assessed. As part of the plot, the Islamic Revolutionary Guard Corps-Qods Force attempted to use a dual Iranian-U.S. national to recruit Mexican criminal organizations to conduct the assassination, raising our concerns that Iran may seek to leverage its growing ties to Latin America to conduct activities in the U.S. Iran has recently been linked to terrorist operations in Azerbaijan, Georgia, India, and Thailand.

Iran's Islamic Revolutionary Guard Corps-Qods Force and Ministry of Intelligence and Security have been involved in the planning and execution of terrorist acts and the provision of lethal aid—such as weapons, money, and training—to these groups, in particular Lebanese Hezbollah. Hezbollah has directly trained Syrian government personnel inside Syria and has facilitated the training of Syrian forces by Iran's terrorist arm, the Islamic Revolutionary Guard Corps - Qods Force (IRGC-QF). Iran's relationship with Hezbollah has gradually evolved since the 1980s from a traditional state sponsor-proxy relationship to a strategic partnership, both pursuing their aims against Israel and the United States.

South Asia-Based Militants. Pakistani and Afghan militant groups – including Tehrik-e Taliban Pakistan (TTP), the Haqqani Network, and Lashkar-e Tayyiba (LT) – continue to pose a direct threat to U.S. interests and our allies in the region, where these groups probably will remain focused. We continue to watch for indicators that any of these groups, networks, or

individuals are actively pursuing or have decided to incorporate operations outside of South Asia as a strategy to achieve their objectives.

TTP's claim of responsibility for the 16 August attack on Pakistan's Kamra air base and its threat to attack Coalition supply lines through Pakistan underscore the threat the group poses in the region. TTP leaders have repeatedly threatened attacks against the United States, including after the death of Bin Ladin in May 2011. TTP's claim of responsibility for the failed Times Square bombing in May 2010 demonstrates its willingness to act on this intent.

The Haqqani Network continues a campaign of high profile attacks in Afghanistan and has conducted multiple attacks against NATO and Afghan Government targets, notably the 18-hour multi-pronged assault against military, security, and government facilities in Kabul and three other cities in April. Earlier this month, the Secretary of State notified Congress of the Administration's intent to designate the Haqqani Network as a Foreign Terrorist Organization under the Immigration and Nationality Act and as a Specially Designated Global Terrorist Entity under Executive Order 13224. Moreover, we remain concerned by the Haqqani Network's ability to provide facilitation and safe haven for local and global groups such as al-Qa'ida and to enable these groups to influence one another.

LT leaders have maintained a regional focus. LT provides training to a wide range of Pakistani and Western militants, some of whom could plot terrorist attacks in the West without direction from LT leaders. LT members frustrated with the group's focus on South Asia likewise could leave LT to join a more globally focused group such as al-Qa'ida. LT leaders almost certainly recognize that an attack on the U.S. would bring intense international backlash upon Pakistan and endanger the group's safehaven there.

LT has demonstrated a willingness to attack Western interests in South Asia in pursuit of its regional objectives, as it did through a high-profile operation targeting hotels frequented by Westerners during the Mumbai attacks in 2008.

The Evolving Threat from Homegrown Violent Extremists

Homegrown violent extremists (HVEs), including those who are inspired by al-Qa'ida's ideology, continue to pose a threat to the United States. HVEs inspired by al-Qa'ida are almost certainly entering a period of transition as U.S.-based violent extremists adjust to the deaths and disruption of influential English-language figures who helped al-Qa'ida's ideas resonate with some in the U.S.

Now-deceased AQAP members Anwar al-Aulaqi and Samir Khan were probably best positioned to create propaganda specifically for an American audience and mobilize HVEs. Their propaganda remains easily accessible online and will likely continue to inspire HVE violence.

The growth of on-line English language violent extremist content during the past three years has fostered a shared identity—but not necessarily operational collaboration—among

HVEs. Plots disrupted during the past year were unrelated operationally, but may demonstrate a common cause in rallying independent violent extremists to plot against the U.S.

Lone actors or insular groups pose the most serious HVE threat to the homeland. HVEs could view lone offender attacks as a model for future plots in the United States and overseas. The perceived success of previous lone offender attacks combined with al-Qa'ida and AQAP's propaganda promoting individual acts of terrorism is raising the profile of this tactic.

The arrests last year of Texas-based Saudi Khalid Aldawsari and U.S. Army Private First Class Naser Abdo, as well as attacks in France, underscore the threat from lone offenders who are able to adapt their plans quickly by rapidly changing timelines, methods, and targets to meet existing circumstances—all without consulting others.

THE ROLE OF NCTC

NCTC's Core Missions

The overarching mission of NCTC is to lead the effort to combat international terrorism. In 2004, the 9/11 Commission observed that “the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative and agile responses.” That observation—as true today as it was in 2001—led the Commission to recommend the creation of a National Counterterrorism Center which should “break the mold of a national government organization” and be a center for joint strategic operational planning and joint intelligence.

In 2004 Congress established NCTC and set forth the Center's key responsibilities. These responsibilities are captured in NCTC's mission statement: “Lead our nation's effort to combat terrorism at home and abroad by analyzing the threat, sharing that information with our partners, and integrating all instruments of national power to ensure unity of effort.”

Intelligence Integration and Analysis. NCTC serves as the primary organization in the U.S. government for integrating and assessing all intelligence pertaining to international terrorism and counterterrorism. NCTC has a unique responsibility to examine all international terrorism issues, spanning geographic boundaries to identify and analyze threat information, regardless of whether it is collected inside or outside the United States.

NCTC has access to the full catalogue of reporting—both foreign and domestic—on international terrorism issues. NCTC's strategic analyses are vetted and coordinated throughout the intelligence community, which adds multiple analytic perspectives. NCTC produces coordinated assessments on such critical terrorism issues as terrorist safe havens, state sponsors of terrorism, counterterrorism cooperation worldwide, and regional terrorism issues and groups. NCTC also regularly prepares intelligence assessments that are integrated into NCTC's Directorate of Strategic Operational Planning to inform policymakers on the progress of U.S. counterterrorism efforts.

NCTC's analytic cadre includes detailees and assignees from across the intelligence community and government, ensuring NCTC products reflect the diversity of the entire intelligence community and not the analytic view of one group or agency.

Watchlisting. NCTC hosts and maintains the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. NCTC has developed and maintains the Terrorist Identities Datamart Environment (TIDE) on known and suspected terrorists and terrorist groups. In this role, NCTC advances the most complete and accurate information picture to our partners to support terrorism analysts. We also support screening and law enforcement activities that ultimately help prevent terrorist plans and operations against U.S. interests.

Situational Awareness and Support to Counterterrorism Partners. NCTC supports our counterterrorism partners at both the federal and state and local levels.

In particular, our unique, centralized access to intelligence information on terrorist activity enables our analysts to integrate information from foreign and domestic sources and to pass that information in a timely manner to other agencies. Below are several examples:

- NCTC provides around-the-clock support to domestic counterterrorism activities through the NCTC Operations Center, which is co-located with FBI Counterterrorism Division Watch. NCTC produces and disseminates daily situational awareness products and chairs secure video teleconferences three times a day to facilitate timely information exchanges between counterterrorism partners.
- The Interagency Threat Assessment and Coordination Group (ITACG), located at NCTC, led by senior DHS and FBI officers, and reporting to NCTC, brings together federal and non-federal intelligence, law enforcement, and first responder detailees, who are dedicated to providing relevant intelligence to state, local, tribal, and private sector partners. ITACG ensures that shared information is timely, relevant, and framed into situational awareness products for public safety officials—including police officers and firefighters—enhancing their capabilities to quickly assess and effectively respond to suspected and actual terrorist activities. In response to potential Congressional action to eliminate DHS' funding for the ITACG, we are exploring with FBI and DHS ways to preserve and sustain key counterterrorism intelligence functions within NCTC, and to complement DHS and FBI's efforts. Our role is to integrate information and to ensure it can be shared with the people who need to know.
- NCTC facilitates the dissemination of information at unclassified levels to support DHS and FBI efforts to inform law enforcement and local officials of potential dangers to include near-real-time export of watchlist data to the FBI's Terrorist Screening Center.
- NCTC provides threat information to DHS regarding individuals who have been identified as overstaying their visas in the United States, and we work regularly with

DHS and FBI to provide briefs to federal, state and local officials at Fusion Centers regarding counterterrorism matters.

- NCTC ensures the timely dissemination of finished intelligence and situational reporting via the NCTC Online CURRENT—the premier classified website and repository for counterterrorism reporting and analysis. The site is available on multiple platforms with more than 10,000 monthly users from 45 different organizations, including FBI-led Joint Terrorism Task Forces (JTTFs). It is also available on DHS's Homeland Secure Data Network to certain state and local officials in the fusion centers.

Strategic Operational Planning. NCTC is charged with conducting strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities. In this role, NCTC looks beyond individual department and agency missions toward the development of a single, unified counterterrorism effort across the federal government. NCTC develops interagency counterterrorism plans to help translate high level strategies and policy direction into coordinated department and agency activities to advance the President's objectives.

These plans address a variety of counterterrorism goals, including regional issues, weapons of mass destruction-terrorism, and countering violent extremism. The strategic operational planning process integrates all phases of the planning cycle—developing a plan, monitoring its implementation, and assessing its effectiveness and resource allocations—and creates communities of interest to coordinate and integrate implementation.

For example, NCTC is joining with DHS and the FBI to conduct workshops across the United States that enable cities to better develop and refine their response plans to evolving terrorist threats. These "Joint Counterterrorism Awareness Workshops" increase the ability of federal, state, local and private sectors partners to respond to a threat by discovering gaps in capabilities, planning, training and resources, as well as identify existing programs or resources that can close those gaps. The workshops also provide a venue to share best practices at the state and local levels and serve as a basis for identifying issues and gaps that may subsequently be addressed nationwide. We have held these workshops in a number of major U.S. cities, most recently in Los Angeles.

Key NCTC Initiatives

Facing a dynamic and complex terrorist environment, NCTC is changing and adapting to build on the past several years of experience to meet these threats and the challenges they present. With lessons learned from AQAP's December 2009 failed airline bombing and other plots, NCTC has implemented several key initiatives to advance our ability to identify and prevent terrorist attacks.

Information Sharing. NCTC is promoting information integration and sharing across the counterterrorism community with the development of the Counterterrorism Data Layer (CTDL). The CTDL provides NCTC users with a single access point to millions of pieces of government counterterrorism-related data gathered from multiple government data sets. Prior to

December 2009 analysts were required to search multiple networks and integrate this information manually, making it difficult to identify and explore potential links of relevance. Different formats, information fields, and naming conventions further complicated our efforts. Now, NCTC's data systems are being developed to ingest relevant data and to allow NCTC analysts to identify, search, exploit, and correlate terrorism information in a single environment.

Thanks to the support of our key counterterrorism partners, including DHS and the FBI, NCTC is also making significant progress in acquiring priority data sets. Today, thanks to NCTC's unique access to all terrorism-related intelligence possessed or acquired by the government, NCTC analysts can search across key homeland security and intelligence information and get back a single list of relevant results. Moreover, sophisticated analytical tools are in place to permit analysts to conduct analytic searches, conduct link analysis and data visualization, and triage information – all designed to identify potential threats at the earliest possible moment.

As a part of this effort, I would note that the FISA Amendments Act – which authorizes intelligence agencies to collect invaluable intelligence regarding international terrorists, cybercriminals, and weapons proliferators by targeting non-Americans overseas – is set to expire at the end of this year. These provisions were thoughtfully crafted and carefully implemented to ensure the privacy and civil liberties of Americans are protected. Reauthorizing this legislation is critical and must be done as soon as possible to avoid any gap in our collection capabilities.

Finally, we are committed to handling data in a manner that retains the trust of the American people and remains true to the oaths we have taken to support and defend the Constitution. Specifically, we protect information through procedures approved by the Attorney General under Executive Order 12333, and we adhere to the requirements of the Privacy Act. In fact, our recently updated Attorney General Guidelines) incorporates a series of additional safeguards, oversight mechanisms, and reporting requirements designed to ensure we protect civil liberties and privacy when executing our mission. Compliance with these protections is reviewed at several levels—including NCTC's Civil Liberties and Privacy Officer, ODNI's Office of General Counsel, ODNI's Civil Liberties and Privacy Office, and the Intelligence Community Office of Inspector General.

Pursuit Group. NCTC created the Pursuit Group to develop tactical leads and pursue terrorism threats. The formation of the Pursuit Group has provided the counterterrorism community with a group of co-located analysts that have unparalleled data access and expertise, enabling the Pursuit Group to focus exclusively on information that could lead to the discovery of threats aimed against the homeland or U.S. interests abroad.

With teams comprised of personnel from across the intelligence community, with access to the broadest range of terrorism information available, Pursuit Group analysts are able to identify actionable leads that could otherwise remain disconnected or unknown. Pursuit Group analysts can ensure that terrorism cases are examined as thoroughly as possible by pursuing non-obvious and unresolved connections, identifying unknown, known or suspected terrorists, and focusing on seemingly unimportant details that could yield relevant information. The Pursuit

Group provides investigative leads, collection requirements, and potential source candidates to operational elements such as the FBI, CIA, or DHS for intelligence purposes or action.

Watchlisting and TIDE Enhancements. NCTC has adopted important reforms in the watchlisting process and has improved NCTC's receipt, processing, and quality of information sharing in support of the Center's watchlisting and screening responsibilities. One of the key gaps we identified in the watchlisting process was the need to enhance existing TIDE records with additional information. NCTC is now taking a more aggressive and innovative approach to seek methodologies and data repositories to ingest biographic, biometric, and derogatory information. As the threat continues to evolve, our watchlisting experts are proactively working with NCTC's Pursuit Group and the counterterrorism community to expedite the sharing of information to build more complete terrorist identities. We have also enhanced our ability to store, compare, match, and export biometrics such as fingerprint, facial images, and iris scans.

The community watchlisting guidance was revised in 2010 to provide flexibility to push forward information that previously had not met the requirements. Nevertheless, nominations of U.S. persons to a watchlist must still be supported by "reasonable suspicion" that the person is a "known or suspected terrorist," and a person cannot be watchlisted based solely upon a First Amendment protected activity.

NCTC Domestic Representatives. NCTC has developed a domestic representative cadre, deploying officers to serve as counterterrorism liaison representatives in seven cities around the country. These officers partner with FBI-led JTTFs and with fusion centers, bringing the national counterterrorism intelligence picture to regional federal, state, and local officials. The NCTC representatives engage with counterterrorism partners at all levels and provide analytic insights drawn from the full catalogue of counterterrorism intelligence collection. Based on the positive feedback we have received about this program, we are sending representatives to two additional cities and will be aligned with the DNI domestic representative program to provide nationwide coverage.

Countering Violent Extremism. As our understanding of the threat evolves, so too must our approach to defeating it. Over the past ten years, the government has expanded its counterterrorism efforts to include a focus on preventing al-Qa'ida and its adherents from recruiting and radicalizing to violence the next generation of terrorists. We recognize that al-Qa'ida's recruitment is not constrained by geographical boundaries, which is why we are working closely with U.S. government partners both overseas and at home. We also recognize that communities are best placed to identify and prevent recruitment efforts.

Therefore, working side by side with FBI, DHS, DOJ, State, and DoD, we are building whole-of-government approaches focusing on expanding government and community understanding of all forms of violent extremism, including al-Qa'ida-inspired radicalization to violence. Domestically, in partnership with DHS and FBI, NCTC developed a "Community Awareness Briefing" to inform members of American communities about the threat of terrorist recruitment and to facilitate discussions with those communities about their role as potential catalysts in efforts to counter the al-Qa'ida narrative. NCTC is working with federal, state, and local partners to broadly disseminate the briefing to communities around the country. We are

II

UNCLASSIFIED

also working with DHS and FBI to work with local law enforcement on approaches to community engagement in this context. Internationally, NCTC works with our colleagues at the State Department to support CVE work in embassies across Europe, North Africa and South Asia.

NCTC continually examines al-Qa'ida-inspired violent radicalization in order to understand and track this dynamic threat. We published the Radicalization Dynamics Primer, which includes a new framework that describes the process of radicalization, mobilization, and engagement in violent action for al-Qa'ida- inspired individuals. The Primer was coordinated throughout the Intelligence Community, and is intended as a reference guide for U.S. policymakers, law enforcement officers, and analysts—including civilian and military personnel—who assess or take action on radicalization to violence trends in their areas of responsibility. NCTC, in collaboration with FBI and DHS, also developed a training curriculum to enable law enforcement and government agencies to more effectively identify, counter, and report on violent extremists in the homeland. Several hundred federal, state, local government and law enforcement representatives across the country have received the training and given it positive reviews.

* * *

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for the opportunity to testify before you this morning.

The talented men and women who work at NCTC perform a unique and vital service to the nation, and we benefit from the integration of analysts and planners from across the intelligence community, the military, and other federal, state, and local partners. As NCTC bolsters its efforts to meet the challenges ahead, our progress is dependent on our diverse and dedicated workforce. Maintaining this workforce—through continued commitment and support from the FBI, DHS and other organizations—is a priority for the Center.

The men and women I am privileged to represent appreciate this Committee's interest and guidance as they work around the clock to identify and disrupt potential terrorist threats. Thank you for your continued support of our mission.



Department of Justice

STATEMENT OF

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

“HOMELAND THREATS AND AGENCY RESPONSES”

PRESENTED

SEPTEMBER 19, 2012

**Statement of
Robert S. Mueller, III
Director
Federal Bureau of Investigation**

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

**At a Hearing Entitled
“Homeland Threats and Agency Responses”**

**Presented
September 19, 2012**

Good morning, Chairman Lieberman, Ranking Member Collins, and Members of the Committee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

As you know, the Bureau has undergone unprecedented transformation in recent years. Since the attacks of September 11th, we have refocused our efforts to address and prevent emerging terrorist threats. The terrorist threat is more diverse than it was 11 years ago, but today, we in the FBI are better prepared to meet that threat.

We also face increasingly complex threats to our nation’s cyber security. Nation-state actors, sophisticated organized crime groups, and hackers for hire are stealing trade secrets and valuable research from America’s companies, universities, and government agencies. Cyber threats also pose a significant risk to our nation’s critical infrastructure.

As these threats continue to evolve, so too must the FBI change to counter those threats. We must continue to build partnerships with our law enforcement and private sector partners, as well as the communities we serve. Above all, we must remain firmly committed to carrying out our mission while protecting the civil rights and civil liberties of the people we serve.

Counterterrorism

Counterterrorism remains our top priority.

International Terrorism

We face a fluid, dynamic, and complex terrorist threat. We have seen an increase in the sources of terrorism, a wider array of terrorism targets, a greater cooperation among terrorist groups, and an evolution in terrorist tactics and communications methodology.

In the past decade, Al Qaeda has become decentralized, but the group remains committed to high-profile attacks against the West. Records seized from Osama bin Laden's compound more than one year ago confirm Al Qaeda's intent. The May 2012 conviction of an Al Qaeda operative who plotted to conduct coordinated suicide bombings in the New York City subway system emphasizes the reality of the threat.

Our experience has been that several key al Qaeda in the Arabian Peninsula (AQAP) figures were born or educated in the United States; they understand our culture and our security protocols, and they use this understanding to develop and refine new tactics and techniques for their proposed attacks. Al Qaeda affiliates and surrogates, especially AQAP, represent the top counterterrorism threat to the nation. These groups have attempted several attacks on the United States, including the failed Christmas Day airline bombing in 2009, and the attempted bombing of U.S.-bound cargo planes in October of 2010.

AQAP leaders have published English-language articles in the Internet detailing their intent to strike the United States. They are also making use of social media to share their knowledge with individuals of similar mindsets. They realize the value of reaching English-speaking audiences, and are using the group's marketing skills to inspire individuals to undertake attacks in the United States, without having to travel or train abroad.

We also remain concerned about the threat from homegrown violent extremists. Over the past few years, we have seen increased activity among extremist individuals. These individuals have no typical profile; their experiences and motives are often distinct. But they are increasingly savvy and willing to act alone, which makes them difficult to find and to stop.

For example, in February 2012, the FBI arrested Amine El Khalifi, a 29-year-old Moroccan immigrant, for allegedly attempting to detonate a bomb in a suicide attack on the U.S. Capitol. According to court documents, Khalifi believed he was conducting the terrorist attack on behalf of Al Qaeda, although he was not directly affiliated with any group.

Another example is the case of Rezwan Ferdaus, a 26-year-old U.S. citizen and graduate student living in Boston, Massachusetts. During the fall of 2011, Ferdaus planned to use unmanned, remote-controlled aircraft to attack locations in Washington, D.C., including the U.S. Capitol. Although he espoused loyalty to Bin Laden and al Qaeda, Ferdaus was not affiliated with any group or other would-be terrorists. He had become radicalized on his own, influenced

by radical websites advocating violent extremism, among other things. In July, Ferdaus agreed to plead guilty to attempting to damage and destroy a federal building by means of an explosive and attempting to provide material support to terrorists. The agreement is subject to review and acceptance by the district court.

To better address this evolving threat, the FBI has established a Countering Violent Extremism (CVE) Office within the National Security Branch (NSB) that will improve our effectiveness in empowering our state, local, and community partners to assist in this effort. The duties and goals of this office include developing a better understanding of, and countering the threat of, violent extremism in the United States; strengthening community partnerships; providing to state and local officials and to community leaders unclassified briefings regarding the threat of violent extremism; addressing CVE-related operational and mission-support needs, including investigations, analysis, and training; and coordinating the FBI's interests with regard to CVE matters with those of other agencies to ensure that the efforts of the U.S. government are aligned.

Webster Commission Report on Fort Hood

In 2009, following the attack on Fort Hood, the FBI requested a full - and independent - investigation of the manner in which the FBI handled and acted on counterterrorism intelligence before and after the Fort Hood shootings. Former FBI Director William Webster agreed to undertake that independent review. On July 19, 2012, Judge Webster delivered to the FBI the completed Webster Commission Report on Fort Hood.

The Commission found shortcomings in FBI policy guidance, technology, information review protocols, and training, and made 18 recommendations for corrective and enhancing measures in those areas. The FBI concurs with the principles underlying the recommendations and has already taken action – and had taken action, even prior to the release of the report – to implement the recommendations based on a combination of the Commission's work, the FBI's own internal review of the Fort Hood shootings, and the report of this Committee.

The Webster Commission reported that it was impressed with the quality and the commitment of the FBI's intelligence analysts and the integration of analysts into the FBI's work. The FBI has taken significant steps to strengthen the integration of intelligence and operations, and we will continue to examine innovative ways to continue our transformation from an investigative-led model to an intelligence-led model, where intelligence drives our investigative strategies, enhances our understanding of threats, and increases our ability to address and mitigate those threats. The Directorate of Intelligence will continue to evolve to more effectively provide strategic direction, oversight and support to the FBI's Intelligence Program as we expand the intelligence components in each of our operational divisions.

Domestic Terrorism

In addition to the threats related to international terrorism discussed above, we confront domestic terrorism – domestic acts of violence in furtherance of political, religious, racial, or social ideology. Unfortunately, we have seen a surge in lone offender incidents, as we witnessed with the shooting at the Sikh Temple in Wisconsin.

Many lone offenders may have some affiliation with known domestic terrorist organizations, such as violent white supremacist groups, anarchists, animal rights and environmental extremists, and militia groups, whose activities may violate federal law. These lone offenders may be loosely affiliated with such groups, but their actions typically are not directed by these groups. They may be self-trained, self-financed, and self-executing, but they are motivated to take action in furtherance of their ideological beliefs.

We in the FBI maintain comprehensive coverage of known domestic terrorist groups and their general membership. But lone offenders pose a significant concern in that they stand on the periphery.

We are working closely with our counterparts in the Department of Homeland Security to educate our law enforcement, private sector, and community partners to be on the lookout for suspicious individuals and activities. We want our partners to be attuned to the threat of domestic terrorism, whether by known groups or lone offenders, and to know how best to reach out to law enforcement for assistance.

In addition, each JTTF across the country includes Special Agents dedicated to investigating domestic terrorism. We are working with the Bureau of Prisons to combat violent radicalization of incarcerated individuals by groups with a wide range of underlying ideologies. We are also working with the Department of Defense to identify members of the military who may be affiliated with and attempt to assist or join groups engaged in terrorist activity.

In every domestic terrorism investigation – and indeed, in every investigation – we in the Bureau strive to balance our need to keep the American public safe with the constitutional rights of every citizen, including their First Amendment rights to free speech and freedom of assembly.

Cyber Security

As this Committee knows, the cyber threat has evolved and grown significantly over the past decade. Foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property — information that can improve the competitive advantage of state-owned companies.

Unlike state-sponsored intruders, hackers for profit do not seek information for political power; rather they seek information for sale to the highest bidder. These once-isolated hackers have joined forces to create criminal syndicates. Organized crime in cyber space offers a higher profit with a lower probability of being identified and prosecuted. And hacker groups such as Anonymous and Lulz-Sec are pioneering their own forms of digital anarchy.

With these diverse threats, we anticipate that cyber security may well become our highest priority in the years to come. Computer intrusions and network attacks are the greatest cyber threat to our national security. That is why we are strengthening our cyber capabilities, in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

We are focusing the Cyber Division on computer intrusions and network attacks. Such intrusions pose the greatest cyber threat to our national security. We will re-unite non-intrusion programs currently run by the Cyber Division, including Innocent Images and Intellectual Property Rights, with their counterparts in the Criminal Investigation Division. And because even traditional crime is now facilitated through the use of computers, we are enhancing the technological capabilities of all FBI investigative personnel. We are also hiring additional computer scientists to provide expert technical support to critical investigations in the field.

As part of these efforts, we are creating two distinct task forces in the field. First, we will have Cyber Task Forces that will be focused on intrusions and network attacks. The current cyber squads in each of our Field Offices will form the nucleus of these task forces. We must also work together to protect the most vulnerable among us: our children. To that end, we will also create Child Exploitation Task Forces in each field office, which will focus on crimes against children. As we have in the past, we welcome the participation of our federal, state and local partners, as we move forward, with these initiatives.

We are also increasing the size and scope of the National Cyber Investigative Joint Task Force – the FBI-led multi-agency focal point for coordinating and sharing of cyber threat information. The National Cyber Investigative Joint Task Force brings together 18 law enforcement, military, and intelligence agencies to stop current and predict future attacks. With our partners at DOD, DHS, CIA, and the NSA, we are targeting the cyber threats that face our nation. The Task Force operates through Threat Focus Cells – specialized groups of agents, officers, and analysts that are focused on particular threats, such as botnets.

With our partners at the Department of Homeland Security and the National Cyber-Forensics Training Alliance, we are using intelligence to create an operational picture of the cyber threat – to identify patterns and players, to link cases and criminals.

The FBI also has 63 Legal Attaché offices around the world, through which we share information and coordinate investigations with our international counterparts. We also have

Special Agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands, working to identify emerging trends and key players in the cyber arena.

Together with our intelligence community and law enforcement agency partners, we are making progress toward defeating the cyber threat – through our use of human sources, technical surveillance, and computer science.

In April 2011, with our private sector and law enforcement partners, the FBI dismantled the Coreflood botnet. This botnet infected an estimated two million computers with malware that enabled hackers to seize control of the privately owned computers, to steal personal and financial information. With court approval, the FBI seized domain names and re-routed the botnet to FBI-controlled servers. The servers directed the zombie computers to stop the Coreflood software, preventing potential harm to hundreds of thousands of users.

And last fall, we worked with NASA's Inspector General and our partners in Estonia, Denmark, Germany, and the Netherlands to shut down a criminal network operated by an Estonian company by the name of Rove Digital. The investigation, called Operation Ghost Click, targeted a ring of criminals who manipulated Internet "click" advertising. They redirected users from legitimate advertising sites to their own advertisements and generated more than \$14 million in illegal fees. This "click" scheme impacted more than 100 countries and infected four million computers, half a million of which were here in the United States. We seized and disabled rogue servers, froze the defendants' bank accounts, and replaced the rogue servers with legitimate ones, to minimize service disruptions. With our Estonian partners, we arrested and charged six Estonian nationals for their participation in the scheme.

We must continue to share information with our partners in law enforcement, in the Intelligence Community, and in the private sector. We must segregate mission-centric data from routine information. We must incorporate layers of protection and layers of access to critical information. And when there is a compromise, we must limit the data that can be gleaned from it.

We must also work together to determine who is behind any given computer intrusion or network attack. We can use the ability to attribute an attack to a specific attacker to help deter future attacks. We cannot simply minimize vulnerabilities and deal with the consequences. Collectively, we can improve cyber security and lower costs – with systems designed to catch threat actors, rather than simply to withstand them.

Technology

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts.

We are using technology to improve the way we collect, analyze, and share information. In 2011, we debuted new technology for the FBI's Next Generation Identification System, which enables us to process fingerprint transactions much faster and with more accuracy. We are also integrating isolated data sets throughout the Bureau, so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

Sentinel, the FBI's next-generation information and case management system, was deployed to all employees on July 1, 2012. Sentinel moves the FBI from a paper-based case management system to a digital system of record. It enhances the FBI's ability to link cases with similar information through expanded search capabilities. It also streamlines administrative processes through "electronic workflow," making new case information and intelligence available more quickly to agents and analysts. The FBI will continue developing Sentinel's capabilities according to employee feedback and organizational requirements.

Going Dark

As technology advances, both at the FBI and throughout the nation, we must ensure that our ability to obtain communications pursuant to court order is not eroded. The increasingly mobile, complex, and varied nature of communication has created a growing challenge to our ability to conduct court-ordered electronic surveillance of criminals and terrorists. Many communications providers are not required to build or maintain intercept capabilities in their ever-changing networks. As a result, they are often not equipped to respond to information sought pursuant to a lawful court order.

Because of this gap between technology and the law, law enforcement is increasingly unable to access the information it needs to protect public safety and the evidence it need to bring criminals to justice.

We are thankful for Congress' support in funding the National Domestic Communications Assistance Center. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

It is only by working together – within the law enforcement and intelligence communities, and with our private sector partners – that we will find a long-term solution to this growing problem. We must ensure that the laws by which we operate keep pace with new threats and new technology.

Civil Rights, Civil Liberties, and the Rule of Law

Intelligence and technology are key tools we use to stay ahead of those who would do us harm. Yet as we evolve and update our investigative techniques and our use of technology to keep pace with today's complex threat environment, we must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution.

The world around us continues to change, but our values must never change. Every FBI employee takes an oath promising to uphold the rule of law and the United States Constitution. This oath is not to be taken lightly. In my remarks to New Agents, upon their graduation from the FBI Academy, I emphasize that it is not enough to catch the criminal; we must do so while upholding his civil rights. It is not enough to stop the terrorist; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights – these are not our burdens. These are what make all of us safer and stronger. In the end, we in the FBI will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

Conclusion

Chairman Lieberman and Ranking Member Collins, I thank you for this opportunity to discuss the FBI's priorities and the state of the Bureau as it stands today. Mr. Chairman, let me again acknowledge the leadership that you and this committee have provided to the FBI. The transformation the FBI has achieved over the past 11 years would not have been possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.

###

**Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Thomas R. Carper**

**“Homeland Threats and Agency Responses”
September 19, 2012**

| | |
|-------------------|---------------------------------------|
| Question#: | 1 |
| Topic: | cybersecurity |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: There has been substantial discussion about the President possibly issuing an Executive Order on cybersecurity. Please describe the Department’s current authority for securing the cyber networks of the nation’s critical infrastructure and provide any other details regarding what an Executive Order might include with respect to the Department.

Response: In accordance with current authorities as detailed in the Homeland Security Act of 2002, the Federal Information Security Management Act, and as directed in Homeland Security Presidential Directive 7, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, and OMB Memoranda M-10-28, the Department of Homeland Security (DHS) collaborates with members of the public and private sectors to enhance the protection of critical information systems.

The National Infrastructure Protection Plan (NIPP) and the complementary Sector-Specific Plans provide a consistent, unifying structure for integrating current and future critical infrastructure protection efforts. Under the NIPP, and in partnership with the public and private sectors, Sector Specific Agencies (SSAs) are responsible for prioritizing risks to cyber critical infrastructure within their respective sectors as part of an all-hazards approach to risk management.

With respect to critical infrastructure, DHS works with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. Protecting critical infrastructure requires an integrated approach toward physical and cyber security and depends on close partnerships with the private sector to mitigate and respond to cybersecurity threats. DHS supports this effort by sharing actionable cyber threat information with the private sector, helping companies identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident.

| | |
|-------------------|---------------------------------------|
| Question#: | 1 |
| Topic: | cybersecurity |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

The DHS Office of Infrastructure Protection coordinates national public-private partnership efforts across the critical infrastructure sectors identified in the NIPP while the DHS Office of Cybersecurity and Communications (CS&C) provides support to all sectors to assist them in understanding cyber risk and in developing effective and appropriate protective measures. This is done through cyber threats and vulnerabilities analysis; distribution of threat warnings; providing solutions to critical research and development needs; and coordinating the vulnerability, mitigation, and consequence management response to cyber incidents to ensure that computers, networks, and information systems remain safe.

DHS also works with Federal agencies to secure unclassified Federal civilian government networks as well as with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities. As the lead agency for securing civilian government computer systems, CS&C co-chairs the Cross Sector Cyber Security Working Group and the Industrial Control Systems Joint Working Group, which focus on collaboration and cross-sector engagement on cybersecurity vulnerabilities, information sharing, best practices and standards.

In 2011, DHS resolved more than 100,000 cyber incidents and released more than 5,000 actionable alerts and advisories, which it shared with various government, private sector, and critical infrastructure stakeholders, as well as the public. DHS has also deployed over 25 teams of cybersecurity experts to respond to significant private sector cyber incidents and last year conducted 78 assessments for control systems entities, providing them with tailored recommendations for improving their cybersecurity.

| | |
|-------------------|---------------------------------------|
| Question#: | 2 |
| Topic: | sequestration |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: If Congress cannot agree to an adequate deficit reduction plan by January 1, 2013, it's my understanding that sequestration could result in a cut of roughly \$4 billion at the Department of Homeland Security. Reports indicate that that aviation security, immigration enforcement, border security and disaster relief accounts would be losing roughly half a billion each or more. What type of impact could the proposed sequestration budget cuts have on your Department management and agency operations?

Response: Pursuant to the Sequestration Transparency Act of 2012 (STA), the President, through the Office of Management and Budget (OMB) reported to Congress that the sequestration could result in budget cuts totaling \$4.1 billion for the Department of Homeland Security (DHS).

Cuts of the magnitude that would be required by sequestration could impact DHS's frontline operations – rolling back progress in securing the Nation's borders; increasing wait times at U.S. land ports of entry and airports; impacting aviation and maritime safety and security; decreasing our ability to defend critical infrastructure from attack; hampering disaster response time; and delaying the implementation of critical cybersecurity capabilities.

| | |
|-------------------|---------------------------------------|
| Question#: | 3 |
| Topic: | reporting process |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: Federal agencies must have a reliable financial management system and reporting process to ensure they have the resources and tools necessary to carry out their missions. This Committee has closely watched the Department of Homeland Security's efforts to improve its accounting systems and obtain a "clean" or unqualified financial audit opinion. Last spring, I was very pleased when you announced that DHS would become "audit ready" this year – paving the way for the Department to actually pass a financial audit. Can you provide the Committee with an update on your progress for obtaining a "clean" or unqualified financial audit opinion? How can Congress assist DHS to meet your goals?

Response: In FY 2012, the Department of Homeland Security (DHS) earned a qualified audit opinion on all financial statements, for the first time in the Department's history. In FY 2011, the Department achieved a significant milestone when it earned a qualified audit opinion on its FY 2011 Balance Sheet and Statement of Custodial Activity. Building on this, the Department continued to make substantial progress in FY 2012, expanding the scope of the FY 2012 financial statements integrated audit to include the Statement of Changes in Net Position, the Statement of Net Cost, and the Statement of Budgetary Resources. The Department continues to make progress remediating previously identified material weakness conditions and significant deficiencies. DHS is also diligently working to leverage the Management Directorate's A-123 annual process testing to realize audit efficiencies. As the Department continues to work towards the opinion on the financial statements and internal controls, we are focused on achieving progress that is sustainable in the coming years.

The Department appreciates and values the continued support of the Congress as DHS continues to ensure taxpayer dollars are managed efficiently, with integrity, diligence, and accuracy, and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency.

| | |
|-------------------|---------------------------------------|
| Question#: | 4 |
| Topic: | border technology |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: This Committee has continually challenged the Administration to work smarter with federal dollars and to find programs where we can get better results for less money. One area that we have closely followed is the Department of Homeland Security's use of technology to secure the border. As you well know, the Government Accountability Office issued several critical reports on the Department's "SBI-net" program and has raised similar concerns with DHS's new technology efforts on the border. A few months ago, the DHS Inspector General issued a report that raised many questions about the Department's management and use of unmanned aerial systems on the border. Given the fact that GAO and the Inspector General have raised many concerns with the Department's border technology programs, what steps is the Department taking to make smarter, more cost-effective investments in border technology? How are you measuring the success of all this infrastructure and technology we have placed on the border?

Response: In 2009, due to repeated technical problems, cost overruns, and schedule delays, Secretary Napolitano asked CBP for an analysis of the SBInet program. Based on this analysis, Secretary Napolitano froze funding for SBInet beyond the ongoing, initial deployments of Block 1 and in 2010 ordered a Department-wide reassessment of the SBInet program that incorporated an independent, quantitative, science-based Analysis of Alternatives (AoA) to determine if SBInet was the most efficient, effective and economical way to meet our nation's border security needs with respect to technology.

In 2011, the Department published the SBInet AoA report providing substantial detail and documentation of the underlying methods and assumptions, geographical and technology performance calculations, and relevant detailed cost efficiencies and economic factors included in the study and findings. The AoA resulted in a plan for technology deployment that was designed to be more cost efficient, operationally appropriate, and based upon measurable and defensible analysis. In addition, the Department is taking steps to implement measures to assess the effectiveness of technology deployments.

Under the Department's new technology strategy, the government will acquire existing technology through fixed price contracts in order to avoid technical challenges and higher costs often associated with asking contractors to design and develop "custom built" complex sensor and control systems. At the same time, awarding fixed price contracts requires more time than other contract types because the government needs to develop solicitation packages (e.g., Request for Proposals) that contain very detailed operational

| | |
|-------------------|---------------------------------------|
| Question#: | 4 |
| Topic: | border technology |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

and system requirements specifications, detailed site condition documentation, high confidence pricing assumptions and estimates, as well as completed system support plans against which the future contractors would prepare detailed bids. DHS is executing this upfront contracting phase deliberately and as quickly as is prudent. This strategy is expected to yield more favorable (less expensive) and predictable (minimizing cost growth) financial terms for contracted systems and services. The new Arizona strategy is illustrative of improvements and progress in planning and managing technology investments across the entire Department.

Over the past two years, the U.S. Border Patrol has been operating two SBInet Block 1 surveillance systems in high-priority regions of the Arizona border, and has been able to measure the effectiveness of the new technology—in conjunction with additional agents deployed to the region—through several factors, discussed below.

Improved Situational Awareness

The areas covered by SBInet Block 1 technology in both the Tucson and Ajo Stations in Arizona are rugged (and in the case of the Ajo Station, extremely remote as well.) The few available roads are primitive, usually not maintained, and become impassable during the summer monsoons. During the fall, winter, and spring seasons, overuse by vehicles cause these roads to break down to thick silt beds, making passage difficult or impossible even with the use of a four wheel drive vehicle. Much of the area is inaccessible by conventional vehicles and must be patrolled on foot, by horse, ATV, or motorcycle. Rough and rocky terrain, flat desert covered in cactus and brush, and numerous mountainous regions are predominant in the area.

The persistent surveillance and detection capabilities of the Block 1 system provide an unprecedented level of situational awareness. This allows the stations to use manpower and resources more effectively in these areas. Because the system allows operators to detect, classify, and track border intrusions, fewer agents are required to conduct these activities and more resources are available to respond to border intrusions.

Improved Operational Effectiveness

Because of the improved situational awareness in the Block 1 viewsheds, the effectiveness of enforcement operations has improved significantly. The Block 1 system provides the Border Patrol a higher probability of detection of incursions, leading to a higher probability of apprehension, and as such, the level of operational effectiveness (the ratio of arrests to known entries) seen today in the Tucson and Ajo Station border zones within the Block 1 viewshed has never been higher.

| | |
|-------------------|---------------------------------------|
| Question#: | 4 |
| Topic: | border technology |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Thomas R. Carper |
| Committee: | HOMELAND SECURITY (SENATE) |

Decreased Activity

As a result of the increased levels of operational effectiveness gained through improved situational awareness, illegal activity in the areas covered by Block-1 technology has dropped sharply. Since the deployment of fixed tower technology, arrests in the Tucson Station area have dropped nearly 70 percent and nearly 50 percent in the Ajo area.

The decrease in illegal border entries has led to the decrease in citizen and rancher complaints as well as the destruction of public and private lands and property. The Buenos Aries National Wildlife Refuge is located in the heart of the SBInet Block 1 viewshed. Both DHS officials and Department of Interior Refuge Managers have reported to Congress that since the inception of SBInet Block 1, migrant and drug smuggling activity has almost ceased traversing through the Refuge's protected land.

Increased Officer Safety

Also, as a result of the SBInet Block 1 deployment, agent safety in the Tucson and Ajo Stations has improved. Within the diverse physical and asymmetric threat environment encountered at our borders, improvements in agent safety are realized when a variety of tactical advantages are provided to the agents. These tactical advantages can range from improved situational awareness, to the detailed awareness of terrain, changes in threat status/activities/tactics (e.g., location of threat, real time information on threat), and improved agent training and skills. Block 1 provides a clear enhancement with added area covered by the radar and camera which allows agents in the station to monitor and support agents in the field and provide them real time threat information.

**Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Susan M. Collins**

**“Homeland Threats and Agency Responses”
September 19, 2012**

| | |
|-------------------|---------------------------------------|
| Question#: | 5 |
| Topic: | terrorist attacks |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Susan M. Collins |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: The 9/11 Commission’s report observed that, “[I]magination is not a gift usually associated with bureaucracies.” You describe in your testimony that all of AQAP’s major attacks, including the two underwear bomb plots and the printer cartridge attack, employed tactics to deliberately thwart known security measures and exploit failures of imagination.

What “black swan” or imaginative “outside the box” threat worries you most?

Response: The continued threats against our aviation sector by Al-Qa’ida in the Arabian Peninsula (AQAP) underscore the importance of DHS’s commitment to layered and risk-based security.

However, imaginative threats need not be as complex as the printer cartridge plot and can involve efforts of a single individual, in order to cause significant loss of life. As we have seen through a series of violent incidents involving active shooters, including the shooting in Aurora, Colorado, the shooting in Oak Creek, Wisconsin, the Fort Hood attacks, the shootings at the U.S. Holocaust Memorial Museum, and the 2011 attacks in Utoya, Norway, a single individual can carry out a complex attack that has the capacity to do significant harm. This is why we take a layered approach to security, leveraging intelligence, understanding behaviors and indicators, building local community partnerships, and enhancing awareness of radicalization to violence that may come through mediums, like the Internet.

At the same time, threats from cyber security are real and growing, increasing in both magnitude and scope. In 2011, DHS’s U.S. Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber attacks for the Federal Civilian Executive Branch (dot-gov) networks as well as private sector partners

| | |
|-------------------|---------------------------------------|
| Question#: | 5 |
| Topic: | terrorist attacks |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Susan M. Collins |
| Committee: | HOMELAND SECURITY (SENATE) |

responded to more than 106,000 incident reports, and released more than 5,000 actionable cybersecurity alerts to our public and private sector partners.

The word “cybersecurity” encompasses a broad range of malicious activity, from denial of service attacks, to theft of intellectual property, to intrusions against government networks and systems that control our critical infrastructure. Last year, for example, a water plant for a small town in Texas disconnected its control system from the Internet after a hacker posted pictures of the facility's internal controls. More recently, cyber attackers penetrated the networks of companies that operate natural gas pipelines. And computer systems in critical sectors of our economy—including the financial, nuclear, and chemical industries—are increasingly targeted.

We also face a range of traditional crimes that are now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud – all of which pose severe economic and human consequences. Indeed, a Norton study last year calculated the cost of global cybercrime at \$114 billion annually. When combined with the value of time victims lost, this figure grows to \$388 billion globally.

| | |
|-------------------|---------------------------------------|
| Question#: | 6 |
| Topic: | CVE |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Susan M. Collins |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: In your testimony you describe DHS's new CVE training Webportal and the "CVE Training Guidance and Best Practices" guide DHS published for state and local law enforcement.

This is a good sign of progress, and I welcome the effort to address this threat, but it would seem there is still no lead agency charged with implementing the broader CVE plan and making sure these efforts are complementary rather than duplicative. The Committee's 2009 Fort Hood report called for a "comprehensive approach" to addressing this threat, and that means someone should be in charge of coordinating the implementation of the national strategy.

Can you clarify for me which agency is ultimately responsible for coordinating our efforts to combat homegrown terrorism?

Response: The Department has responsibility for implementing a range of CVE initiatives outlined in the Administration's national *CVE Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States*. This role includes leveraging the Department's analytic, research, and information capabilities, engaging state and local authorities and communities to bolster pre-existing local partnerships, and supporting state, local, tribal, and territorial law enforcement and communities through training, community policing practices, and grants. DHS works closely to coordinate and collaborate on these efforts with the National Counterterrorism Center (NCTC), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and other interagency and community partners.

The SIP outlines a whole-of-government approach where coordination is crucial to successful implementation. Although DHS is responsible for many of the actions outlined in the SIP, the Department ensures that interagency coordination and awareness is a shared effort among DOJ, FBI, NCTC, and other interagency partners. DHS meets with its interagency partners regularly to ensure the priorities in the SIP are implemented in a timely manner and co-chairs two Sub-Interagency Policy Committee (IPC) efforts: a sub-IPC on CVE Training co-chaired with NCTC to coordinate interagency CVE training efforts and the Community Engagement Task Force co-chaired with DOJ to share interagency best practices on engagement and coordinate outreach efforts. In addition, DHS's Internal CVE Working Group meets weekly to coordinate all of the CVE activities taking place across the Department.

| | |
|-------------------|---------------------------------------|
| Question#: | 7 |
| Topic: | CBP staffing |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Susan M. Collins |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: As the ranking member of the Senate Homeland Security and Governmental Affairs Committee, I have always supported efforts that increase our security and promote the right mix of resources. I believe that the proper balance of personnel, technology, and infrastructure is necessary to support the federal government's mission to keep our borders open to our neighbors and closed to those who would do us harm. Keeping this in mind, I have heard concerns from Members of Congress and from key stakeholders, in Maine and nationwide, that staffing at our nation's ports of entry is a significant concern.

The Homeland Security Appropriations Act of 2012 mandated a workforce staffing model from CBP to show, among other things, the appropriate staffing levels at our ports of entry. This report was due to Congress on February 15, 2012.

Given that this deadline has passed, please advise when Congress will receive this report.

Response: The report is in the final review process and an updated workforce staffing model is expected to be submitted in conjunction with the Administration's FY 2014 budget request.

**Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Joseph I. Lieberman**

**“Homeland Threats and Agency Responses”
September 19, 2012**

| | |
|-------------------|---------------------------------------|
| Question#: | 8 |
| Topic: | Strategic Implementation Plan |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: Last December, the White House released its Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States. This plan tasked DHS and other federal agencies with specific roles and responsibilities in areas such as community engagement, training, and research and analysis.

What has the Department of Homeland Security done since last December to carry out the objectives and taskings of the Strategic Implementation Plan?

Response: The Department has responsibility for implementing a range of CVE initiatives outlined in the Administration’s national CVE *Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States*. This role includes leveraging the Department’s analytic, research, and information capabilities, engaging state and local authorities and communities to bolster pre-existing local partnerships, and supporting state, local, tribal, and territorial law enforcement and communities through training, community policing practices, and grants. DHS works closely to coordinate and collaborate on these efforts with the National Counterterrorism Center (NCTC), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and other interagency and community partners.

The Department is working with its Federal, state, local, tribal, and territorial partners to fully integrate CVE awareness into the daily activities of law enforcement and local communities nationwide. Specifically, DHS has made substantial progress in CVE in three key areas:

1. Better understanding the phenomenon of violent extremism through extensive analysis and research on the behaviors and indicators of violent extremism;
2. Enhancing operational partnerships with local communities, State and Local law enforcement, and international partners; and

| | |
|-------------------|---------------------------------------|
| Question#: | 8 |
| Topic: | Strategic Implementation Plan |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

3. Supporting community policing efforts through curriculum development, training and grant prioritization.

Better Understanding the Phenomenon of Violent Extremism

DHS has conducted extensive analysis and research to better understand the threat of violent extremism. This includes over 75 case studies and assessments produced by the DHS Office for Intelligence and Analysis (I&A) since 2009 on homegrown violent extremist activities and potential material support activities in the U.S. on behalf of violent extremist groups or causes, including an in-depth study that looks at the common behaviors associated with 62 cases of Al-Qa'ida-inspired violent extremists. DHS has also produced numerous unclassified homeland security reference aids analyzing domestic violent extremist groups.

Enhancing Operational Partnerships and Best Practices with Local Communities, State and Local Law Enforcement, and International Partners

DHS has made significant advancements in operational CVE exchanges with international partners. We have international CVE partnerships with Australia, Belgium, Canada, Denmark, Germany, the Netherlands, Spain, and the UK, as well as partnerships with international law enforcement organizations such as Europol. For the past year, DHS, Europol, and E.U. partners have exchanged information on U.S. and E.U. based fusion center best practices, CVE training standards, and research and case studies, including a joint case study on the 2011 Norway attacks. These exchanges help us support State and Local law enforcement by equipping them with up to date analysis on the behaviors and indicators of violent extremism, so they can prevent potential future violent extremist incidents from occurring in their communities. In addition, DHS has coordinated with the Department of State to train field-based US Government officials, both domestically and internationally, on how to engage and partner with local communities to build community resilience against terrorist recruitment and radicalization to violence.

The Department has also significantly expanded outreach to communities that may be targeted for recruitment by violent extremists and promote a greater awareness of Federal resources, programs, and security measures available to communities. For example, the DHS Office of Civil Rights and Civil Liberties (CRCL) has held over 72 roundtable events nationwide since 2011, which have helped to address grievances, increase awareness of CVE resources, and build partnerships between state and local law enforcement, local government, and community stakeholders.

| | |
|-------------------|---------------------------------------|
| Question#: | 8 |
| Topic: | Strategic Implementation Plan |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

Supporting Community Policing Efforts through Curriculum Development, Training and Grant Prioritization

Over the past year, DHS has worked closely with the State and Provincial Police Academy Directors, the International Association of Chiefs of Police, the Major City Chiefs Association, the Major City Sheriff's Association, NCTC, DOJ, and the FBI to develop CVE training for Federal, State, Local, and Correctional Facility law enforcement. DHS has hosted seven workshops to receive feedback from front line officers on the training materials, including workshops in Columbus, OH, San Diego, CA, Washington, DC, and Minneapolis, MN and the recent "Train-the-Trainer" CVE Workshop in San Diego, CA during the last week of September 2012. Two workshops were also conducted for correctional facility officers in Sykesville, MD and in Orange County, CA.

On September 28, 2012, DHS launched a new CVE Training Webportal through the Homeland Security Information Network (HSIN) for CVE law enforcement training practitioners nationwide. This Training Webportal serves as an efficient and easy resource to access CVE training materials, which can be incorporated into existing training programs and contains over 160 CVE training resources.

DHS expanded FY2012 grant guidance to include funding for training and local CVE efforts, including participating in CVE training workshops, developing CVE training curriculum, participating in the new CVE Webportal, and incorporating CVE training resources into existing training programs.

Question: The Strategic Implementation Plan indicated that the government would be developing a new strategy to address "online violent extremist radicalization."

i. What is the status of this strategy?

Response: Interagency partners are currently developing a strategy around countering violent extremism online.

Question: ii. What key issues is the strategy likely to address?

Response: The strategy focuses on leveraging internet safety principles to protect communities from violent extremist propaganda.

Question: iii. What is the timetable for developing the strategy? When do you expect to issue it?

Response: As interagency work continues, we will keep the Committee apprised of any developments and timing.

| | |
|-------------------|---------------------------------------|
| Question#: | 9 |
| Topic: | Active Shooter Threats |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: In your written testimony before the Committee you noted the Department's ongoing work with the FBI, NCTC and State and local partners to improve capabilities to prepare for and respond to active shooter attacks like the ones in Mumbai, the Sikh temple in Wisconsin, and the attack on the Family Research Council headquarters here in Washington in August. One of the Committee's long standing concerns has been the safety and security of the more than one million federal personnel, and countless visitors, who occupy the more than 9000 federal buildings nationwide that the Federal Protective Service bears the responsibility for protecting.

How have you assessed the threat of an active shooter attack around or within federal buildings, and how are DHS and the FPS ensuring both federal personnel and the armed contract guards it uses to protect federal buildings are properly prepared to prevent or respond to this type of attack?

Has the Department assessed and compared the threats of an active shooter versus explosive threats against federal buildings and personnel? If so, what is the Department's assessment of the threats?

Response: As you mention, the Department of Homeland Security's Federal Protective Service (FPS) is the lead agency for protecting the government facilities sector, which includes more than 9,000 Federal buildings and 1.4 million Federal employees and visitors who occupy them throughout the country every day. If a specific threat to a Federal building is identified, DHS makes appropriate notifications to FPS and works with its partners in the Intelligence Community to share relevant information with law enforcement officials.

On an ongoing basis, the Department's Office of Intelligence and Analysis (I&A) produces products for law enforcement and first responders on the potential threat and indicators of active shooters, lone offenders, small-unit assault tactics, and explosive devices in the Homeland. These products are designed to provide a baseline understanding of potential threats that can augment risk assessments produced by the National Protection and Program Directorate (NPPD).

FPS also produces regular information bulletins and threat assessments, which are distributed to stakeholders such as Protective Security Officers and law enforcement to increase their awareness and knowledge of threats to Federal facilities. For example, the quarterly Federal Facility Threat Picture (FFTP) is an unclassified assessment of the

| | |
|-------------------|---------------------------------------|
| Question#: | 9 |
| Topic: | Active Shooter Threats |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

current known threats to the facilities under the jurisdiction of FPS. The FFTP focuses on the threats posed by international terrorists, domestic violent extremists, lone offenders, and criminal organizations who may seek to attack or exploit elements of the Government Facilities Sector.

FPS conducts Active Shooter Response training for all of its personnel and also offers "Active Shooter Tenant Awareness Training" to all federal agencies/employees that occupy space within GSA owned or leased facilities. This training program was developed in 2009 and, since its inception, more than 1,000 training sessions have been conducted at facilities nationwide. FPS conducted more than 500 training sessions in FY 2012 and anticipates approximately 600 training sessions in FY 2013.

FPS also conducts regular briefings with stakeholders regarding the threats to Federal facilities and provides information about the threat streams we track. Recently, FPS provided an Active Shooter briefing to members of the Government Facilities Sector, Government Coordinating Council in August 2012.

| | |
|-------------------|---------------------------------------|
| Question#: | 10 |
| Topic: | Cybersecurity Practices |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: One of the central concerns raised by opponents of our cybersecurity legislation is that the government, and specifically DHS, would not consult and collaborate with the private sector to determine what cybersecurity practices are critical and feasible for the private sector. I believe this concern is unfounded. Our legislation always envisioned outcome-based performance practices developed by the Government in close collaboration with the private sector that would allow companies to select any means they believed appropriate to meet the goals set forth by the practices. A cybersecurity practice that would substantially impact a company's bottom-line would be impracticable.

Can you describe how you envision DHS working with the private sector to ensure close collaboration?

Response: Private industry owns and operates the vast majority of the Nation's critical infrastructure and cyber networks. Therefore, protecting critical infrastructure and cyberspace – including the systems and networks that support the financial services, energy and defense industries – requires close partnerships with the private sector.

The Department of Homeland Security (DHS) has always taken a collaborative approach when working with the private sector to inform critical infrastructure prioritization and risk management efforts. For example, the Department's Industry Engagement and Resilience (IER) program currently provides cybersecurity expertise to the 18 critical infrastructure and key resources sectors defined under the National Infrastructure Protection Plan. Together with public and private partners, IER develops and implements cyber risk management approaches and provides opportunities to increase cybersecurity awareness.

The Department's current efforts working with the private sector to reduce cyber risk to critical infrastructure have led to greater collaboration among private sector stakeholders, helping sectors prioritize risks of concern to focus their cyber efforts and establishing business cases for investing limited resources in cyber risk management strategies. This partnership is based on a framework that is technology-neutral and focused on risk based outcomes.

One of the tools developed by IER is a flexible, scalable, and repeatable cyber risk management approach to help critical infrastructure sectors, state and local governments, and other public and private sector organizations manage their cyber critical

| | |
|-------------------|---------------------------------------|
| Question#: | 10 |
| Topic: | Cybersecurity Practices |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

infrastructure risk. It is known as the Cybersecurity Assessment and Risk Management Approach (CARMA) and was originally developed while IER was conducting its cybersecurity risk assessment for the Information Technology Sector. Since then it has successfully been used by the Emergency Services Sector and Transportation Systems Sector for gaining a strategic view of cyber risks.

In addition, the U.S. Secret Service works closely with the private sector through Electronic Crimes Task Forces (ECTFs), which bring together law enforcement, the private sector, and academia to prevent, detect, mitigate and investigate cyber attacks on our nation's financial and critical infrastructure. The ECTFs focus on identifying and locating international cybercriminals involved in network intrusions, bank frauds, data breaches, and other cyber-related crimes. There are currently 31 ECTFs, including task forces in London, England and Rome, Italy. Membership in our ECTFs include: approximately 300 academic partners; over 2,700 international, federal, state, and local law enforcement partners; and over 3,100 private sector partners.

| | |
|-------------------|---------------------------------------|
| Question#: | 11 |
| Topic: | bioterrorist attack |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

Question: As you are aware, the World at Risk report put out by the WMD Commission three years ago, and led by former Senators Graham and Talent, expressed the concern that the risk of a bioterror attack was more likely than any other weapon of mass destruction. Further, the report predicted that such an event could occur somewhere in the world within the five years after the release of the commission's report and that the government was not yet adequately prepared to respond to such an attack.

How do you assess the current bioterror threat to the homeland?

Response: We agree with the Director of National Intelligence's (DNI) statement for the record before the Senate Committee on Armed Services in February 2012 that biological terrorism is an enduring threat to the United States and will remain so for the foreseeable future. As the DNI Director highlighted, we assess that small scale biological attacks, which could occur with little or no warning, represent a significant threat because terrorist organizations and other violent extremists remain interested in conducting this type of attack. We would be happy to provide a more detailed assessment in a classified briefing.

Question: How is the federal government working across agencies and departments to ensure that we are prepared in the event of a bioterrorist attack?

Response: As was stated before your Committee at the October 2011 hearing "Examining progress towards protecting against biological threats 10 years after the anthrax attacks", the White House provides overall strategy and guidance on preparedness for biological threats through the issuance of a number of national strategies and Presidential Directives. In the aggregate, these strategies and directives set the framework for DHS and Federal partners to identify and take action on required preparedness activities to enhance biopreparedness. The diversity of the threat and broad array of prevention and response measures needed to counter biological threats necessitates a government wide effort to build and sustain preparedness. Within their statutory missions, Federal departments and agencies coordinate bioterrorism preparedness activities through a number of interagency mechanisms.

Coordination occurs through the National Security Staff-led Interagency Policy Committee (IPC) process as well as other interagency policy forums dependent on mission needs. The Domestic Resilience Group and Countering Biological Threats IPCs tap the expertise of all departments and agencies to address biodefense priorities.

| | |
|-------------------|---------------------------------------|
| Question#: | 11 |
| Topic: | bioterrorist attack |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

DHS has key responsibilities and has taken tangible actions to improve preparedness against a biological attack. These actions span the biodefense spectrum, from threat awareness and analysis, prevention and protection, surveillance and detection, to response and recovery.

Threat Awareness and Analysis

In the area of threat analysis, DHS has established a standing interagency working group to define informational product needs and collect intelligence community and subject matter expert analysis to deliver robust biological threat assessments to the interagency for use in policy and resource allocation decisions. In particular, these threat assessments are used by the Department of Health and Human Services (HHS)-led Public Health Emergency Medical Countermeasure Enterprise (PHEMCE), which brings together four key interagency partners—Department of Homeland Security (DHS), Department of Defense, Department of Veterans Affairs (VA), and Department of Agriculture (USDA). Working together, these agencies coordinate and exchange information to optimize preparedness and response for public health emergencies in connection with the creation, stockpiling and use of medical countermeasures.

In addition, DHS also leads an interagency Biodefense Net Assessment that examines emerging trends in biodefense issues. Through its leadership of the Integrated Consortium of Laboratory Networks, DHS is strengthening the surge capacity of 500 state, local and private sector laboratories belonging to eight networks managed by five federal agencies whose coordinated efforts could be called upon in a mass bioterrorist attack.

DHS has advocated for and been successful in obtaining appropriate security clearances for public health professionals supporting State and local fusion center operations. This effort is critical to integrating the public health and emergency management disciplines in preventing, detecting and responding to a potential biological attack. Threat analysis is a key foundation of DHS activities to assess risk of biological events, informing Federal partners for planning and acquisition of appropriate countermeasures.

Prevention and Protection

In the area of prevention and protection, DHS has worked with Federal partners and set the standard for making available life-saving medical countermeasures to ensure that Departmental mission essential functions can continue in the event of a biological attack. This effort is in direct support of the Presidential Executive Order seeking a rapid federal

| | |
|-------------------|---------------------------------------|
| Question#: | 11 |
| Topic: | bioterrorist attack |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

response to support state and local jurisdictions in the event of a biological attack. Similarly, FEMA is leading a robust regional planning initiative to ensure proactive Federal support to State and local partners in the area of medical countermeasure distribution and dispensing. As it does with other sectors, DHS assesses the vulnerabilities of key biological response facilities, such as high containment laboratories and vaccine manufacturers, for site security vulnerabilities and works with operators to address those issues in order to enhance community and national resilience.

Surveillance and Detection

The National Strategy for Biosurveillance (released in July 2012) promotes interagency collaboration around the goal of informing decisionmaking for incidents that include intentional or naturally-occurring biological threats. The Department's National Biosurveillance Integration Center (NBIC), established in 2007 as directed by Congress, developed its first strategic plan. The NBIC Strategic Plan articulates a clear approach with a series of measurable steps and initiatives to enhance the biosurveillance capability of the United States targeting an array of naturally-occurring, accidental, and intentional biological threats. This capability enables early warning and shared situational awareness of acute biological events and support better decisions in the event of a biological event.

BioWatch is the only federally-managed, locally-operated nationwide bio-surveillance system designed to detect the intentional release of select aerosolized biological agents. Deployed in more than 30 metropolitan areas throughout the country, the system is a collaborative effort of health personnel at all levels of government. By its design, the DHS-managed BioWatch environmental surveillance program fosters federal interagency coordination.

DHS is the executive agent for the Federal Biological Assessment Threat Response protocol (BATR). The BATR Protocol provides a rapid national-level interagency consultation process designed to support consistent, coordinated action and desired outcomes to prevent, protect, mitigate, respond and recover from high-consequence bioterrorism and biosecurity threats and incidents.

Response and Recovery

To support response and recovery in the event of a biological attack, the Department has used the direction contained in Presidential Policy Directive-8, National Preparedness, to ensure that all WMD scenarios, including a biological attack, are part of an all-hazards approach to national preparedness. One product required by PPD-8, The National Preparedness Goal (NPG), delineates the core capabilities needed for the nation to

| | |
|-------------------|---------------------------------------|
| Question#: | 11 |
| Topic: | bioterrorist attack |
| Hearing: | Homeland Threats and Agency Responses |
| Primary: | The Honorable Joseph I. Lieberman |
| Committee: | HOMELAND SECURITY (SENATE) |

prevent, protect, mitigate, respond to, and recover from incidents that pose the greatest risk to the security of the Nation. These core capabilities extend across all levels of government and the private sector. FEMA is leading an inclusive effort among stakeholders at all levels in the development of the NPG and subsequent planning efforts.

The Department has conducted and participated in a number of biological event-specific table-top exercises, workshops and facilitated discussions. These events were conducted on many levels, from internal DHS activities, events engaging federal partners, to regional, State and local jurisdictional response activities. In all cases, these exercises and workshops were developed and conducted to enhance preparedness in the event of biological attacks.

**Post-Hearing Questions for the Record
Submitted to the Honorable Matthew G. Olsen
From Senator Joseph I. Lieberman**

**“Homeland Threats and Agency Responses”
September 19, 2012**

1. US Government Efforts to Counter Violent Islamist Extremism

Last December, the White House released its Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States. This plan tasked the National Counterterrorism Center (NCTC) and other federal agencies with specific roles and responsibilities in areas such as community engagement, training, and research and analysis.

- a. What has NCTC done since last December to carry out the objectives and taskings of the Strategic Implementation Plan? Please provide specific examples.
- b. The Strategic Implementation Plan indicated that the government would be developing a new strategy to address “online violent extremist radicalization.”
 - i. What is the status of this strategy?
 - ii. What key issues is the strategy likely to address?
 - iii. What is the timetable for developing the strategy? When do you expect to issue it?

2. Terrorist Intent to Carry Out Cyber Attacks

- a. From your position as Director of NCTC, what is your assessment of the possibility of terrorist groups using cyber tools to carry out attacks on critical infrastructure?
- b. Is there reason to believe that nation-states that have advanced cyber capabilities could share that capability with terrorist groups that lack the capacity but not the intent to attack to America?

Note:

The classified responses to Senator Lieberman’s questions are on file at the Office of Senate Security.

**Post-Hearing Questions for the Record
Submitted to the Honorable Matthew G. Olsen
From Senator Susan M. Collins**

**“Homeland Threats and Agency Responses”
September 19, 2012**

1. The authorities provided in the 2008 FISA Amendments law expire at the end of this year. Director Olsen, in your opening statement, you testified that reauthorizing this legislation is “critical and must be done as soon as possible to avoid any gap in our collection capabilities.” The House has voted to renew this legislation, but the Senate has yet to act. Eleven years after 9/11, some Americans still have some doubts about the necessity of this authority.

Would you describe for the American people what risk there is in allowing the FISA Amendments legislation to expire?

2. The 9/11 Commission’s report observed that, “[I]magination is not a gift usually associated with bureaucracies.” You describe in your testimony that all of AQAP’s major attacks, including the two underwear bomb plots and the printer cartridge attack, employed tactics to deliberately thwart known security measures and exploit failures of imagination.

What “black swan” or imaginative “outside the box” threat worries you most?

3. In your testimony you describe some of the work NCTC has been doing to implement the Administration’s national strategy to combat homegrown terrorist and violent Islamic extremism. NCTC has developed a training briefing for local communities, held summits, and actively supported CVE efforts at our embassies.

These are good signs of progress, and I welcome the effort to address this threat, but it would seem there is still no lead agency charged with implementing the broader CVE plan and making sure these efforts are complementary rather than duplicative. The Committee’s 2009 Fort Hood report called for a “comprehensive approach” to addressing this threat, and that means someone should be in charge of coordinating the implementation of the national strategy.

Can you clarify for me which agency is ultimately responsible for coordinating our efforts to combat homegrown terrorism?

4. The past year has seen an apparent uptick in Iranian sponsored and initiated terrorist attacks. Last October we learned of an Iranian plot to assassinate the Saudi ambassador to the U.S. and attack the Israeli embassy in Washington. Iran’s proxy, Hezbollah, also has a history of fund raising and money laundering in the U.S. As conflict over Iran’s nuclear program threatens to escalate, these activities should raise grave concerns.

Are you confident that NCTC has a good understanding of Hezbollah’s operational capabilities inside the U.S.?

Note:

The classified responses to Senator Collins’ questions are on file at the Office of Senate Security.

TOP SECRET//HCS/SI-G//ORCON/NOFORN

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

December 10, 2012

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

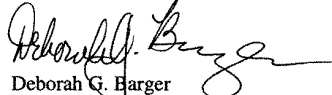
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Lieberman and Ranking Member Collins:

(U) Enclosed please find National Counterterrorism Center (NCTC) Director Matthew Olsen's responses to the post-hearing Questions for the Record from the 19 September 2012 Senate Homeland Affairs and Governmental Affairs Committee Hearing titled "Homeland Threats and Agency Responses."

(U) Please do not hesitate to contact me if you require further assistance regarding this or any other matter.

Sincerely,


Deborah G. Harger
Director of Legislative Affairs

Enclosure:

(U) Responses to Questions for the Record from 19 September 2012 Hearing

UNCLASSIFIED when separated from enclosures

DRV From: HCS 4-04
DECL On: 25X1-human

TOP SECRET//HCS/SI-G//ORCON/NOFORN

