A NEW PERSPECTIVE ON THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

FEBRUARY 13, 2013

Serial No. 113–1

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

81–461 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
KEITH J. ROTHFUS, Pennsylvania
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

CONTENTS

A NEW PERSPECTIVE ON THREATS TO THE HOMELAND

Wednesday, February 13, 2013

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to call, at 10:09 a.m., in Room 311, Cannon House Office Building, Hon. Michael T. McCaul [Chairman of the committee] presiding.

Present: Representatives McCaul, King, Miller, Meehan, Duncan, Marino, Palazzo, Barletta, Stewart, Rothfus, Hudson, Daines, Brooks, Perry, Thompson, Jackson Lee, Keating, Payne, O'Rourke, Gabbard, Vela, Horsford, and Swalwell.

Chairman MCCAUL. The Committee on Homeland Security will come to order. The committee is meeting today to hear testimony on the evolving homeland threat landscape. I now recognize myself for an opening statement.

Let me first say what an honor it is to be elected by my peers to serve as the Chairman of this powerful committee, and at the same time, would like to recognize the man who sat in this chair for 7 years, Peter King, who—just let me thank you for your great service and dedication to the cause of protecting the American people. I sure do appreciate that.

Mr. KING. Thank you, Chairman.

Chairman MCCAUL. Also, as I look at the pictures on the wall of New York, your hometown, Mr. Chairman, I know we plan to visit there the following week. We are kind of reminded of the unfortunate catalyst for the creation of this committee. They will remain on the wall to remind us constantly that our promise is "never again."

After 9/11, President Bush declared, "We are fighting a new kind of war against determined enemies. And public servants long into the future will bear the responsibility to defend Americans against terror."

Over a decade later, we now know these words remain true. The threats we face have adapted and the Department of Homeland Security's mission and capability have yet to be solidified. The Members of this committee are some of the public servants the President spoke about. It is our duty to continue to improve DHS and defend our freedom, security, and way of life.

Essential to defending our homeland is securing our borders. Coming from Texas, I am particularly concerned with conditions on our Southwest Border. We are and will remain a Nation of immi-

grants and no one denies our immigration system is broken and needs to be reformed.

However, as immigration reform takes center stage, we cannot repeat the mistakes of the past. The 1986 immigration reform did not stop the flow of illegal immigrants and we cannot support reforms today unless they hinge on gaining effective control of our borders.

Until the administration creates a comprehensive National strategy to secure our borders that includes a reasonable definition of operational control that we can measure, then we cannot quantify success or failure. My overriding goal is to prevent repeating this debate 10 years from now.

All Americans, whether an immigrant or citizen born here, require a secure border that prevents drugs, weapons, and violence from damaging our communities.

Drug cartels fight for primacy on our Southern Border, sending narcotics into our homes. Smugglers weaken our economic competitiveness at our ports of entry while terrorists still seek entry into the United States undetected.

Increasingly, DHS has the opportunity to use existing technologies returning from the theaters of war that make securing our border cheaper and easier than ever before. Consequently, as we embark on an immigration reform debate, we must be mindful that the first step is to control our border, and I will be introducing legislation soon to accomplish that goal.

I have developed a framework for legislation to compel the Department and its components to create and implement a strategy to control our borders that includes measurable progress. I am working with outside groups and my colleagues on both sides of the aisle and in both chambers to be sure the strategy is workable and has the support that it needs.

If fully implemented, the ability exists to gain effective control of our borders within 3 years. The strategy must meet three key criteria. It must ascertain situational awareness of our borders, it must create metrics to measure progress based on outcomes, and it must integrate the Department of Homeland Security components that presently overlap or contradict.

This task is long overdue and the time to achieve this goal is now. As the committee moves forward, we build upon the success of the vice chair of this committee, Mrs. Miller, who is Chair of the Subcommittee on Border and Maritime Security.

She has been a real leader on these issues not only for this committee but for the entire House, and I am glad to have her as a partner, and this committee appreciates the path that she has paved in pushing for a stronger, smarter, border security strategy.

Other threats to our Nation do not cross our physical borders. They instead invade our digital networks. DHS is tasked with securing our civilian Federal networks and equally important, protecting our critical infrastructures.

DHS is responsible for coordinating the National protection, prevention, mitigation of, and recovery from cyber incidents. DHS is also charged with disseminating domestic cyber threat and vulnerability analysis and investigating cyber crimes within their jurisdiction.

As these threats increase, and they are, it is essential that the Federal Government has the capability and capacity to defend against a cyber attack that could have devastating consequences on our economy and our way of life.

I do not need to stress the importance of this mission because China is hacking into major American publications and to military secrets, and Iran allegedly targeted our financial institutions in Aramco and the Saudi peninsula just recently.

These are just some of the latest in a series of increasingly regular attacks against the homeland and reports this week also claim that China is currently targeting U.S. trade secrets valued at tens of billions of dollars.

My visit to the NSA and with General Alexander, the director of NSA, was sobering to say the least. DHS has been building its capability to protect us from cyber attacks and it will be the priority of this committee to help them improve their efforts through legislation. A whole-of-Government cyber strategy that is responsive to the threat landscape is necessary and will require insight into the most dangerous cyber actors.

This committee has a major role in crafting such a strategy. In the next hearing before this committee we will focus on the President's Executive Order on cybersecurity.

As we work to meet these challenges, we will never forget the present threat of terrorism. While our military efforts have scattered and disseminated the core of al-Qaeda's operations and leadership, terrorist franchises such as those that attacked the BP facility in Algeria last month have found new safe havens allowing them to reconstitute.

One of my constituents, Fred Buttaccio from Katy, Texas was killed during this terrorist takeover of the facility. I attended his funeral and presented an American flag to his widow.

Scattered across the map are increasing numbers of organizations sympathetic to al-Qaeda's message reaching out to al-Qaeda operatives in joining their global jihad. Iran continues to expand its sphere of influence, strategically advancing its position in the Western Hemisphere.

To face these challenges, DHS must improve. Unorganized financial management drains resources from necessary work while structural waste and duplication shut down solutions.

To take a recent example, the Department decided to remove 174 full-body scanners from airports across the country because they cannot adapt to new imaging requirements, and one report alleges these scanners cost $150,000 for each unit. This faulty procurement process has set our travel security back while also angering ordinary passengers.

This committee will work towards building a better Department so that it can rise to meet a new decade and evolving threats head-on. Looking on to the 113th Congress, we will not turn our back on that goal, and I appreciate these witnesses coming here today to help us better understand the threats against us and what needs to be done to meet them.

In closing, I would like to reiterate what we said at our last organizational meeting that Mr. Thompson, the Ranking Member, we

look forward to working with you in a bipartisan way to accomplish our shared goal of protecting the homeland.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

FEBRUARY 13, 2013

In the years I have sat in this hearing room, upon the walls have hung a series of pictures taken on that day, almost 12 years ago, which served as the unfortunate catalyst for the creation of this committee. Today those images remain to remind us of the purpose we serve here—to remind us of our promise, "never again."

After 9/11 President Bush declared:

"We're fighting a new kind of war against determined enemies. And public servants long into the future will bear the responsibility to defend Americans against terror."

Over a decade later, we now know those words remain true. The threats we face have adapted, and the Department of Homeland Security's mission and capability have yet to be solidified. The Members of this committee are some of the "public servants" the President spoke about. It is our duty to continue to improve DHS, and defend our "freedom, security, and way of life."

Essential to defending our homeland is securing our borders. Coming from Texas, I am particularly concerned with conditions on our Southwest Border. We are, and will remain, a nation of immigrants, and no one denies that our immigration system is broken. However, as immigration reform takes center stage, we cannot repeat the mistakes of the past. The 1986 immigration reform did not stop the flow of illegal immigrants and we cannot support reforms today unless they hinge on gaining effective control of our borders. Until the administration creates a comprehensive National strategy to secure our borders—that includes a reasonable definition of operational control we can measure—we cannot quantify success or failure. My overriding goal is to prevent repeating this debate 10 years from now.

All Americans—whether an immigrant or citizen born here—require a secure border that prevents drugs, weapons, and violence from damaging our communities. Drug cartels fight for primacy on our Southern Border, sending narcotics into our homes; smugglers weaken our economic competitiveness at our ports of entry; while terrorists still seek entry into the United States undetected. Increasingly, DHS has the opportunity to use existing technologies returning from theaters of war that make securing our border cheaper and easier than ever before. Consequently, as we embark on immigration reform we must be mindful that the first step is to control our border—and I will be introducing legislation to accomplish that goal.

I have developed a framework for legislation to compel the Department, and its components, to create and implement a strategy to control our borders that includes measurable progress, and I am working with outside groups and my colleagues on both sides of the aisle and in both chambers to be sure the strategy is workable and has the support it needs.

If fully implemented, the ability exists to gain effective control of our borders within 3 years. The strategy must meet three key criteria. It must ascertain situational awareness of our borders. It must create metrics to measure progress based on outcomes. It must integrate Department of Homeland Security components that presently overlap or contradict.

Other threats to our Nation do not cross our physical borders—they instead invade our digital networks. DHS is tasked with securing our civilian Federal networks and—equally important—protecting our critical infrastructure. DHS is responsible for coordinating the National protection, prevention, mitigation of, and recovery from cyber incidents. DHS is also charged with disseminating domestic cyber threat and vulnerability analysis and investigating cyber crimes within their jurisdiction. As these threats increase, it is essential the Federal Government has the capability and capacity to defend against a cyber attack that could have devastating consequences on our economy and way of life.

I do not need to stress the importance of this mission because China is hacking major American publications and military secrets, and Iran is allegedly targeting our major financial institutions. These are just the latest in a series of increasingly regular attacks against the homeland. Reports this week also claim that China is currently targeting U.S. trade secrets valued at tens of billions of dollars.

DHS has been building its capability to protect us from cyber attacks, and it will be a priority of this committee to help them improve their efforts through legislation. A whole-of-Government cyber-strategy that is responsive to the threat land-

scape is necessary, and will require insight into the most dangerous cyber actors. This committee has a major role in crafting such a strategy, and the next hearing before this committee will focus on the President's Executive Order 13636* on cybersecurity.

As we work to meet these challenges, we will not forget the present threat of terrorism. While our military efforts have scattered and decimated the core of al-Qaeda's operations and leadership, terrorist franchises such as those that attacked the BP facility in Algeria last month have found new safe havens allowing them to reconstitute. One of my constituents, Frederick Buttaccio, from Katy, Texas was killed during the terrorist takeover of this facility.

Scattered across the map are an increasing number of organizations sympathetic to al-Qaeda's message, reaching out to al-Qaeda operatives, and joining their global jihad. Iran continues to expand its sphere of influence, strategically advancing its position in the Western hemisphere.

To face these challenges, DHS must improve. Unorganized financial management drains resources from necessary work, while structural waste and duplication slow down solutions. To take a recent example, the Department has decided to remove 174 full-body scanners from airports across the country because they cannot adapt to new imaging requirements. One report alleges these scanners cost $150,000 for each unit. This faulty procurement has set our travel security back, while also angering passengers.

This committee will work toward building a better Department, so that it can rise to meet a new decade, and evolving threats, head-on. Looking ahead to the 113th Congress, we will not turn our back on that goal, and I appreciate these witnesses coming here today to help us better understand the threats against us—and what needs to be done to meet them.

Before closing, I would again like to reiterate what I said at our organizational meeting last month—Mr. Thompson, we look forward to working with you to accomplish our shared goal of protecting the homeland.

ATTACHMENT.—FRAMEWORK FOR OPERATIONAL CONTROL OF AMERICA'S BORDERS

We cannot repeat the mistakes of the past by failing to ensure border security is a primary component to reforming our immigration system. The committee is currently consulting with outside policy and operations experts to introduce legislation to compel DHS to establish a comprehensive National Strategy to secure our borders. We can no longer supply resources on an ad-hoc basis and expect to make lasting progress. The committee will hold a series of hearings to examine the current border landscape, and what must be done to achieve full awareness of who and what is crossing our borders. I look forward to working with my colleagues on both sides of the aisle in both chambers, and with the Department, to ensure the development and implementation of a National Strategy is achieved.

There are myriad National and departmental policies addressing counternarcotics, terrorism, and transnational criminal organizations, all of which touch on border security, yet still there is no clearly articulated, centralized National strategy with a sole focus on securing the border. DHS must create a holistic strategy that looks at the overall picture of the border and applies resources based on threat levels and anticipated changes in migration.

Four Guiding Principles for Legislation Establishing a National Strategy.—Gain situational awareness using advanced technologies, to formulate useable metrics, while eliminating agency overlap (SAFE).

1. Situational Awareness.—In order to allocate resources appropriately, we must have situational awareness—an overall idea of what must go where. We cannot continue to throw scarce resources at isolated problems, only to see them shift. DHS must present to Congress a long-term analysis of where the United States is vulnerable based off of a holistic picture of our borders.

2. Advanced Technologies.—The administration must work to incorporate existing technology such as Department of Defense Sensor Surveillance equipment used in Iraq and Afghanistan in order to gain comprehensive visibility of the border landscape. Using proven, effective technologies to enhance our border security efforts will save taxpayer dollars and make our citizens safer.

3. Formulate Metrics.—In 2010, Secretary Napolitano stopped using the metric of "operational control." At that time, DHS claimed to have only 44% of the border under operational control. We can no longer base our security solely on only apprehensions, without knowing the total number of individuals who cross un-

---

*Executive Order 13636, Improving Critical Infrastructure Cybersecurity.

detected. Nor can we base success on the number of resources allocated to different sectors or components. Gaining situational awareness will allow DHS to create a new metric to define progress—based off of the number of apprehensions relative to the total number of illegal crossings. Only when we have the full picture can we gauge our own progress, and we must base progress on outcomes, instead of resources.

4. Eliminate Overlap.—The Department of Homeland Security must present to Congress its plan to better integrate its agencies to combat all of the threats we face on our borders. DHS's subordinate components should not unnecessarily duplicate each other's efforts—they should instead work in complementary fashion to ensure our National security.

Mr. MCCAUL. The Chairman now recognizes the Ranking Member, Mr. Thompson from Mississippi.

Mr. THOMPSON. Thank you very much, Chairman McCaul, for holding this hearing today. Likewise, I look forward to working with you on many of the items you outlined in your opening statement.

However, today we will hear from witnesses who will provide an overview of some of the areas you have identified as priorities. I look forward to their testimony and thank each of them before appearing today.

Before we hear their testimony, I think it is important to point out that as Members of Congress, each of us has a responsibility to ensure that the Department is able to adequately perform its mission of protecting the Nation from and responding to terrorist attacks, man-made catastrophes, and natural disasters.

As Members of this committee, each of us has a responsibility to assure the success of the homeland security mission. That mission cannot be achieved without appropriate funding, vigorous oversight, and targeted legislation.

We cannot play our part in ensuring the success of the homeland security mission if we are not willing to use the full weight of the committee structure, both subcommittee and the full committee, to pursue a well-crafted agenda.

That agenda should result in bringing our bills to the floor and assuring that our oversight yields effective outcomes. Our energies will be wasted and our opportunities will be squandered if we do not work towards the goal of making the people of this Nation safer.

Therefore, Mr. Chairman, I commend you for issuing a statement of priorities in the hope that the work of this committee and each of its subcommittees will remain focused on those objectives and our mission during this session of Congress.

One of your priorities is border security. Since 2004, we have doubled the number of Border Patrol agents and more than doubled the number of unauthorized aliens removed from this country. In our examination of border security, we cannot be limited by calling for more of the same.

DHS currently lacks a border security strategy that coordinates CBP, ICE, and the Coast Guard. We must continue to press DHS for such a strategy. Without it, we cannot be certain that our border control resources are strategic and well-coordinated.

Another priority is cybersecurity. As you know, today the administration released an Executive Order on cybersecurity. It is my understanding that the strategy calls for strong privacy and civil liberties protection and recognizes the necessity and necessary leader-

ship of the Department of Homeland Security in establishing a volunteer program to promote the adoption of a cybersecurity framework.

This strategy sounds a great deal like the PRECISE Act, a bill this committee marked up last Congress but was prevented from moving to the floor by the Majority leadership. As we review cybersecurity, I hope we can try once again to take the PRECISE Act to the floor of the House.

Third, I appreciate your identification of the management and administrative functions of the Department as one of your priorities. As you may know, since the inception of the Department, I have worked to bring accountability and transparency to the personnel in contracting practices.

The Department cannot succeed unless every component is brought into an organizational structure that gives headquarters command and control over the most basic personnel rules and contracting procedures. Without centralized authority and accountability, we should not be surprised by stories of waste, fraud, and abuse.

Fourth, I look forward to working with you to explore the terrorist threat, no matter where that threat originates. We must not take a myopic approach. We must protect this country from all enemies, foreign and domestic. Our view of the terrorist threat must include domestic terrorism. The focus on domestic terrorism was noticeably absent in the last Congress.

Finally, I noticed that disaster response and recovery was not included in your list of priorities. I would urge you to add this important area.

No corner of this Nation is safe from the devastation of a natural disaster. Our people must know that we will not forget them and are committed to improving the systems that must serve them in their most dire moment whether it is Hattiesburg, Mississippi, or New York City, New York.

Again, Mr. Chairman, I look forward to working with you and thank you for holding this hearing.

With that, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

Today we will hear from witnesses who will provide an overview of some the areas you have identified as priorities. I look forward to their testimony and thank each of them for appearing today. Before we hear the testimony, it is important to point out that as Members of Congress, each of us has a responsibility to ensure that the Department is able to adequately perform its mission of protecting this Nation from and responding to terrorist attacks, man-made catastrophes, and natural disasters.

As Members of this committee, each of us has a responsibility to assure the success of the homeland security mission. That mission cannot be achieved without appropriate funding, vigorous oversight, and targeted legislation. We cannot play our part in assuring the success of the homeland security mission if we are not willing to use the full weight of the committee structure—both subcommittees and the full committee—to pursue a well-crafted agenda. That agenda should result in bringing our bills to the floor and assuring that our oversight yields effective outcomes. Our energies will be wasted and our opportunities will be squandered if we do not work toward the goal of making the people of this Nation safer.

Therefore, Mr. Chairman, I commend you, for issuing a statement of priorities and hope that the work of this committee and each of its subcommittees will remain focused on those objectives and our mission during this session of Congress.

One of your priorities is border security. Since 2004, we have doubled the number of Border Patrol agents and more than doubled the number of unauthorized aliens removed from this country. In our examination of border security, we cannot be limited by calling for more of the same. DHS currently lacks a border security strategy that coordinates CPB, ICE, and Coast Guard. We must continue to press DHS for such a strategy. Without it, we cannot be certain that our border control resources are strategic and well-coordinated.

Another priority is cybersecurity. As you know, today, the administration released an Executive Order on cybersecurity. It is my understanding that the strategy calls for strong privacy and civil liberties protections and recognizes the necessary leadership of the Department of Homeland Security in establishing a voluntary program to promote the adoption of a Cybersecurity Framework. This strategy sounds a great deal like the PRECISE Act, a bill this committee marked up last Congress but was prevented from moving to the Floor by the Majority leadership. As we review cybersecurity, I hope we can try once again to take the PRECISE Act to the floor of the House.

Third, I appreciate your identification of the management and administrative functions of the Department as one of your priorities. As you may know, since the inception of the Department, I have worked to bring accountability and transparency to their personnel and contracting practices. The Department cannot succeed unless every component is brought into an organizational structure that gives headquarters command and control over the most basic personnel rules and contracting procedures. Without such centralized authority and accountability, we should not be surprised by stories of waste, fraud, and abuse.

Fourth, I look forward to working with you to explore the terrorist threat, no matter where that threat originates. We must not take a myopic approach. We must protect this country from all enemies—foreign and domestic. Our view of the terrorist threat must include domestic terrorism. The focus on domestic terrorism was notably absent in the last Congress.

Finally, I noticed that disaster response and recovery was not included in your list of priorities. I would urge you to add this important area. No corner of this Nation is safe from the devastation of a natural disaster. Our people must know that we will not forget them and are committed to improving the systems that must serve them in their most dire moment—whether in Hattiesburg, Mississippi, or New York City, New York.

Chairman MCCAUL. I thank you the Ranking Member. Let me just comment, us both being from Gulf Coast States that I join with you in your commitment to disaster response, and I look forward to a Congress where I believe we can work in a bipartisan way to get things done.

I have met with Senator Carper and Coburn who Chair and the Ranking Member of the Homeland Security Committee in the Senate. Hopefully we can work in a bicameral way to get something done and passed and signed into one.

So with that, I am pleased to have five distinguished witnesses before us today on this important topic. The first—and actually, all of you are no strangers to this committee.

Admiral Thad Allen is the senior vice president at Booz Allen Hamilton. He completed his distinguished career in the United States Coast Guard as its 23rd Commandant. In 2010, President Obama selected Admiral Allen to serve as the national incident commander for the unified response to the Deepwater Horizon oil spill in the Gulf Coast of Mexico. Prior to his assignment as Commandant, Admiral Allen served as Coast Guard chief of staff.

Mr. Shawn Henry is a retired executive assistant director of the FBI's Cyber Division. He is credited with boosting the FBI's computer crime and cybersecurity investigative capabilities. He oversaw computer crime investigation spanning the globe including denial-of-service attacks, bank and corporate breaches, and state-sponsored intrusions. He is currently the president of CrowdStrike Services.

The Honorable Michael Leiter served under two presidents as the director of the National Counterterrorism Center until—from June 2008 to July 2011. He remains a highly respected voice on terrorism threats and National security.

Currently, Mr. Leiter is the senior counsel to the chief executive officer of Palantir Technologies. In addition, he serves as the national security and counterterrorism analyst for NBC news.

The Honorable David Walker is the founder and CEO of the Comeback America Initiative. In this capacity, he leads CAI's efforts to promote fiscal responsibility. Prior to assuming his current position, Mr. Walker served as the 7th comptroller general of the United States and head of the U.S. Government Accountability Office for nearly 10 years.

I must commend you, you were one of the first to identify really that the debt problem that we have in the United States is truly a National security issue, and for that, we are very grateful.

Mr. Clarke Kent Ervin; no stranger to this committee; no stranger to me. We worked together under attorney general, now Senator John Cornyn. He is a member of the Homeland Security Defense Technology Transfer and International Practice Groups at Patton Boggs Law Firm in Washington, DC.

He previously served as first inspector general for the Department of Homeland Security under President Bush. He has been a member of the Homeland Security Secretary Janet Napolitano's Homeland Security Advisory Council since 2009.

The witnesses' full written statements will appear in the record. The Chairman now recognizes Admiral Allen for 5 minutes for an opening statement.

STATEMENT OF ADMIRAL THAD W. ALLEN (RET.), SENIOR VICE PRESIDENT, BOOZ ALLEN HAMILTON

Admiral ALLEN. Thank you, Mr. Chairman, for the opportunity to be here this morning.

Mr. Thompson, it is good to see you again.

It is good to appear before the committee.

This morning I would like to talk about one specific aspect of homeland security understanding there is a broad set of challenges as you have articulated. We have got a distinguished panel that is going to address things like cybersecurity, which is a very important issue for all of us to think about.

I would like to talk a little bit about the borders and maybe take a different approach on how we think about the borders in advance considering strategy and also the upcoming second Quadrennial Homeland Security Review.

Being from Tucson, Arizona and being raised in the Southwest and having operated for 39 years in the Coast Guard and as part of the Department of Homeland Security since its inception, I think it is important to understand that when we talk about the border we tend to think about the border from where we see it and where we sit.

It is much different at a port of entry and between ports of entry. The maritime domain is a band of various bands of jurisdiction. We have air and space and obviously cyber as well.

I think as we move forward, know that we have passed the 10-year mark of homeland security, we need to stop thinking about border function as an aggregation of the authorities and the jurisdictions of the components that were brought into the Department whether it was the former INS inspection function or the customs inspection function and start to think about it as a system of responsibilities that we as a sovereign nation carry out.

There are geographical and physical aspects to the border and we understand those very, very well and they are drawn on maps, but a lot of the trade and security practices in and around the border actually take place without any human intervention.

You can have cargo leave Europe, pass into the United States, the documentation associated with that and the shippers are evaluated, algorithms are checked, and if there is any suspect cargo, that is pulled aside and is checked.

Absent that, the fees are transferred, tariffs are paid, and you have a light bulb moved from Romania to Omaha. I think looking forward in the Department we need to start thinking about the virtual aspects of the border together with the geographical and physical aspects and not take it as a collection of authorities and jurisdictions of the components.

We need to understand what it is we want to do as a Nation at the border, how to carry out our sovereign responsibility to manage borders in a global commons and understand the interaction of what happens with trade and security.

Operational control of the border is something that has been discussed for a number of years. The fact of the matter is, that varies on where you are at on the border.

Operational control of the border is a very different at Otay Mesa and Juarez than it is in Ojinaga and the big, big bang country of Texas and I think we need to understand that any particular stretch of the border there are different ways to look at what constitutes border security and what is the best way to establish operational control, and I think we need a consensus on how to move forward.

As we transition from the air domains, the sea domains, and the land domains, there needs to be better integration between TSA, the Coast Guard, CBP, and within CBP between the field operations inspection function and the Border Patrol function between the ports of entry.

This includes increased data sharing. You mentioned situational awareness. We need to create a common operating picture that can be shared across those domains and increase the interoperability between the agencies that have authorities and jurisdictions out there.

We need to look at things like preclearance for TSA and CBP and expand that wherever we can. It is better to address those threats before they even get near the United States. That is part of managing the borders as well.

I think if we can come up with a system of systems that constitutes what our strategy and our strategic intent is, our vision for the future of the country in carrying out to those sovereign responsibilities, we should pull ourselves towards that future and not try and incrementally change what was put together in 2003 under the

exigencies of the Homeland Security Act passage, which 10 years later we have not materially changed either organizationally in terms of authorities and jurisdictions or capabilities.

My recommendation to the committee would be to pursue strategic change in the context of the Quadrennial Homeland Security Review that will be conducted in the next year and the better we can integrate the development of strategy and implementation of change in homeland security through that vehicle, it will be consistent with the Homeland Security Act and in my view, should drive resource and budget allocation decisions.

I would be happy to answer any questions, sir.

[The prepared statement of Admiral Allen follows:]

PREPARED STATEMENT OF THAD W. ALLEN

13 FEBRUARY 2013

Mr. Chairman, Ranking Member Thompson, and Members of the committee, I am pleased to have been invited to testify on this important topic and I thank you for the opportunity.

A Retrospective

Mr. Chairman, the 1st of March will mark the Tenth Anniversary of stand-up of the Department of Homeland Security. The Department was officially created on the 24th of January 2003, but the operating components from other departments were not moved to DHS until 1 March 2003 when the Department became operational. From the signing of the Homeland Security Act on 25 November 2012 to the actual operation of the Department on 1 March barely 3 months passed. I am not here to dwell on the past but it is important to understand the circumstances under which the Department was created.

While this could be considered Government at light speed, little time was available for deliberate planning and thoughtful consideration of available alternatives. The situation was complicated by the fact that the law was passed between legislative sessions and in the middle of a fiscal year. Other than Secretary Ridge, early leadership positions were filled by senior officials serving in Government. Confirmation was not required to be "acting." Funding was provided through the reprogramming of current funds from across Government for Departmental elements that did not have existing appropriations from their legacy departments.

Operating funds for components that were transferred were identified quickly and shifted to new accounts in the Department to meet the deadline. Because of the wide range of transparency and accuracy of the appropriation structure and funds management systems of the legacy departments some of the new operational components faced a number of immediate challenges. Estimating the cost of salaries for Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE) required the combination of different work forces, with different grade structures, different career ladders, and different work rules.

Basic mission support functions of the Department such as financial accounting, human resource management, real property management, information resource management, procurement, and logistics were retained largely at the component level in legacy systems that varied widely. Funding for those functions was retained at the component level as well. In those cases where new entities were created (i.e. Departmental-level management and operations, the Under Secretary for Science and Technology, the Under Secretary for Intelligence and Analysis, the Domestic Nuclear Detection Office) support systems had to be created rapidly to meet immediate demands of mission execution. Finally, components and Departmental offices that did not preexist the legislation were located in available space around the Washington, DC area and the Secretary and number of new functions were located at the Nebraska Avenue Complex in Northwest Washington.

At the time of this transition I was serving as the Coast Guard Chief of Staff and was assigned as the Coast Guard executive to overseas the Service's relocation from the Department of Transportation to the new Department. We began planning for eventual relocation as soon as the administration submitted legislation to the Congress. I also assigned personnel to the Transition Planning Office (TPO) that was created in the Office of Management and Budget by Executive Order to prepare for the transition. A considerable challenge during this period was the fact that the

TPO was part of the Executive Office of the President and there were legal limitations on how much of their work could be shared externally. As a result much of that effort was redone or duplicated when the Department was created.

As I noted earlier, my intent is not to dwell on the past but to frame the degree of difficulty facing the leaders attempting to stand up the Department from the outset. Many of these issues persist today, 10 years later. Despite several attempts to centralize and consolidate functions such as financial accounting and human resource management, most support functions remain located in Departmental components and the funding to support those functions remains in their appropriations. Because of dissimilarities between appropriations structures of components transferred from legacy departments there is a lack of uniformity, comparability, and transparency in budget presentations across the Department. As a result it is difficult to clearly differentiate, for example, between personnel costs, operations and maintenance costs, information technology costs, and capital investment. Finally, the 5-year Future Years Homeland Security Plan (FYHSP) required by the Homeland Security Act has never been effectively implemented as a long-rang planning, programming, and budgeting framework inhibiting effective planning and execution of multi-year acquisitions and investments.

In the Washington Area the Department remains a disjointed collection of facilities and the future of the relocation to the St. Elizabeth's campus remains in serious doubt. As the Chief of Staff of the Coast Guard and Commandant I committed the Coast Guard to the move to St. Elizabeth and only asked that we be collocated with our Secretary and not be there alone. The Coast Guard will move to St. Elizabeth's this year . . . alone. One of the great opportunity costs that will occur if colocation does not happen will be the failure to create a fully functioning National Operations Center for the Department that could serve at the integrating node for Departmental-wide operations and establish the competency and credibility of the Department to coordinate homeland security-related events and responses across Government as envisioned by the Homeland Security Act. As with the mission support functions discussed earlier, the Department has struggled to evolve an operational planning and mission execution coordination capability. As a result, the most robust command-and-control functions and capabilities in the Department reside at the component level with the current NOC serving as a collator of information and reporting conduit for the Secretary.

The combination of these factors, in my view, has severely constrained the ability of the Department to mature as an enterprise. And while there is significant potential for increased efficiencies and effectiveness, the real cause for action remains the creation of unity of effort that enables better mission performance. In this regard there is no higher priority than removing barriers to information sharing within the Department and improved operational planning and execution. Effective internal management and effective mission execution require the same commitment to shared services, information systems consolidation, the reduction in proprietary technologies and software, and the employment of emerging cloud technologies.

Mr. Chairman, this summary represents my personal views of the more important factors that influenced the creation and the first 10 years of the Department's operations. It is not all-inclusive but is intended to be thematic and provide a basis for discussion regarding the future. Looking to the future the discussion should begin with the Department's mission and the need to create unity of effort internally and across the homeland security enterprise. I made similar comments before the Senate Committee on Homeland Security and Government Affairs last year.

The Future

The Quadrennial Homeland Security Review was envisioned as a vehicle to consider the Department's future. The first review completed in 2010 described the following DHS missions:

- Preventing Terrorism and Enhancing Security;
- Securing and Managing Our Borders;
- Enforcing and Administering our Immigration Laws;
- Safeguarding and Securing Cyberspace;
- Insuring Resiliency to Disasters.

An additional area of specific focus was the maturation of the homeland security "enterprise" which extends beyond the Department itself to all elements of society that participate in and contribute to the security of the homeland.

The QHSR outcomes were consistent with the fiscal year 2010 budget that was submitted in early 2009 following the change of administrations. That request laid out the following mission priorities for the Department:

- Guarding Against Terrorism;
- Securing Our Borders;

- Smart and Tough Enforcement of Immigration Laws and Improving Immigration Services;
- Preparing For, Responding To, and Recovering From Natural Disasters;
- Unifying and Maturing DHS.

The fiscal year 2010 budget priorities and the follow-on QHSR mission priorities have served as the basis for annual appropriations requests for 4 consecutive fiscal years.

I participated in the first review prior to my retirement and we are approaching the second review mandated by the Homeland Security Act. This review presents an opportunity to assess the past 10 years and rethink assumptions related to how the broad spectrum of DHS authorities, jurisdictions, capabilities, and competencies should be applied most effectively and efficiently against the risks we are likely to encounter . . . and how to adapt to those that cannot be predicted. This will require a rethinking of what have become traditional concepts associated with homeland security over the last 10 years.

Confronting Complexity and Leading Unity of Effort

Last year in an issue of Public Administration Review (PAR), the journal of the American Society for Public Administration (ASPA), I wrote an editorial piece entitled "Confronting Complexity and Leading Unity of Effort." I proposed that the major emerging challenge of public administration and governing is the increased level of complexity we confront in mission operations, execution of Government programs, and managing non-routine and crisis events. Driving this complexity are rapid changes in technology, the emergence of a global community, and the ever-expanding human-built environment that intersects with the natural environment in new, more extreme ways.

The results are more vexing issues or wicked problems we must contend with and a greater frequency of high-consequence events. On the other hand advances in computation make it possible to know more and understand more. At the same time structural changes in our economy associated with the transition from a rural agrarian society to a post-industrial service/information economy has changed how public programs and services are delivered. No single Department, agency, or bureau has the authorizing legislation, appropriation, capability, competency, or capacity to address this complexity alone. The result is that most Government programs or services are "co-produced" by multiple agencies. Many involve the private/non-governmental sector, and, in some cases, international partners. Collaboration, cooperation, the ability to build networks, and partner are emerging as critical organizational and leadership skills. Homeland security is a complex "system of systems" that interrelates and interacts with virtually every department of Government at all levels and the private sector as well. It is integral to the larger National security system. We need the capabilities, capacities, and competency to create unity of effort within the Department and across the homeland security enterprise.

MISSION EXECUTION AND MISSION SUPPORT

As we look forward to the next decade I would propose we consider two basic simple concepts: Mission execution and mission support. Mission execution is deciding what to do and how to do it. Mission support enables mission execution.

Mission Execution . . . Doing the Right Things Right

As a precursor to the next QHSR there should be a baseline assessment of the current legal authorities, regulatory responsibilities, treaty obligations, and current policy direction (i.e. HSPD/NSPD). I do not believe there has been sufficient visibility provided on the broad spectrum of authorities and responsibilities that moved to the Department with the components in 2003, many of which are non-discretionary. Given the rush to enact the legislation in 2002 it makes sense to conduct a comprehensive review to validate the current mission sets as established in law.

The next step, in my view, would be to examine the aggregated mission set in the context of the threat environment without regard to current stove-piped component activities . . . to see the Department's mission space as a system of systems. In the case of border security/management, for example, a system-of-systems approach would allow a more expansive description of the activities required to meet our sovereign responsibilities.

Instead of narrowly focusing on specific activities such as "operational control of the border" we need to shift our thinking to the broader concept of the management of border functions in a global commons. The border has a physical and geographical dimension related to the air, land, and sea domains. It also has a virtual, information-based dimension related to the processing of advance notice of arrivals, analysis data related to cargoes, passengers, and conveyances, and the facilitation of trade.

These latter functions do not occur at a physical border but are a requirement of managing the border in the current global economic system.

The air and maritime domains are different as well. We prescreen passengers at foreign airports and the maritime domain is a collection of jurisdictional bands that extend from the territorial sea to the limits of the exclusive economic zone and beyond.

The key concept here is to envision the border as an aggregation of functions across physical and virtual domains instead of the isolated and separate authorities, jurisdictions, capabilities, and competencies of individual components. Further, there are other Governmental stakeholders whose interests are represented at the border by DHS components (i.e. Department of Agriculture, DOT/Federal Motor Carriers regarding trucking regulations, NOAA/National Marine Fisheries Service regarding the regulation of commercial fishing).

A natural outcome of this process is a cause for action to remove organizational barriers to unity of effort, the consolidation of information systems to improve situational awareness and queuing of resources, and integrated/unified operational planning and coordination among components. The additional benefits accrued in increased efficiency and effectiveness become essential in the constrained budget environment. The overarching goal should always be to act with strategic intent through unity of effort.

A similar approach could be taken in considering the other missions described in the QHSR. Instead of focusing on "insuring resiliency to disasters" we should focus on the creation and sustainment of National resiliency that is informed by the collective threat/risks presented by both the natural and human-built environments. The latter is a more expansive concept than "infrastructure" and the overall concept subsumes the term "disaster" into larger problem set that we will face. This strategic approach would allow integration of activities and synergies between activities that are currently stovepiped within FEMA, NPPD, and other components. It also allows cybersecurity to be seen as an activity that touches virtually every player in the homeland security enterprise.

In regard to terrorism and law enforcement operations we should understand that terrorism is, in effect, political criminality and as a continuing criminal enterprise it requires financial resources generated largely through illicit means. All terrorists have to communicate, travel, and spend money, as do all individuals and groups engaged in criminal activities. To be effective in a rapidly-changing threat environment where our adversaries can quickly adapt, we must look at cross-cutting capabilities that allow enterprise-wide success against transnational organized criminal organizations, illicit trafficking, and the movement of funds gained through these activities. As with the "border" we must challenge our existing paradigm regarding "case-based" investigative activities. In my view, the concept of a law enforcement case has been overtaken by the need to understand criminal and terrorist networks as the target. It takes a network to defeat a network. That in turn demands even greater information sharing and exploitation of advances in computation and cloud-based analytics. The traditional concerns of the law enforcement community regarding confidentiality of sources, attribution, and prosecution can and must be addressed, but these are not technology issues . . . they are cultural, leadership, and policy issues.

Mr. Chairman, this is not an exhaustive list of proposed missions or changes to missions for the Department. It is an illustrative way to rethink the missions of the Department given the experience gained in the last 10 years. It presumes the first principals of: (1) A clear, collective strategic intent communicated through the QHSR, budget, policy decisions, and daily activities, and (2) an unyielding commitment to unity of effort that is supported by an integrated planning and execution process based on transparency and exploitation of information to execute the mission.

Mission Support . . . Enabling Mission Execution

Mr. Chairman, in my first 2 years as Commandant I conducted an exhaustive series of visits to my field commands to explain my cause for action to transform our Service. In those field visits I explained that when you go to work in the Coast Guard every day you do one of two things: You either execute the mission or you support the mission. I then said if you cannot explain which one of these jobs you are doing, then we have done one of two things wrong . . . we haven't explained your job properly or we don't need your job. This obviously got a lot of attention.

In the rush to establish the Department and in the inelegant way the legacy funding and support structures were thrown together in 2003, it was difficult to link mission execution and mission support across the Department. To this day, most resources and program management of support functions rest in the components. As

a result normal mission support functions such as shared services, working capital funds, core financial accounting, human resources, property management, and integrated life cycle-based capital investment have been vexing challenges.

There has been hesitancy by components to relinquish control and resources to a Department that appears to be still a work in progress. The structure of Department and component appropriations does not provide any easy mechanism for Departmental integration of support functions. As a result information sharing is not optimized and potential efficiencies and effectiveness in service delivery are not being realized. As I noted earlier, a huge barrier to breaking this deadlock is the lack of uniformity in appropriations structures and budget presentation. This problem has been compounded by the failure to implement a 5-year Future Years Homeland Security Plan and associated Capital Investment Plan to allow predictability and consistency across fiscal years.

Mr. Chairman, having laid out this problem, I see three possible ways forward. The desirable course of action would be to build the trust and transparency necessary for the Department and components to collective agree to rationalize the mission support structure and come to agreements on shared services. The existing barriers are considerable but the first principals of mission execution apply here as well . . . unambiguous, clearly communicated strategic intent and unity of effort supported by transparency and knowledge-based decisions. A less palatable course of action is top-down directed action that is enforced through the budget process. The least desirable course of action is externally-mandated change. Unfortunately, the current fiscal impasse and the need to potentially meet sequester targets while facing the very real prospect of operating under a continuing resolution for the entire fiscal year 2013 represents the confluence of all of these factors and a fiscal perfect storm. There is a case to act now. We should understand that a required first step that lies within the capability of the Department would be to require standardized budget presentations that can serve as the basis for proposed appropriations restructuring to clearly identify the sources and uses of funds and to separate at a minimum personnel costs, operating and maintenance costs, information technology costs, capital investment, and facility costs.

Creating and Acting with Strategic Intent

Mr. Chairman, I have attempted to keep this testimony at a strategic level and focus on thinking about the challenges in terms that transcend individual components, programs, or even the Department itself. I have spoken in the last year to the Department of Homeland Security Fellows and the first DHS Capstone course for new executives. I have shared many of the thoughts provided today over the last 10 years to many similar groups. Recently, I have changed my message. After going over the conditions under which the Department was formed and the many challenges that still remain after 10 years, I was very frank with both groups. Regardless of the conditions under which the Department was created and notwithstanding the barriers that have existed for 10 years, at some point the public has a right to expect that the Department will act on its own to address these issues. Something has to give. In my view, it is the responsibility of the career employees and leaders in the Department to collectively recognize and act to meet the promise of the Homeland Security Act. That is done through a shared vision translated into strategic intent that is implemented in daily activities from the NAC to the border through the trust and shared values that undergird unity of effort. It is that simple; it is that complex.

I understand the committee is considering whether the Department should develop a comprehensive border strategy that would encompass all components and entities with border equities, including State and local law enforcement. I also understand there is concern about performance metrics associated with carrying out such a strategy. There are also potential opportunities related to the equipment being returned from military operations in Iraq and Afghanistan. Finally, we are witnessing a transition of leadership in Mexico as we continue to jointly address the threat of drug and other illicit trafficking as a major hemispheric threat.

In considering the strategic course of action going forward regarding the management of the border in a global commons or any of the diverse missions of the Department of Homeland Security, we should remember then General Eisenhower's admonition that "Plans are nothing; planning is everything." I have been involved in strategic planning for decades I can attest to their value. Done correctly that value is derived from a planning process that forces critical thinking, challenges existing assumptions, creates shared knowledge and understanding, and promotes a shared vision. Accordingly, I would be more concerned about the process of developing a strategy than the strategy itself. It is far more important to agree on the basic terms of reference that describe the current and likely future operating envi-

ronment and to understand the collective capabilities, competencies, authorities, and jurisdictions that reside in the Department as they relate to that environment and the threats presented.

I believe the Homeland Security Act envisioned that process to be the Quadrennial Homeland Security Review. Accordingly, the committee may want to consider how that process that is already mandated in law might become the vehicle to create strategic intent. Intent that unifies Departmental action, drives resource allocation, integrates mission support activities, removes barriers to information sharing and creates knowledge.

Strategic Intent and the Border

I am often asked, in the wake of the Deepwater Horizon oil spill, "Is it safe to drill offshore?" My answer to that question is relevant to any consideration of how we carry out the sovereign responsibilities of a Nation in managing our border. My answer is that there is no risk-free way to extract hydrocarbons from the earth. The real question is: "What is the acceptable level of risk associated with those activities in light of the fact that it will take a generation to develop alternate fuels?" Likewise, there is no risk-free way to manage a border short of shutting it down. Discussions about operational control of the border and border security too often focus on specific geographical and physical challenges related to managing the land border. While those challenges exist, they cannot become the sole focus of a strategy that does not account of all domains (air, land, sea, space, and cyber) and the risks and opportunities that the border represents. As I mentioned earlier we need to think of the border as a set of functions. We need to think about what is the acceptable level of risk associated with those functions. We cannot neglect trade and become fixated on driving risk to zero; it cannot be done.

Whether it is TSA considering options for passenger and cargo screening, the Coast Guard considering the trade-offs between fisheries and drug enforcement, ICE considering resource allocation to protect intellectual property or remove dangerous aliens, NPPD considering how to deal with cyber threats to infrastructure, or USCIS deciding how immigration reform would drive demand for their services, the real issue is the identification and management of risk. Those decision are made daily now from the Port of Entry at Nogales to the Bering Sea, from TSA and CBP preclearance operations in Dublin to Secret Service protection of the President, and from a disaster declaration following a tornado in Mississippi to the detection of malware in our networks. The question is: How are they linked? Are those actions based on a shared vision that make it clear to every individual in the Department what their role is in executing or supporting the mission?

A strategy for the border or any DHS mission ideally would merely be the codification of strategic intent for record purposes to support enterprise decisions. The creation of self-directed employees that understand their role in Departmental outcomes on a daily basis in a way that drives their behavior should be the goal. If a border strategy is desired, I believe it must be preceded by a far deeper introspective process that addresses how the Department understands itself and its missions as a unified, single enterprise.

Chairman MCCAUL. Thank you, Admiral Allen.

Mr. Henry, you are now recognized for 5 minutes.

STATEMENT OF SHAWN HENRY, PRESIDENT, CROWDSTRIKE SERVICES

Mr. HENRY. Good morning Chairman McCaul, Ranking Member Thompson, and Members of the committee.

I appreciate the opportunity to be here with you this morning to talk to you about the cyber threat that we face as a Nation and some of the significant economic and National security challenges that we are at risk against. I appreciate the level of attention that the committee is affording this issue.

I know I have spoken of cyber threat for so long, but I think it is just so important and it can't be overemphasized. So I need to state it again emphatically that there are foreign adversaries that have targeted every major organization in this country. In each of your districts, major companies that have been breached and there

has been a tremendous impact on the economy there and on their ability to be competitive in a global society.

They have stolen untold billions of dollars of intellectual property, research and development, and corporate strategies and secrets and the volume and sophistication of these cyber threats is only increasing and I don't see that that is going to change in the current environment.

Over time, a cyber adversary with motivation, time, and resources will breach every network that is connected or every computer system that is directly accessible to the internet.

I stated publicly that it is necessary for network administrators to assume they have already been breached rather than waiting for the intrusion detection systems to tell them.

Many have absolutely no knowledge that this is occurring and they don't know that adversaries remain resident on their network many times for months or even years before they are ever identified, if at all.

While I was executive assistant director at the FBI, my agents went out routinely, dozens of times every month, and told companies that they had been breached and they had no idea that that had occurred meaning that all of their proprietary data, their communications, their financial statements had been completely accessible to the adversary with unfettered access on that network.

Organizations therefore, must aggressively, constantly look on their network for the adversary and hunt for those adversaries. Alarmingly and increasingly, attackers are moving beyond mere theft of information and they are moving into the actual manipulation or the destruction of data and with the depth and breadth of access that they have that is not a hard or difficult task to accomplish.

Those with malicious intent can take devastating actions, and it is difficult to say with confidence that our critical infrastructure will be available when we most need it.

There needs to be a paradigm shift in the way we address these issues. Vulnerability mitigation is the current cybersecurity approach in the private sector, and it has been the focus for more than 20 years. We continuously focus on hardening the networks through "Defense-in-Depth", using firewalls and anti-virus, looking at patching vulnerabilities, and employing intrusion detection systems.

This approach generally stops those actors who do not care who they are trying to breach, like the opportunistic burglar who goes from house to house shaking the doorknob.

One mistake, however, is that we are using the same approach against the most sophisticated state-funded actors who actually have specific targets in mind. They have got intelligence requirements and they are looking for very specific information and they will get that information. Again, over time, they will breach those networks.

Unlike the thief of opportunity, they are seeking the Hope Diamond, something very, very specific, and those advanced and well-funded adversaries will make sure that they achieve their goal.

While we must continue to improve our defenses, we must continue to build and have defense-in-depth. We need to focus our ef-

forts on the threat. Employing a threat mitigation strategy requires an increased ability to detect and identify our adversaries and penalize them, not merely defend against them.

It is the identical strategy that we use and employ in the physical world every single day to thwart criminals, terrorists, and spies.

Achieving these goals in the cyber environment will require unprecedented coordination between private industry—which as a whole has network ownership and the ability to achieve these goals—and the Government, which is primarily authorized to investigate and penalize them.

Inevitably we must bring the private sector and the Government together to achieve the goal of threat deterrence. The vast majority of the intelligence that will lead to information and identification of the adversaries resides on private-sector networks; they are, in essence, "crime scenes," and the evidence and artifacts are resident on those networks.

That intelligence can't be shared periodically through human interaction, but it needs to be shared among all victims immediately at network speed.

The Department of Homeland Security may be able to share with vulnerability reduction strategies and guidelines with the private sector and likewise they are responsible for consequence management after a breach.

Additionally, though, under a threat mitigation model, DHS is a potential intermediary between other Government agencies and the private sector where they can collect intelligence which leads to identification and attribution of the adversary.

Likewise, the Government has intelligence collection that will make the private sector infinitely more resilient and they need to share that information aggressively.

I know how the intelligence is collected and I recognize there needs to be a protection of sources and methods, but there is a lot more that the Government is able to do.

Any intelligence sharing between Government and private sector must be done in a way that is respectful of and consistent with privacy of our citizens, and we must start by opening the debate on the limitations of the existing defensive-only security model and the necessity of a threat deterrence model.

I look forward to working with the committee and Congress as a whole to determine a successful course forward for the Nation that allows us to reap the positive benefits and the economic benefits of the internet while minimizing the risk posed by those who seek to do us irreparable harm, and I encourage our further collaboration.

I am happy to answer any questions.

[The prepared statement of Mr. Henry follows:]

PREPARED STATEMENT OF SHAWN HENRY

FEBRUARY 13, 2013

Good afternoon Chairman McCaul, Ranking Member Thompson, and Members of the committee. Thank you for having me here today to discuss the cyber threats facing our Nation, how these threats impact our Government and private-sector networks, and the significant risk posed to our economic and National security. I sin-

cerely believe this is one of the most critical issues facing our Nation, and I appreciate the level of attention this committee is affording it.

THE CYBERSECURITY THREAT

We have spoken of the cyber threats for far too long, but it is too important and cannot be overemphasized. So I'll state it again, emphatically . . . foreign adversaries have targeted every major organization in this country, and have stolen untold billions of dollars of intellectual property, research and development, and corporate strategies and secrets. The volume and sophistication of cyber attacks has increased dramatically over the past 5 years, and in the current environment it will continue to grow.

Given enough time, motivation, and funding, a determined adversary will penetrate any system that is accessible directly from the internet. Even systems not touching the network are susceptible to attack via means other than remote access, including the trusted insider using devices such as USB thumb drives, and the supply chain.

I have stated publicly that it is necessary for network administrators to assume they have already been breached rather than waiting for their intrusion detection systems to alert them to an infiltration. Many have absolutely no knowledge that an adversary was, or remains resident on, their network, often times for weeks, months, or even years. While I was EAD at the FBI, our agents regularly knocked on the door of victim companies and told them their network had been intruded upon and their corporate secrets stolen, because we found their proprietary data resident on a server in the course of another investigation. We were routinely telling organizations they were victims, and these victims ranged in size and industry, and cut across all critical sectors. Organizations must, therefore, actively and constantly hunt for the adversary on their network.

Alarmingly and increasingly, attackers are moving beyond mere exfiltration or theft of data. With the breadth and depth of access they have, adversaries can and have manipulated, disrupted, or destroyed data and infrastructure. Those with malicious intent can take devastating actions, and it is difficult to say with confidence that our critical infrastructure—the backbone of our country's economic prosperity, National security, and public health—will remain unscathed and always be available when needed.

A PARADIGM SHIFT IN STRATEGY

My colleagues at CrowdStrike, George Kurtz and Dmitri Alperovitch, have talked about the deterrence of threat actors for years. Steven Chabinsky, my colleague at the FBI for 17 years, and currently with me at CrowdStrike as SVP of Legal Affairs, also discusses the paradigm shift necessary in cybersecurity strategy.

Vulnerability mitigation is the current cybersecurity approach in the private sector, and has been for the past 20 years. We continuously focus on hardening our networks by "Defense-in-Depth", using firewalls, anti-virus software, patching vulnerabilities, and employing intrusion prevention systems. This approach generally stops those actors who do not care who their specific targets are, but are simply like burglars who are willing to rob anybody's house and take anybody's jewelry.

Our mistake, however, is that we are using the same approach against Advanced Persistent Threat actors who actually have specific targets in mind, and are not going to stop until they have reached their goals. These modern-day cyber burglars are targeting the equivalent of the Hope Diamond, quite specifically, not fungible engagement rings. For our most advanced and well-funded adversaries, there are no substitutes for their targets, regardless of how many, and they will continue their onslaught until they achieve success.

Ironically, our own defensive efforts have actually made the problem worse, by encouraging our adversaries to outperform us, while we outspend them. Although many are not prepared to consider this possibility, the result of our failure to distinguish between the novice and the professional adversary has been a proliferation of more capable malware, created by nation-state adversaries and organized crime groups, and an escalation of their activities in order to defeat our defenses.

WHAT DOES THIS MEAN?

Employing a threat mitigation strategy requires an increased ability to detect and identify our adversaries, and to penalize them. This is the identical strategy we employ in the physical world every single day to thwart criminals, spies, and terrorists.

Achieving these goals in the cyber environment, however, will require unprecedented coordination between private industry—which as a whole has the ownership

and ability to achieve these goals, and governments, which are primarily authorized to investigate and penalize them.

Inevitably we must bring the private sector and the Government together to achieve the goal of threat deterrence. The vast majority of the intelligence that will lead to identification of the adversaries resides on private-sector networks; they are, in essence, "crime scenes", and the evidence and artifacts of the breach are resident on those networks. That threat intelligence, too, can't be shared periodically via e-mail at human speed; it needs to be shared among all victims, in real-time, at network speed. The private sector, then, can fill tactical gaps that the Government is blind to. This can be done while respecting privacy, a critical and absolutely necessary element of intelligence sharing.

The Department of Homeland Security (DHS) naturally has the responsibility for developing and promulgating necessary vulnerability reduction strategies and guidelines. Likewise, they are responsible for consequence management after a breach. Additionally, though, with a threat mitigation model, DHS is a potential intermediary between other Government agencies and the private sector to facilitate the analysis and dissemination of "big data"—collected intelligence—leading to identification and attribution of adversaries.

Likewise, the Government has intelligence collection on the threat actors that is different from, and additive to, that collected by the private sector. Knowing what I do about that intelligence, and how it's collected, I am certain the Government can share much more data with industry than is currently shared today. That intelligence will add infinite value, and it can be packaged and shared with the private sector without threatening the integrity of the sources and methods through which it's collected. Again, privacy is and must remain a key tenet of any intelligence sharing strategy.

When the adversary is identified, the Government can then use its resources and actions—whether it's law enforcement, the intelligence community, diplomatic, or financial—to mitigate the threat posed by these sophisticated opponents. The consistent threat posed by adversaries will subside only when the cost to operate outweighs any potential gain.

CONCLUSION

We face significant challenges in our efforts to combat the cyber threat. I am optimistic that by strengthening partnerships, effectively sharing intelligence, and successfully identifying our adversaries, we can best protect businesses and critical infrastructure from grave damage.

We must start, however, by opening the debate on the limitations of the existing defensive-only security model and the necessity of a threat deterrence model. Further, we need a public discussion of how Government and industry can jointly work together to achieve a safer cyber environment by shining a light on our adversaries instead of consistently telling victims to "just do more."

I look forward to assisting the committee, and Congress as a whole, to determine a successful course forward for the Nation that allows us to reap the positive economic and social benefits of the internet while minimizing the risk posed by those who seek to do us irreparable harm.

I encourage our further collaboration, and I'm happy to answer any questions.

Chairman MCCAUL. Thank you, Mr. Henry.

Mr. Leiter is now recognized.

STATEMENT OF MICHAEL E. LEITER, FORMER DIRECTOR OF THE NATIONAL COUNTERTERRORISM CENTER

Mr. LEITER. Chairman McCaul, Ranking Member Thompson, it is a pleasure to be back in front of the committee and I will take the liberty of speaking on behalf of all of my co-witnesses; it is especially nice to be up here as a former Government official.

I am extremely happy that this committee is looking at all homeland threats because I think with that change in the counterterrorism threat or terror threats that we have seen over the past several years and the very stark fiscal landscape we face, this is a very appropriate time to do so.

With the death of Osama bin Laden and the weakness of al-Qaeda in Pakistan, we see the lowest level of sophisticated threat

to the homeland from Pakistan that we have seen since 2001, and that is a very, very good news story thanks to the work of the men and women of the U.S. Government and our allies.

That being said, as the Chairman noted, the splintering of al-Qaeda into a more distributed group with rising dangers in Yemen, North Africa, East Africa, Europe, and the homeland does pose new challenges.

In my view, the al-Qaeda affiliate in Yemen, AQAP, still continues to pose the most serious, sophisticated threat that we face. As we saw in 2009, 2010, and 2012, the organization remains committed to sophisticated IED attacks against the United States and the homeland.

East Africa is surprisingly a brighter spot, something I thought I might never say about Somalia, but in fact, U.S. efforts and Kenyan partnership has reduced that threat and most importantly to this committee, fewer Americans traveling to the region to fight in the jihad than we have seen for years.

On the other hand, North Africa of course is proven some serious darkness over the past several months especially, but I do want to say this carefully, but while the attacks in Benghazi and the BP oil facility are absolutely tragic, in my view, the major change in the region is not a massive increase in the popularity of AQIM, but rather the huge shift that occurred in the region with the fall of the government in Libya, the availability of weapons, the loss of partner security services in the region, and the coup d'état in Mali.

All of that have combined to create a safe haven which is in fact dangerous but I think still does not rise to the level of seriousness that that we have previously seen in Pakistan or we see today in Yemen.

I especially commend the committee for looking into the threat of Hezbollah and Iran, which has often been overlooked over the past 10 years. I think with growing tension between the United States, Israel, and Iran, Hezbollah has proved increasingly active over the past several years, most notably the Bulgarian recognition that Hezbollah targeted and killed six tourists last year and many other failed Hezbollah attacks.

The Hezbollah's and the Iranian Quds Force growing presence in Venezuela and elsewhere in the world could prove a serious problem for the United States and our allies were there to be a conflict with Iran.

I would also add that Iranian aggressive cyber attacks against Saudi Aramco and RasGas, destructive cyber attacks, could also portend for a combined physical and cyber attack by Iran, were certain red lines crossed.

With that as a threat landscape and looking ahead, let me offer some quick views as to things that we have to guard against now 12 years after 9/11.

The first is what I term terrorism fatigue and although this committee does not experience it, many in the United States, and I fear many in Congress do. After hearing about terrorism for 10 or 12 years, people simply don't want to talk about it anymore and there are two specific threats associated with this.

First, with all of our counterterrorism successes that we have had over the past 12 years, which really are incredible, I fear that

any small attack, no matter how small can result in political finger-pointing and a real crucification of our counterterrorism professionals, and although we of course have to look at how we can do this job better, we have to guard against ex-poste investigations that lack a serious appreciation for the ex-ante difficulties of counterterrorism work.

Second, I believe this terrorism fatigue can lead to dangerous lethargy within the Executive branch. I saw over and over again how hard and quickly the Executive branch could work immediately after an attack and then as the months, weeks and months passed by, I saw the impetus for rapid and important change start to drop away. So I hope this committee can hold the Executive branch's feet to the fire on these topics.

Second, weapons of mass destruction. Although this remains a very low likelihood event and we have done very well in combating terrorist acquisition of WMD, the high consequences of such an attack especially biological or radiological or God forbid, improvised nuclear devices, cannot be forgotten and these require long-term investments.

Third, our counterterrorism partnerships. I won't go into detail here but suffice to say with the Arab awakening we have lost some of our most critical partners in the counterterrorism fight and that has significantly increased the risk to the homeland in my view.

Fourth, and this became a high-profile issue over the past several weeks, I believe we have to stay on the offense on all fronts. Perhaps unsurprisingly given my service in the Obama and Bush administrations, I am quite supportive of the policy outlined in the Department of Justice white paper. I am equally supportive of the President's call for greater transparency, and I would urge this committee to work with the intelligence committee to make sure you have the transparency into these programs.

But ultimately I believe that these offensive measures combined with other measures, because this is only one tool, are absolutely critical to homeland security.

Last but not least, and a good transition to the good Honorable David Walker. We have spent close to $100 billion a year on counterterrorism. This is the time to rationalize that and figure out how we can get the most bang for our buck to make sure that the American people are safe.

I think the committee and look forward to working with the Congress in the future.

[The statement of Mr. Leiter follows:]

PREPARED STATEMENT OF MICHAEL E. LEITER

FEBRUARY 13, 2013

OVERVIEW

Chairman McCaul, Ranking Member Thompson, and Members of the committee, thank you for inviting me to testify on my perspectives—which I hope are at least partially "new"—on threats to homeland security. Although the membership on this committee has changed over the years, this body has always been at the forefront of understanding threats and shaping our Government's response to them. On behalf of those who continue to serve in homeland security and intelligence organizations, I want to thank the committee for its continuing oversight and support.

As the 113th Congress considers the current threat landscape, I believe you are correct to reevaluate broadly the state of terrorism and our associated response. Al-

though the growing presence of al-Qaeda-associated elements in North Africa and Syria highlight how the threat of terrorism continues, we have made remarkable strides against the threat of catastrophic attacks like what we experienced on 9/11. Combined with a fiscal reality that precludes the sort of spending we have maintained since that tragic event, this is a historic moment to rationalize and calibrate our response to terrorism, cyber threats, and other related threats to the homeland.

THE THREAT LANDSCAPE

Today al-Qaeda and its allies in Pakistan are at their weakest point since 9/11. The death of Osama bin Ladin and the continued decimation of senior ranks has made the organization a shadow of its former self. Ayman al Zawahiri is not bin Ladin and although the organization still attempts to provide strategic guidance and global propaganda, its influence continues to wane. Whether this trajectory can be maintained with a significant decrease of the U.S. presence in Afghanistan in the coming years will be, in my view, the single biggest determinant of al-Qaeda Core's relevance for the coming decade.

The degradation of al-Qaeda's "higher headquarters" and relatively well-coordinated command and control has allowed its affiliates and its message to splinter, posing new dangers and challenges. Al-Qaeda affiliates or those inspired by its message have worrisome presences in Yemen, East Africa, North Africa, Syria, Western Europe, and of course to a lesser degree the United States.

Beginning with Yemen, in my view al-Qaeda in the Arabian Peninsula (AQAP)—as I stated 2 years ago—continues to pose the most sophisticated and deadly threat to the U.S. homeland from an overseas affiliate. The death of operational commander Anwar al-Awlaki significantly reduced AQAP's ability to attract and motivate English speakers, but its operational efforts continue with lesser abatement. As we saw in 2009, 2010, and 2012, AQAP has remained committed—and able—to pursue complex attacks involving innovative improvised explosives devices. Although some of the organization's safe haven has been diminished because of Yemeni and U.S. efforts, the inability of the government of Yemen to bring true control to wide swaths of the country suggests that the group will pose a threat for the foreseeable future and (unlike many other affiliates) it clearly remains focused on transnational attacks.

East Africa, surprisingly to many, is a brighter spot in our efforts. Although al-Shabaab remains a force and poses significant risks in the region—most especially in Kenya and to the fledgling government in Somalia—its risk to the homeland is markedly less today than just 2 years ago. Kenya's offensive in the region shattered much of al-Shabaab's power base and most importantly for this committee the attractiveness of Somalia to Americans and other Westerners is radically less than was the case. The relative flood of Americans has turned into a trickle, thus significantly reducing the threat of trained terrorists returning to our shores.

As the world witnessed over the past 6 months, however, al-Qaeda in the Islamic Maghreb (AQIM) has shifted the focus in Africa as the organization has made gains in Mali, Libya, and the rural areas of Algeria. But while the attacks in Benghazi and on the Algerian oil facility are of course tragic, in my view the major change to the region is not a massive increase in AQIM's attractiveness, but rather the huge shift that occurred with the virtual elimination of Libya's security services, the associated flood of weapons in the region, and the coup d'état in Mali.

AQIM has thus far proven a less tactically proficient and more regionally-focused criminal organization than other al-Qaeda affiliates. Although we cannot blindly hope this remains the case, we should also not read too much into recent events. Regional capacity-building, targeted offensive measures, and forceful engagement with governments like France, Algeria, and Libya that have a huge vested interest in the region should remain at the forefront of our strategy. And we must roundly condemn those who against every lesson of the past several years might be willing to pay ransoms to AQIM and its affiliates.

One notable area of concern that we must forcefully combat in the region—and one which the United States is uniquely able to address given our global footprint—is the cross-fertilization across the African continent that has recently accelerated. Coordination amongst al-Shabaab, AQIM, Boko Haram, and others is particularly problematic as it allows each organization to leverage the others' strengths. We must use our intelligence capabilities to define these networks and then assist in disrupting them. And our screening of travelers to the United States must recognize the dangers associated with these networks.

The most troubling of emerging fronts in my view is Syria, where Jabhat al-Nusra has emerged as the most radical of groups within the opposition. Given the enormous instability in Syria, which has to some degree already spread to Iraq and else-

where in the Levant, Jabhat al-Nusra has become a magnet for al-Qaeda-inspired fighters from around the globe. With little likelihood of rapid improvements in Syria, the al-Nusra front will almost certainly continue to arm, obtain real-world combat experience, and attract additional recruits—and potentially state assistance that is flowing to the FSA. Moreover, Jabhat al-Nusra's ideology not only contributes to the threat of terrorism, but more broadly it is contributing significantly to the regional Sunni-Shia tension that poses enormous risks. The rapid removal of Bashar al-Assad would not solve these problems, but an on-going civil war does in my view worsen the situation.

Without declaring victory, we should also have some optimism about al-Qaeda-inspired terrorism in Western Europe and especially the homeland. As recent studies have shown, there has been a continuing decline in numbers of significant homeland plots that have not been closely controlled by the FBI since 2009. In addition, the relative sophistication of homeland terrorists has not increased. Combined with successful counterterrorism efforts in Western Europe—most particularly huge strides in the United Kingdom—the picture faced today is far brighter than just 3 years ago.

Similar optimism cannot be applied to the threat posed by Lebanese Hezbollah, especially given its successful and foiled attacks over the past 2 years. Most notably, Hezbollah attack in Bulgaria killed six tourists and highlights the extent to which the group (and its patrons in Iran) continue to see themselves as being in an on-going unconventional war with Israel and the United States. Predicting Hezbollah and Iranian "redlines" is a notoriously challenging endeavor—as illustrated by the surprising 2011 plot to kill the Saudi Ambassador to the United States—but both organizations almost certainly would launch attacks at least outside the United States were there a strike on Iranian nuclear facilities.

There is little doubt that both Hezbollah and the IRGC Qods Force maintain a network of operatives that could be used for such strikes. In this regard the heavy Iranian presence in Latin America and Iranian cooperation with Venezuelan President Hugo Chávez is of particular concern. Although not every Hezbollah member and Iranian diplomat is a trained operative, a significant number could in the case of hostilities enable other operatives to launch attacks against Israeli or U.S. diplomatic facilities, Jewish cultural institutions, or high-profile individuals. In addition, and generally unlike al-Qaeda affiliates, the specter of Hezbollah or Iranian-sponsored cyber attacks is disturbingly real. Recent Distributed Denial-of-Service (DDOS) attacks on major U.S. financial institutions, as well as even more destructive Iranian-sponsored attacks on Saudi Aramco and Qatar-based RasGas, have highlighted the extent to which physical attacks might be combined with cyber attacks.

LOOKING AHEAD

This threat picture, although complex and dynamic, is in many ways more heartening than that which we faced from 2001 until at least 2010. Numerous organizations continue to threaten terrorist attacks, but as a very general matter the threats are away from the homeland and the scale of the attacks is markedly less than what we saw in September 2001 or even 2006, when al-Qaeda came dangerously close to attacking up to ten transatlantic airliners. It is not that events like Benghazi are not tragic. But threats to U.S. diplomatic facilities in Libya are of a radically different type than planes flying into civilian facilities in New York and Washington. In this regard, this is an appropriate juncture to look at a few of our biggest risks and challenges.

Terrorism Fatigue.—After 10-plus years of near-constant public discussion of terrorism—in our politics, the media, and through public messaging—many have simply had enough. This is not all bad as an unhealthy obsession with the threat of terrorism at the expense of countless other societal woes, such as cyber threats and drug violence on the Southwest Border, would in many ways hand our enemy a victory. On the other hand, there is real value in public discussion of terrorism: It can build resilience in the population and it can lead to the tackling of tough public policy questions like targeted killings and domestic intelligence. With terrorism fatigue we run a real risk of not addressing these issues in a way that provides a lasting counterterrorism framework. In this regard I actually see the current discussion around the use of drones as quite a heartening sign.

Terrorism fatigue poses at least two additional challenges. First, with all of our counterterrorism success such victories have become expected and any failure—no matter how small—can result in political finger-pointing and excoriation of our counterterrorism professionals. In effect we have become victims of our own success and unlike in 2001, perfection has become a political expectation. Although we

should continuously examine how we can improve our capabilities, we must guard against ex poste investigations that lack a serious appreciation for the ex ante difficulties of counterterrorism.

Second, terrorism fatigue can cause dangerous lethargy within the Executive branch on issues that do not appear to require immediate attention but which can do longer-term damage to counterterrorism efforts. I have repeatedly seen urgency morph into bureaucratic sluggishness as time passes since the last attack on issues like information sharing and interagency cooperation. Whether it is countering violent extremism programs or information access for the intelligence community, we must not take our foot off the gas pedal.

Weapons of Mass Destruction.—There is no doubt that smallish terrorist attacks or at least attempts will continue to occur at home and abroad. Such attacks can cause enormous pain and suffering to victims and their families, but they are clearly of a scale—at least with respect to absolute numbers killed—that is dwarfed by other societal ills such as routine criminal activity. The same cannot be said of terrorists' use of weapons of mass destruction—and more specifically biological weapons or an improvised nuclear device (IND).

Although we have also made progress in reducing the likelihood of terrorists obtaining WMD, for the foreseeable future we are faced with the possibility that a terrorist organization will successfully acquire these weapons. In this case, technology is not yet our friend as the ease with which these weapons can be obtained and hidden continues to exceed our ability to detect them.

Weapons of mass destruction pose a unique challenge as they are the prototypical low-likelihood, high-consequence event and thus determining the proper allocation of resources to combat them is particular contentious. That being said, we must continue to protect against the most dangerous of materials (e.g., HEU) being obtained by terrorists, secure weapons in the most dangerous places (e.g., Pakistan), and pursue research and development that will assist in detecting chemical and biological weapons in places where they would do the most harm.

Counterterrorism Partnerships.—Counterterrorism has always been and continues to be a "team sport." Although the United States can do much alone, we have always been incredibly reliant on a vast network of friendly nations that have extended massively our intelligence, law enforcement, military, and homeland security reach. Even before the Arab Awakening we witnessed some weakening of these partnerships. Whether it was fatigue on our partners' part, their own resource challenges, or differing views on the proper scope of counterterrorist efforts (e.g., fights over data sharing between the United States and the European Union), these partnerships have been under some pressure. Post-Arab Awakening we face an exponentially more daunting task, having lost some of our most valuable partners in the very places we need them most.

Again, part of the challenge is that we have been a victim of our own success. Al-Qaeda is simply not viewed as the same existential threat that it was in 2001. But without robust partnerships it will be increasingly difficult for us to detect and disrupt rising al-Qaeda (or other groups') cells, thus making it more likely that they will metastasize and embed themselves in ways that makes them more dangerous and more difficult to displace.

To maintain our partnerships we must carefully preserve funding for programs that provide critical capabilities—and potentially more important, a positive U.S. presence—for our allies. The increase in funding for special operations forces is a good step, but relatively tiny investments in Department of State and Justice programs can also deliver real results in this realm. In addition, we will have to approach new governments in the Middle East with sophistication and ensure they continue to view terrorism as a mutual threat.

Staying on the Offense—on all Fronts.—Over the past week an enormous amount has been said about targeted killings, especially of U.S. persons. In my view, having served under both Presidents George W. Bush and Obama, such targeted killings are a vital tool in the counterterrorism toolbox. And regrettably, in some cases that tool must also be used against U.S. persons like Anwar al-Awlaki who was a senior al-Qaeda operational commander who was continuing to plot attacks against the United States.

Perhaps unsurprisingly, I am supportive of the legal outline contained in the released Department of Justice white paper. From my perspective, the memorandum and administration practice (contrary to claims by some) appropriately constrains the President's authority, has provided extensive Congressional oversight and the opportunity to limit the program, and provides realistic standards given the inherent challenges of intelligence and counterterrorism. As I have previously implied, however, I am equally supportive of the current public debate on the issue. In fact, I believe bringing greater visibility to some programs could be useful not only to

build U.S. support, but also to build greater international understanding if not support—a key element in our ideological efforts.

As supportive as I am of targeted killings in appropriate circumstances, I am equally supportive of ensuring that these are not our only counterterrorism tools employed. I do believe that our reliance on kinetic strikes has in some cases allowed other efforts to atrophy or at least pale in comparison. This is enormously dangerous, as we cannot strike everywhere nor can we lethally target an ideology. As we increase targeted killings we must double-down on our soft power and ideological efforts—building capacity in civilian security forces, increasing the rule of law to diminish under-governed or ungoverned safe havens, and the like—lest we win a few battles and lose a global war.

Resources.—Finally, and not entirely inappropriately, counterterrorism resources at the Federal, State, and local levels will undoubtedly decline significantly in the coming years. It is difficult to estimate accurately how much has been spent on counterterrorism over the past 11 years, but the amount certainly comes close if not exceeds $100 billion a year. Some of this was undoubtedly well spent, but it is folly to think that inefficiencies and redundancies do not exist widely. In this sense, a bit of frugality is likely a very good thing.

The question, however, is whether we will be willing or able to make smart reductions to preserve critical capabilities. Our historic ability to direct funds where the threat is greatest—as opposed to where the political forces are strongest—have not been good. Perhaps the declining threat will mean that we can continue to spend imperfectly, but this is surely a dangerous bet to make.

We should use this imposed frugality to do serious mission-based—as opposed to Department- and agency-specific-based—budgeting in the Federal Government. This approach will require enormous changes within the Executive and Congressional branches, but looking across the counterterrorism budget, identifying the critical capabilities we must preserve, and then figuring out how that matches Department-specific budgets can be done. And if we are serious about maintaining these capabilities we have little choice.

CONCLUSION

More than a decade after 9/11, combatting terrorism isn't over. No one should be surprised by this fact. Nor should anyone be surprised that we are fighting in different places and, although some approaches are the same as they were in 2001, many of our tools must evolve with the evolving threat. Moreover, having the benefit of almost 12 years of National effort we are in a better place today to balance our counterterrorism efforts with other significant threats to our homeland, most notably state-sponsored cyber intrusions, theft, and attacks, and cross-border violence and instability due to counternarcotic efforts in Mexico. To the extent we have built up robust counterterrorist capabilities and we must maintain them, but we must also—to the extent possible—make sure these tools are applied effectively to other homeland security missions.

This committee has been central to much of what has been accomplished over the past 10 years. I very much hope—and expect—that it will be central to an inevitable transition, while never forgetting the tragedy that was the impetus for its creation. I hope that I have been helpful in giving a new perspective on these issues to help address these evolving challenges. Thank you for inviting me to testify, and for this committee's leadership on these critical issues.

Chairman MCCAUL. Thank you Mr. Leiter. We appreciate your testimony and certainly miss your briefings in a classified setting.

Now, Mr. Walker, you are recognized for 5 minutes.

STATEMENT OF DAVID M. WALKER, FOUNDER AND CEO, THE COMEBACK AMERICA INITIATIVE

Mr. WALKER. Chairman McCaul, Ranking Member Thompson, distinguished Members of the committee, thank you for the opportunity to testify.

The perspective I will bring is primarily more on management issues facing DHS. I have got over 40 years of leadership experience in all three sectors of the economy including 10 years as comptroller general of the United States and head of the GAO. In fact,

I testified on numerous occasions at the onset of creating the Department of Homeland Security.

First picking up on something the Chairman said earlier, from a macro perspective as has been stated by Admiral Mike Mullen, former chairman of the Joint Chiefs of Staff, myself, and others, the single greatest threat to our Nation's security is our own fiscal irresponsibility and mounting debt burdens.

Absent a change in course, our Nation's debt level will become unsustainable. This will threaten our future position in the world, our economy at home, our National security, our homeland security, and even our domestic tranquility over time.

While legislation in recent years including the Budget Control Act, the American Taxpayer Relief Act of 2012, was intended to help address this challenge. They have not addressed the three key drivers of our structural deficits; known demographic trends, rising health care costs, and an outdated and inadequate tax system.

As a result, we still face mounting deficit and debt burdens and the portion of the Federal budget that is on autopilot is scheduled to increase from the current 67 percent and go up.

Ladies and gentlemen, the Congress had control of 97 percent of the budget 100 years ago. Now it controls 33 and going down. That must change.

Therefore, a critical step to securing our Nation's future and our homeland is to reach a grand fiscal bargain that restores fiscal sanity, recaptures control of the budget, and ensures adequate financing for the departments and agencies that fall under the expressed and enumerated responsibilities as envisioned by our Nation's founders including homeland security.

Given the inevitability that the Federal Government will have to do more with less it is important more than ever that Federal agencies, including DHS, have a comprehensive and integrated strategic plan that is future-focused, results-oriented, resource-constrained, and that considers customers, employees, and other key stakeholders.

In my experience, there are three key elements that any organization must have to be successful. It has to have a plan, it has to have a reasonable budget, and it has to have outcome-based performance measures.

Unfortunately, over 200 years after our creation, the U.S. Government still doesn't have any one of these three. The DHS has done a better job, but there is still room for improvement.

From the DHS perspective, this past November marked the 10th anniversary of the formation. It is appropriate to look back. There are several areas I think that improvement is needed.

First, it must improve its strategic planning process. GAO and others have noted this need. DHS relies on partners to achieve a lot of its mission. There has to be a lot more consultation and coordination with those partners in order to achieve an effective plan and execution of that plan.

It needs to improve its financial management practices although it has made real progress, and in particular, it needs to improve its information technology and acquisition and contracting practices; some of the issues were mentioned previously and the waste that has occurred in that regard.

Third, there is a clear and compelling need to address human capital challenges at DHS. It is a major organization; the third-largest in Government. It is only as successful as its people and yet it has one of the lowest morales of any Federal agency with regard to its employees.

I would add two more items that aren't in my testimony but I think they are important. As I testified when I was comptroller general, there are certain large, complex, and high-risk agencies that should have a chief operating officer, a level two executive, which is a Presidential appointment, Senate confirmation, with statutory qualification requirements, with a 5- to 7-year tenure, and with a performance contract. We need that in large, high-risk agencies in order to deal with these challenges efficiently and effectively and in a timely manner.

Last, but not least, it is not in my testimony, but I will mention it; look, we are going to have serious budget constraints. We are going to have to do more with less. I think you have to also look at the possibility of user fees or other types of fees to be able to fund some of the costs of services associated with DHS that relate to individuals or goods, and I will leave that to your good judgment.

Last, but not least, there are a lot of things that need to be done in Government some of which have not been able to get done through the normal process. I would commend to your consideration of forming a Government transformation task force that would be able to make recommendations to the Congress that would be guaranteed hearings and guaranteed a vote focusing on economy, efficiency, effectiveness, and credibility to Federal Government.

I am happy to answer questions about this if you would like.

Thank you, Mr. Chairman, Ranking Member, happy to answer any questions.

[The prepared statement of Mr. Walker follows:]

PREPARED STATEMENT OF DAVID M. WALKER

FEBRUARY 13, 2013

Good morning Chairman McCaul, Ranking Member Thompson, and distinguished Members of the committee. I am honored to be here to offer my perspective on the current state of the Department of Homeland Security and how it can best achieve its important mission, that of helping to secure our country and its citizens.

The perspective I bring to this issue is based on my almost 40 years of experience across multiple sectors of the economy, spanning over 20 years of private sector experience, over 15 years of total Federal Government service, including almost 10 years as comptroller general of the United States and head of the U.S. Government Accountability Office (GAO), and almost 5 years in the non-profit sector. During my tenure as U.S. Comptroller General, I gained extensive knowledge of homeland security issues, and I testified before Congress on numerous occasions about this topic, including during the planning and formation of the Department of Homeland Security (DHS) in 2002. I am currently the founder and CEO of the Comeback America Initiative, which educates and engages the public about the threat posed by our Nation's structural deficits and mounting debt burdens, and possible ways to address them.

As has been stated by Admiral Mike Mullen, myself, and others, the single greatest threat to our Nation's security is our own fiscal irresponsibility and mounting debt burdens. Absent a change in course, our Nation's debt levels will become unsustainable. This will threaten our position in the world, economy at home, our National security, and even our domestic tranquility over time.

While legislation in recent years, including the Budget Control Act and the American Taxpayer Relief Act of 2012, was intended to help address our fiscal challenge, they have not addressed the three key drivers of our structural deficits: Known demographic trends, rising health care costs, and an outdated and inadequate tax system. As a result, the portion of the Federal budget that is on autopilot is set to increase from its current 67%, and the Nation's longer-term deficits will grow over time. According to last week's updated budget projections from the Congressional Budget Office, under current law, mandatory spending, including interest, will consume 76% of the Federal budget in 2023. Discretionary spending will be squeezed to roughly 24% of total spending, with non-defense discretionary spending being about 12% of total spending. As a percent of GDP, non-defense discretionary spending will decrease to 2.7%, well below the historical average of the past 40 years (4%). Therefore, a critical step to securing our Nation's future is to reach a "grand bargain" that restores fiscal sanity, recaptures control of the budget, and ensures adequate financing for the departments and agencies that fall under the express and enumerated Constitutional roles and responsibilities of the Federal Government, including homeland security.

Given the inevitability of our Federal Government having to do more with less, it is more important than ever for all Federal agencies, including DHS, to have a comprehensive and integrated strategic plan that is future-focused, results-oriented, resource-constrained, and that considers customers, employees, and other key stakeholders. In my experience, there are three key elements any organization must have to be successful: (1) It must have a plan; (2) it must have a budget; and (3) it must have outcome-based performance metrics. Unfortunately our Federal Government as a whole fails on all three of these. DHS has done a better job, but there is still plenty of room for improvement.

This past November marked the 10th anniversary of the formation of DHS, and the Department has made meaningful strides during that time to improve its performance, during some trying times, when it comes to homeland security threats. I recall during my testimony before Congress in 2002, when Congress was considering the creation of the Department, pointing out that a consolidation of 22 separate agencies was one of the biggest transformational changes the Federal Government had ever undertaken. In fact, at the time I stated that "the experiences of organizations that have undertaken transformational change efforts along the lines that will be necessary for the new department to be fully effective suggest that this process can take up to 5 to 10 years to provide meaningful and sustainable results". Now that 10 years have passed, it is appropriate to explore areas that DHS can focus on to more effectively achieve its critically important mission.

First, I believe DHS must improve its strategic planning processes. It is vitally important for any organization to have a strategic plan to guide its actions, allocate resources, and measure results. Unlike the Federal Government as a whole, DHS has made real progress in its Department-wide planning. However, GAO and others have recommended that DHS provide more opportunity for stakeholder participation in its planning process. Given DHS's reliance on partners to achieve its mission, in both the public and private sector, it is vitally important for those stakeholders to be meaningfully engaged in the planning process. In addition, DHS must do a better job of integrating risk management into its planning process, especially given the nature of its mission. Integrating risk management practices as a key element of its planning process is also critical to achieving sustainable success in an atmosphere of constrained resources. DHS planning must also involve the development of more outcome-based performance measures to guide allocation of limited resources.

Second, DHS must improve its financial management practices. While DHS has made progress in improving its financial management practices since its inception, a lot more work needs to be done. For example, failure to fully integrate its financial management system, and various internal control weaknesses, have resulted in DHS not being able to achieve an unqualified audit opinion on its financial statements since the Department's creation. DHS also has a number of material internal control weaknesses that need to be addressed.

In addition to integrating its financial management systems, DHS must make further strides in modernizing and integrating other management practices and systems. DHS faces serious challenges in integrating its IT, financial, human capital, and acquisition systems. These challenges have contributed to cost overruns, schedule delays, and an inability to achieve stated Departmental goals and objectives. Furthermore, with regard to acquisition management, DHS should implement more strategic and portfolio-based investment practices, and execute existing acquisition policy more effectively.

GAO has stated that "DHS culture has emphasized the need to rapidly execute missions more than sound acquisition management practices. Most major programs

lack reliable cost estimates, realistic schedules, and agreed-upon baseline objectives . . . " DHS must improve these practices if it is to effectively fulfill its mission.

Third, there are clear and compelling human capital challenges that DHS must address if it is to effectively achieve its mission in a sustainable manner. Any organization is only as successful as its people, and based on recent analysis employee morale at DHS is amongst the lowest at all Federal agencies. Furthermore, given the demographic trends facing Government at all levels, it is vitally important that DHS employ strategic workforce planning that focuses on acquiring, developing, and retaining a workforce capable of achieving its mission. This includes appropriate succession planning and recruiting practices.

The issues I have highlighted are areas where Congress can employ its oversight responsibilities to ensure DHS is best able to fulfill its mission in the future, especially in an era of serious fiscal challenges. However, I also encourage the Congress to consider creating a Government Transformation Task Force, similar to that being advocated by the Government Transformation Initiative (GTI), for which I serve as chairman of the board. Under GTI's proposed approach, an independent body, authorized by statute, would be created to recommend ways the Federal Government can operate more economically, efficiently, and effectively. The task force would be made up of non-conflicted leaders with proven track records of transforming organizations in the public, private, and/or non-profit sectors. It would issue reports and recommendations outlining ways to help Government focus on results, plan strategically, streamline operations, leverage technology, adopt best practices, and otherwise improve performance. Congress should be required to consider the task force recommendations in a timely fashion.

Our Nation's poor financial condition and mounting debt burdens require that Congress think outside the box and develop new ways to make Government more future-focused and results-oriented. The creation of such a task force could help restructure our Government to meet the needs of the 21st Century, while achieving efficiencies that allow it to live within the resource-constrained reality that our current fiscal path will require.

When testifying before the creation of DHS I said that, "Strong and visionary leadership will be vital to creating a unified, focused organization, as opposed to a group of separate units under a single roof." DHS has made real progress in this regard, but more action is required. At the same time, greater vision and leadership is required to help ensure that the Federal Government as a whole can effectively address the many sustainability challenges that we face. This is essential if we want to effectively discharge our stewardship obligation to our children, grandchildren, and future generations of Americans.

I thank you again for the opportunity to testify before your distinguished committee, and I would be happy to answer any questions you may have.

Chairman MCCAUL. Thank you Mr. Walker, and as I mentioned in my opening statement, management reform and applying more of a business model to the Department to identify waste and inefficiencies will also be a top priority, and I appreciate your testimony.

Mr. Ervin, you are now recognized.

STATEMENT OF CLARK KENT ERVIN, PARTNER, PATTON BOGGS, LLP

Mr. ERVIN. Thank you very much, Mr. Chairman.

Chairman McCaul, Ranking Member Thompson, Chairman King, and Members, thank you very much for this opportunity to testify today.

Let me start by joining my colleagues, Mr. Chairman, in congratulating you on your ascension to the Chairmanship. It is not every day that one gets to testify before a dear, personal friend, and a former colleague.

I have worked very closely with both Ranking Member Thompson and you, Chairman King, over the years and look forward to continuing to do so.

It seems not so long ago that the Nation was beginning to turn its attention away from the threat of terrorism. With the end of the

war in Iraq, the beginning of the end of the war in Afghanistan, the killing of Osama bin Laden and that of his would-be rival for that dubious title, public enemy No. 1, Anwar al-Awlaki, as well as the devastatingly successful drone campaign against various and sundry al-Qaeda lieutenants and foot soldiers in Pakistan, Yemen, and Somalia, the absence, thankfully, of successful terror attacks, and the absence for some time of even significant aborted terror plots, even some sophisticated analysts and observers had come to think that terrorism had returned to the status of a second-order concern for policymakers and war fighters.

If anything good has come out of the crises in Mali, Benghazi, and Syria and out of the renewed and intensified controversy, occasioned by a recent movie and recent confirmation hearings over drone strikes and enhanced interrogation techniques, it is the understanding of the sobering fact that, our signal victories and wholly understandable war-weariness notwithstanding, terrorists of one stripe or another continue to pose a grave threat to the world in general and to our homeland in particular.

If anything, the terror threat today is more complicated than it was a decade ago because, as Mr. Leiter noted, the threat is more diffuse, with "al-Qaeda Core" having metastasized, cancer-like, into various virulent regional cells throughout most of the world.

We face today's terrorism threat in a severely constrained fiscal environment, with huge defense cuts looming like a proverbial Sword of Damocles, limiting policymakers' and war fighters' options to a degree unprecedented in recent history.

For all these reasons, in this tenth anniversary year of DHS, I would argue for placing "security" back at the front and center of "Department of Homeland Security."

By that I mean that the rightful acknowledgement that the Department has multiple important missions to carry out: Preparing for and responding to natural disasters; dealing with the issue of immigration; patrolling our coast line, et cetera, to name just a few. Its chief role is to do its part to detect, deter, and defend the Nation from terror attacks.

Now I would be remiss if I did not acknowledge the progress that DHS, working with its partners at the Federal, State, and local governmental level, the private sector, and the American people, has made, through two administrations now; one Republican, in which I served, and one Democratic, in helping to secure the Nation.

Our aviation sector in particular, on which terrorists understandably, remain fixated, is far more secure than it was on September 10, 2011. But, I remain concerned about various aspects of even our aviation system even, like, for example, the continued vulnerability of air cargo on passenger planes, and our use of devices at airport passenger checkpoints that are really anomaly detectors, as opposed to what we really need, namely, explosives detectors.

I worry, too, about our relative lack of focus over the years on securing our mass transit sector. The successful attacks over the years in London, Madrid, and Moscow, and the aborted terror plots in New York City all show that mass transit is also in terrorists' cross hairs, and sooner or later, they will attempt to strike here again, and if we are not careful, one day they will succeed.

I worry also about our maritime sectors, specifically, the smuggling of radioactive material in containers and hope that we will redouble our efforts to try to find a way to scan not just cargo about which we have suspicions, but all cargo if possible in an effective, efficient, and economical manner, without bringing global commerce to a halt.

Call me a worry wart, but I don't trust terrorists to complete a shipping manifest accurately or to do business only with unknown shippers, and so a risk-based automated target system largely based on such trust gives me pause. As President Reagan would say, "Trust, but verify."

Finally, cyber-threats. I look forward to learning more about the President's Executive Order later today, but we all I think would agree that it is no substitute for legislation and hope very much that the administration and the Congress will work together in a bipartisan way to enact a law this year that will further secure our Nation against this potentially catastrophic threat.

Finally, the success of the Department on all of these fronts will require adroit leadership on the part of Secretary Napolitano, working with the Congress in general, and with this committee and your Senate counterpart in particular.

Given the grave threats and our severe fiscal constraints, there is no time to waste and not a single dollar to waste. I would applaud Secretary Napolitano for taking steps like pulling the plug on costly and inefficient and ineffective procurements like SBInet and DNDO's ASP program, and I also hope that this year that using the fiscal crisis in which we are in, we can ensure that going forward we direct counterterrorism grants only to those localities most at risk of terror attack.

With that, Mr. Chairman, again, thank you very much for having me here today to testify and like others, I look forward very much to your questions.

[The prepared statement of Mr. Ervin follows:]

PREPARED STATEMENT OF CLARK KENT ERVIN

FEBRUARY 13, 2013

Chairman McCaul, Ranking Member Thompson, and Members, thank you very much for inviting me to testify before you today at this important hearing. It is a great joy for me to testify before you, Mr. Chairman, recalling as I do with delight our years together as fellow deputy attorneys general to then-Texas Attorney John Cornyn. It is not every day that one gets to testify before a Chairman who happens to be a dear personal friend dating back many years. Congratulations on your ascension to the Chairmanship, and I look forward to working with you going forward. And, of course, though we were not colleagues likewise in a prior life, I count you, too, as a friend, Ranking Member Thompson, and am delighted to be working with you again in your key role on this key committee.

It seems not so long ago that the Nation was beginning to turn its attention away from the threat of terrorism. With the end of the war in Iraq; the beginning of the end of the war in Afghanistan; the killing of Public Enemy No. 1, Osama bin Laden, and that of his would-be rival for that dubious title, Anwar al-Awlaki, as well as the devastatingly successful drone campaign against various and sundry al-Qaeda lieutenants and foot soldiers in Pakistan, Yemen, and Somalia; the absence, thankfully, of successful terror attacks, and the absence for some time of even significant aborted terror plots, even some sophisticated analysts and observers had come to think that terrorism had returned to the status of a second-order concern for policymakers and war fighters.

If anything good has come out of the crises in Mali, Benghazi, and Syria, and out of the renewed and intensified controversy, occasioned by a recent movie and recent

confirmation hearings, over drone strikes and enhanced interrogation techniques, it is the underscoring of the sobering fact that, our signal victories and wholly understandable war weariness notwithstanding, terrorists of one stripe or another continue to pose a grave threat to the world in general and to our homeland in particular. And, if anything, the terror threat today is more complicated than it was a decade ago because the threat is more diffuse, with "al-Qaeda Core" having metastasized, cancer-like, into various virulent regional cells throughout most of the world. And, we face today's terrorism threat in a severely constrained fiscal environment, with huge defense cuts looming like a proverbial Sword of Damocles, limiting policymakers' and war fighters' options to a degree unprecedented in recent history.

For all these reasons, in this tenth anniversary year of DHS, I would argue for placing "security" back at the front and center of "Department of Homeland Security." By that I mean that the rightful acknowledgement that the Department has multiple important missions to carry out—preparing for and responding to natural disasters; extending the benefits of and enforcing the penalties in our existing immigration laws and working with the rest of the administration and Congress to reform our immigration system; patrolling our coastline and rescuing mariners in distress; and protecting the President and other senior administration officials and visiting foreign diplomats, to name a few—its chief role is to do its part to detect, deter, and defend the Nation from terror attacks.

I would be remiss if I did not acknowledge the huge progress that DHS, working with its partners in Federal, State, and local governments, the private sector, and among the American people, has made, through two administrations now, one Republican and one Democratic, in helping to secure the Nation. Our aviation sector in particular, on which terrorists, understandably, remain fixated, is far more secure than it was on September 10, 2011.

But, I remain concerned about certain aspects of even our aviation system, like, for example, the continued vulnerability of air cargo on passenger planes, and our use of devices at airport passenger checkpoints that are, really, anomaly detectors, as opposed to what we really need, namely, explosives detectors.

I worry, too, about our relative lack of focus over the years on securing our mass transit sector. The threat to mass transit is not merely theoretical. The successful attacks in London, Madrid, and Moscow, and the aborted plots against mass transit in New York City, all show that mass transit is also in terrorists' crosshairs, and sooner or later, they will attempt to strike here again. If we are not careful, one day they will succeed.

I worry also about our maritime sector, specifically, the smuggling of radioactive material in containers, and hope that we will redouble our efforts to try to find a way to scan not just cargo about which we have suspicions, but all cargo in an effective, efficient, and economical manner, without bringing global commerce to a halt. Call me a "worry wart," but I don't trust terrorists to complete a shipping manifest accurately or to do business with only "unknown shippers," and so a "risk-based" automated target system largely based on such trust gives me pause. As President Reagan would say, "Trust, but verify."

And, finally, cyber-threats. Every passing day shows that cyber-crime and cyber-terrorism are clear and present dangers to our Nation. We will either do everything in our power to prevent a devastating cyber-attack on our Nation now, or sit here (if we are lucky enough still to be around) 5 years from now, or 10 years from now, or 20, and lament the fact that we did not. It is imperative that both the administration and Congress put partisanship and ideology aside to devise and enact, this year, a law to make our Nation more secure from this potentially cataclysmic threat.

To conclude, making progress on all these fronts will require adroit leadership on the part of Secretary Napolitano and her leadership team, working in concert with the Congress, with your committee and your Senate counterpart in particular. Given the grave threats, and our severe fiscal constraints, there is no time to waste, and not a single dollar to waste. I would applaud her for to taking steps like pulling the plug on costly and ineffective procurements like SBInet and DNDO's ASP program, and, I hope that this year, and in the many lean years likely still to be ahead, that she will have Congressional support for directing counterterrorism grants to only those localities most at risk of terror attacks.

Again, Mr. Chairman, Mr. Ranking Member, and Members, thank you for inviting me to appear before you today and I look forward to responding to your questions.

Chairman MCCAUL. Thank you, Mr. Ervin. Your comments on the necessity for cyber legislation is a good segue into my 5 minutes of questions. I recognize myself for 5 minutes.

Mr. Henry, as I mentioned my trip to the NSA yesterday, my briefings with General Alexander highlight the sobering reality that we are under attack as a Nation and our interests are under attack overseas.

The enormous amount of intellectual property stolen as you mentioned, the espionage, and the cyber warfare primarily, China, Russia, Iran, and Iran's latest attacks on Aramco in the Saudi peninsula and our own financial institutions, which is probably occurring, as I speak cause me great harm.

I think we need to move quickly on this so I wanted to ask you real quickly, what is your assessment on the role of DHS? In addition, if you have had a chance to read the draft Executive Order, what is your assessment of that as well?

Mr. HENRY. Thank you, Chairman.

As far as DHS, I think that one of the critical areas in everything that we do as it relates to cyber is the collection and dissemination of intelligence.

As I mentioned in my statement, we have been focusing on reducing the vulnerabilities for so long, but it is really critical for us to identify who the adversaries are and to take steps as a Nation to thwart their efforts and to mitigate that threat.

I think as it relates to intelligence sharing, DHS has a role in collecting perhaps or deconflicting across multiple agencies—the FBI, NSA, DOD, and others—who collect intelligence related to the threat and how do we take that very critical information and intelligence and synthesize it so that it can be shared effectively in a manner that best helps the private sector prepare to defend their networks and also to help take the intelligence that is collected off of the network every single day by the private sector and to get that into the hands of the right people who can take actions to thwart the threat; to help do the attribution to identify there is a particular nation and we know this particular nation is taking this action against U.S. interests.

It is impacting our economic and National security, and as a Government there are steps that we can take whether they be economic, some type of trade sanctions, law enforcement actions, some intelligence community actions. There are steps that we can take but it can only happen if that intelligence is synthesized and shared both ways. I think that DHS can play a role in the critical area.

Chairman MCCAUL. On the Executive Order?

Mr. HENRY. So the Executive Order I just had a moment to look at it this morning. I think it talks about that. It talks about how intelligence is shared, information is shared between the private sector and the U.S. Government. So I think elaborating on that, the devil's in the details of course how we actually build that out.

I also agree with the statement that somebody made about the comprehensive whole-of-Government response here, and I think the Executive Order also talks about that. It has to be a comprehensive plan and it has to work across all sectors. There is not an agency or an organization that this doesn't touch and everybody has got to have a piece of that response.

Chairman MCCAUL. I agree with that. Moving on to the border, I just visited the L.A. port. There is a threat to our West Coast

with these boats coming up from South America. There is a threat to the Caribbean, the Southwest Border we focus quite a bit on, and of course the Northern Border as well.

The Southwest Border particularly, Admiral Allen, we are going to come up with a bill, an authorization bill. What would you recommend that we focus on for a comprehensive strategy?

Admiral ALLEN. Mr. Chairman, I think it is important to take a risk-based approach. Given the resource constraints we are dealing with, the budget environment, and the physical realities of the border, and I mentioned some of them earlier. I think we need to understand the risk that is presented by the border. We don't want to drive that risk to zero because we will shut down trade.

In my view, the best thing we can do is increase situational awareness. In the maritime environment, that would be maritime building awareness, our ability to understand what is out there through a combination of information sharing, sensor information, and a collection of information on the movement of vessels that is available through positioning systems that are there right now.

That needs to be centrally known, shared, and coordinated with the various databases that are resident in the other components to create a comprehensive common operating picture and a common intelligence picture that allows us to queue our resources.

Specifically in relation to the Southwest Border maritime environment that you are talking about, there is extraordinary cooperation between the CBP and the Coast Guard there an actually with the Navy fleet commander down there that makes resources available.

What we need to do is refine our ability to understand what is happening in the maritime environment, to be able to identify legitimate flows from illegitimate flows, and be able to focus those resources.

That needs to be done in my view by coordinating and consolidating command centers where we can, information, sharing where we can, and then queuing those resources in a collective manner.

Chairman MCCAUL. I think the technology piece is a piece that has not been finalized down there, and I think that is where we are going to be focusing quite a bit on getting technology down there to better secure it.

Last, and it has to be very quickly, Mr. Walker, what was it—you had mentioned a management restructuring and some specific positions that you would recommend. Can you——

Mr. WALKER. One, Government is a large, complex, and very expensive enterprise and as it has been mentioned, we have limited resources. We need to allocate those based upon risk.

My view is when you look at the Department of Homeland Security, which is a combination, an amalgamation of many other departments and agencies in the past, there is a need for a chief operating officer; a level two official that would be responsible for the management process that would be based upon statutory qualification requirements, would have a term appointment, and a performance contract.

We look to other countries, we see that this exists. I mean, you know, the United States is not an island. We need to learn from history. We need to learn from others, and I think it is a concept

that makes sense in certain agencies such as DHS and DOD, for example.

Last thing is there is a lot of great recommendations that are made by the GAL, by inspectors general, by, you know, even good work that is done by these committees as well as OMB, but a lot of these recommendations never get implemented. You know, whether it is duplicated programs, whether it is best practices problems, you know, crossing many different functions in Government.

I think there is a need for a capable, credible, and non-conflicted statutory group that would end up being able to look at a number of areas, make recommendations to the Congress with guaranteed hearings and a guaranteed vote building off of like a Hoover Commission approach if you will because the simple fact of the matter is whether it is Simpson Bowles, and Domenici to Weber, or anything else, they are dealing with the big-ticket items.

On the other hand, there are billions and billions and billions of dollars the grow every year that we are not coming to grips with that, that we are gonna have an extraordinary mechanism to deal with that are not being dealt with.

Chairman MCCAUL. I think that the outside reading group really kind of encapsulates the DHS Accountability Act that was introduced last Congress, passed the House, unfortunately not the Senate. I hope I can, in working with the Ranking Member, we can reintroduce that legislation.

With that, I now recognize the Ranking Member.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I would like to enter into the record a letter from Secretary Napolitano kind of highlighting concerns around sequestration and what that would possibly do to adversely impact——

Chairman MCCAUL. Without objection, that is so ordered.

[The information follows:]

LETTER FROM HON. JANET NAPOLITANO TO RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 13, 2013.

The Honorable BENNIE G. THOMPSON,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR REPRESENTATIVE THOMPSON: Thank you for your letter regarding the potential impacts of the March 1st sequestration. The Department of Homeland Security (DHS) shares your deep concerns about the effects this unprecedented budget reduction to Fiscal Year (FY) 2013 funding will have on DHS, its missions, and our Nation's security and economy.

Reductions mandated by sequestration would undermine the significant progress the Department has made over the past 10 years and would negatively affect our ability to carry out our vital missions. Sequestration would roll back border security, increase wait times at our Nation's land ports of entry and airports, affect aviation and maritime safety and security, leave critical infrastructure vulnerable to attacks, hamper disaster response time and our Surge Force capabilities, and significantly scale back cybersecurity infrastructure protections that have been developed in recent years. In addition, sequestration would necessitate furloughs of up to 14 days for a significant portion of our front-line law enforcement personnel, and could potentially result in reductions in force at the Department. The following provides specific examples of the potential impacts of Sequestration on the Department:

- U.S. Customs and Border Protection (CBP) would not be able to maintain current staffing levels of Border Patrol Agents and CBP Officers as mandated by Congress. Funding and staffing reductions will increase wait times at airports, affect security between land ports of entry, affect CBP's ability to collect rev-

enue owed to the Federal Government, and slow screening and entry programs for those traveling into the United States.

- U.S. Immigration and Customs Enforcement (ICE) would not be able to sustain current detention and removal operations or maintain the 34,000 detention beds mandated by Congress. This would significantly roll back progress that resulted in record-high removals of illegal criminal aliens this past year, and would reduce ICE Homeland Security Investigations' activities, including human smuggling, counter-proliferation, and commercial trade fraud investigations.
- The Transportation Security Administration would reduce its front-line workforce, which would substantially increase passenger wait times at airport security checkpoints.
- The U.S. Coast Guard (USCG) would have to curtail air and surface operations by nearly 25 percent, adversely affecting maritime safety and security across nearly all missions areas. A reduction of this magnitude will substantially reduce drug interdiction, migrant interdiction, fisheries law enforcement, aids to navigation, and other law enforcement operations as well as the safe flow of commerce along U.S. waterways.
- Furloughs and reductions in overtime would adversely affect the availability of the U.S. Secret Service workforce, and hinder on-going criminal investigations.
- Reductions in funding for operations, maintenance, and analytical contracts supporting the National Cybersecurity Protection System (NCPS) would impact our ability to detect and analyze emerging cyber threats and protect civilian Federal computer networks.
- The Federal Emergency Management Agency's Disaster Relief Fund would be reduced by over a billion dollars, with an impact on survivors recovering from future severe weather events, and affecting the economic recoveries of local economies in those regions. State and local homeland security grants funding would also be reduced, potentially leading to layoffs of emergency personnel and first responders.
- The Science and Technology Directorate would have to stop on-going research and development including: Countermeasures for bio-threats, improvements to aviation security and cybersecurity technologies, and projects that support first responders.
- The Department would be unable to move forward with necessary management integration efforts such as modernizing critical financial systems. This would hinder the Department's ability to provide accurate and timely financial reporting, facilitate clean audit opinions, address systems security issues, and remediate financial control and financial system weaknesses.

Hurricane Sandy, recent threats surrounding aviation and the continued threat of homegrown terrorism demonstrate how we must remain vigilant and prepared. Threats from terrorism and response-and-recovery efforts associated with natural disasters will not diminish because of budget cuts to DHS. Even in this current fiscal climate, we do not have the luxury of making significant reductions to our capabilities without placing our Nation at risk. Rather, we must continue to prepare for, respond to, and recover from evolving threats and disasters—and we require sufficient resources to sustain and adapt our capabilities accordingly. We simply cannot absorb the additional reduction posed by Sequestration without significantly negatively affecting front-line operations and our Nation's previous investments in the homeland security enterprise.

The Department appreciates the strong support it has received from Congress over the past 10 years. As we approach March 1, Congress is urged to act to prevent Sequestration and ensure that DHS can continue to meet evolving threats and maintain the security of our Nation and citizens. Should you have any questions or concerns at any time, please do not hesitate to contact me[.]

Yours very truly,

JANET NAPOLITANO.

Mr. THOMPSON. Thank you.

Mr. Ervin, let us look at TSA as a point of conversation. Most of us here go through airports every week. The assumption is that the screening technology that we all go through is good.

What has been your concern about TSA's approach to technology and whether we are really identifying all the vulnerabilities or are we just—just tell me what your concerns are.

Mr. ERVIN. Right. Well, thank you for that Mr. Thompson. I guess I would say several things. First of all, as I mention just

briefly in my testimony, it seems to me that the chief problem with the current technology that we deploy at checkpoints, advanced imaging technology, to use the technical term, which encompasses millimeter wave machines and also backscatter machines, and it is the backscatter machines that the Chairman talked about in his opening statement that we are not able to meet the privacy concerns and as a result have been pulled back.

Both of them—while one could argue that one is more effective than the other—both of them are anomaly detectors as opposed to explosives detectors.

By that I mean that all those machines do is show that there is something on the person of the passenger that is out of the ordinary and it is therefore incumbent upon the screener observing that image to determine that there is in fact anomaly and then to inquire further as to whether that anomaly isn't in fact an explosive and therefore should be of concern.

Instead, as I say, I think what we need to do is to skip a step, take out a step, and instead to deploy machines that are automated explosive detectors, which is to say immediately without any human intervention determine that there is in fact or is not which of course is usually the case an explosive and I think that would be a huge advantage.

There are certain companies that have such technology. That technology is being tested by TSA to be fair, but I think we need to redouble our efforts to deploy it. I guess——

Mr. THOMPSON. My point, to support what the Chairman has said, one of the things we will look at is how we do procurement and contracting with the Department. We know all of these vulnerabilities are out there, but we can't get the through-put to the point of reality.

So, Mr. Chairman, I look forward to—as we go forward.

Admiral Allen, Congress passed some legislation long time ago saying that we should screen in-bound cargo coming in to this country from foreign areas, and we are woefully beyond the point of the Congressional mandate.

Do you see that also as a vulnerability from a security standpoint to this country not knowing what is coming in the containers to this country?

Admiral ALLEN. Mr. Thompson, there is always going to be a risk in any cargo entering the country and any inspection regime associated with that.

As I stated earlier, we need to understand the risk that is inherent in these flows in trades and then try and attack it where we best get the return on our resources.

I know that 100 percent container inspection has been discussed for many, many years. I myself think that that is a little bit of a bridge too far in terms of resources and the technology available to accomplish that and make that actually an effective way to secure cargo.

I think we need to look at emerging technologies. Some of the other Members here have alluded to different types of sensing equipment that could actually interrogate these containers while they were being moved themselves.

I think in the long run, it has to do with evaluating data intelligence and sharing information is the way to go. I know there is a desire to see 100 percent screening of containers. I don't think it is realistically achievable in the near-term, sir.

Mr. THOMPSON. What is realistic in your opinion?

Admiral ALLEN. Well, considering the technology challenges and the costs associated with it, sir, I think that it would be very, very difficult to achieve that goal in the current budget environment and current technology environment.

Mr. THOMPSON. Good answer.

Mr. Walker, you talked about creating a commission or a individual who has some responsibility for certain challenges within DHS. Can you go a little farther in how you see that——

Mr. WALKER. Sure.

Mr. THOMPSON [continuing]. Individual operating?

Mr. WALKER. Sure. There is two issues. One is a micro-issue for the Department of Homeland Security and the other is a macro-issue that deals with the Government at large.

The Department of Homeland Security is the third-largest Federal agency. It is accumulation, amalgamation of a bunch of different, you know, previous organizations. It has got a very important mission. It has got very limited resources, and it has got a number of fundamental management challenges that exist and will continue to exist.

We need to have somebody focused full-time on management transformation and execution; economy, efficiency, effectiveness, credibility.

We need to focus, have somebody focus full-time on the issue of risk assessment. There is no such thing as zero risk. You have to be able to allocate limited resources to mitigate as much risk as possible.

In my view, while deputy secretaries typically try to do some of this job and to differing degrees of success and this has nothing to do about the current incumbent or prior individuals that were there, it is just a big darn job and that we need to recognize that we need to have people in those jobs that have appropriate qualification requirements who will be there for enough time to be able to get things done.

That is why say 5- to 7-year term with a performance contract focused on results so that we are in effect professionalizing part of the management and execution of Government. I think——

Mr. THOMPSON. If the Chairman will indulge me, are you saying that individual will also have the authority to fix whatever they encounter?

Mr. WALKER. Well, there is two things. One of which is they will identify to the extent that they have the authority under current law then they would fix it.

The second is the macro issue I am talking about. If you look at duplicate programs, if you look at problems with procurement, human capital, whatever, there are a number of things that exist throughout Government and that have not been effectively addressed for a variety of reasons in the normal course.

I believe there is a need to create some type of a statutory task force where the Congress would buy in and the President would

buy in that would be comprised of individuals who are capable, credible, with proven transformational change experience in the private sector, public sector, and/or not-for-profit who don't have conflicts, who would oversee a process to review different functions or programs that would make recommendations focused on economy, efficiency, effectiveness, and credibility that would be guaranteed hearings and guaranteed a vote.

If you look at, you know, whether it is the Grace Commission or the good work that Vice President Gore did, you know, on reinventing Government, there is a lot of things that come out that frankly never get acted on and I think we have to recognize that given our current and projected financial condition and the fact that the agencies that are discretionary spending including this Department that is envisioned by the Constitution, but nonetheless is getting squeezed—not—didn't say homeland security but domestic tranquility and I would argue that this is part of domestic tranquility, then, you know, we have got to figure out a new way to try to be able to address these long-standing problems to free up more resources to mitigate the risk and to execute on mission.

Mr. THOMPSON. Thank you very much.

I appreciate the Chairman's indulgence.

Chairman MCCAUL. I thank the Ranking Member. I plan to recognize Members who are in accordance with the committee rules, those who were present at the start of the hearing, by seniority, and those coming in after the hearing will be recognized in the order of arrival.

With that, Chairman King is now recognized.

Mr. KING. Thank you, Mr. Chairman.

Let me thank all of the witnesses for their Government service over the years. It is greatly appreciated.

Director Leiter, let me just focus on a few things in your statement. You mentioned the concern about terrorism fatigue both in the Government and among the general public.

You also referenced the concern about improvised nuclear devices. I know in New York we are very concerned about dirty bombs, the impact that would have whether it was in lower Manhattan, Wall Street, Times Square area. Both, you know, the loss of human life, which would be significant enough, but also the economic impact it would have on the country perhaps costing billions of dollars in the economy making it uninhabitable for 6 to 8 months.

In response to that, we set up the Secure the Cities Program, which was intended to be not just for the New York area and this includes Long Island, Connecticut, and New Jersey, but also to serve as a template for the country for other urban areas around the country.

When you were with MCTC, did you have an opportunity to observe Secure the Cities or discuss with Commissioner Kelly all?

Mr. LEITER. I did not, Congressman, but I spent an extensive amount of time with the NYPD counterterrorism officials throughout the region in New York, New Jersey, and Connecticut.

In my regard, I think this is a very good program. I would associate myself with previous comments that a risk-based approach on these topics is absolutely critical.

If we simply slice the salami and try to get all of the funding everywhere in the country to defend against low-likelihood but high-consequence events like an improvised nuclear device, we will not cover the places that are most likely to be hit and we have to take some risk there.

Certainly major metropolitan areas, New York, Chicago, Los Angeles—this is not to say that other parts of the country are not important—but we have to prioritize because if we try to spend the money everywhere, we either will run out of money or we won't be able to protect anything effectively.

Mr. KING. Thank you.

Mr. Ervin, if anyone was literally present at the creation of the Department it has been you, and you have been involved in many capacities ever since the Department was created, both as a Government official and as a private citizen.

As Director Leiter said, you mention the importance of risk-based funding in your statement. You also pointed to mass transit and that has been—again it is perhaps a parochial concern of mine since we have 5 million passengers every day whether it is the subway system, Long Island Railroad, Path subways. We have had six attempted plots against the mass transit system in New York.

What though would you suggest that we do since to me it is much easier to secure an airport, much easier to make airliners secure. I think in New York we have over 1,000 entrances and exits just on the subway system. How you can possibly secure that? Is it technology? Is it personnel? Is it intelligence gathering?

Mr. ERVIN. Well, thank you for that, Mr. Chairman. I am glad you underscored that because as I said in my statement, just briefly, I really worry about that and think that we have, relatively speaking, underprepared for it.

I think you put your finger on it. We certainly cannot secure the mass transit sector in the same way or attempt to secure it in the same way that we secure the aviation sector for all of the reasons you cite.

I think what we need to do going forward is what New York City does very well, but I think we need to see that model replicated in other cities around the country that don't have the same degree of threat that New York has.

I think New York is unique in that regard, but are likewise in terrorist crosshairs—Washington, DC; Los Angeles; Chicago; and by that I mean, it is what you said. It is a combination of personnel and technology.

The good news is, after every scare, mass transit scare, in around the world and in this country we see—not just in New York City but in the cities that I mentioned—an increased police presence, the greater deployment of technology, but what tends to happen is that that is just time-limited.

When the issue fades from the headlines, those resources are taken away and that is understandable to some degree given the budget constraint we are in and the fact that to a very large degree, mass transit, unlike aviation security, is financed at the State and local level.

Given our fiscal environment and given this threat, I think we need to redirect our resources so that a greater percentage of TSA's

budget in particular and the overall DHS budget is directed to mass transit sector given, as I say, the threat that the mass transit sector poses to our country.

Mr. KING. I would suggest also, and the question, of course, though, that we factor in—I think you agree with this—the financial impact a successful attack on any of our urban centers would have, whether it is in New York, Los Angeles, Chicago, Boston, Philadelphia—go down the line, and that would impact billions and billions of dollars.

Mr. ERVIN. No question about it, sir. You know, mass transit is called mass for reason. There are huge numbers of people, as you note, who are affected by mass transit, and we know that terrorists' intention is to maximize the number of people killed and maximize the number of people injured, to maximize the psychic impact of it, and to maximize the economic impact.

We certainly saw that in 9/11 with regard to the aviation sector. We would see that with regard to the mass transit sector if God forbid there were successful attacks.

Mr. KING. Thank you, Mr. Ervin.

My final statement will be to Mr. Leiter. You testified before our committee in January 2011, and you said that al-Awlaki was the most dangerous person in the world followed by bin Laden.

Within 8 months, they were both gone. Anybody else you want to mention today?

[Laughter.]

Mr. LEITER. Mr. Chairman, Mr. King, that is a dangerous question and my answer is even more dangerous, but what I would say is it shows that focused or prioritizing where our most deadly enemies are and doing so with greater transparency, so our elected officials have an opportunity to weigh-in with the Executive branch and make their views known about whether or not someone should or should not be legitimately targeted, is an important role for this committee, the intelligence committee, the armed services committee.

In my view, the fact that someone is an American citizen, although tragic and a weighty decision for the President, clearly cannot immunize that person from being stopped from launching attacks, and sometimes we have to do that using deadly force.

Mr. KING. Thank you, Mr. Leiter.

Thank you, Mr. Chairman.

Chairman MCCAUL. The Chairman now recognizes the gentleman from Massachusetts, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman.

I am gonna just drill down on one issue that I brought up in the past but still remains a problem. Since 2001, there's been over 1,300 perimeter security breaches at airports.

So even though we have an easier job at airports, I don't think that job is being done frankly, and as history has shown us, one unsafe airport compromises every airport in the entire country.

In October 2011, I introduced an amendment in the authorization bill for this committee that seeks to protect U.S. travelers and threats resulting from airport perimeter breaches by asking TSA to map out a plan to conduct security vulnerability assessments at

airports throughout the United States—not just the 17 percent that they had checked at that point of the airports.

So going forward, what is the best way to address perimeter security at the airports? We have that the public going through gates and radiation and screening and doing all kinds of things as they approach the gate yet we are wide-open in my opinion; pretty darn close to wide-open around our perimeters.

Could any of you comment on that? Because I continually see no action going forward with the Department in this respect.

Mr. ERVIN. Can I say a word about that, Mr. King? I am really glad you raised it. Perimeter security at airports is an issue that is not often talked about, but like you I worry about that as a vulnerability. I guess I would say a couple of things.

One is I would commend to you and I am sure you are aware of it and others, the work that Los Angeles has done in this regard. There is a forward appointment of police officers, which can serve as a deterrent effect—obviously nothing is perfect—but can serve as a deterrent effect.

There are random searches of cars before they approach the airport. I think we need to see the wider deployment of this in airports around the country.

We all should recall the incident in Edinborough I believe back in 2010 or something like that where an airport was breached and there were—I believe there—certainly there were injuries, I think there were deaths as well, within the pre-checkpoint area of the airport.

There is no screening whatsoever that happens and so in the same way, and Admiral Allen can talk about this, in the same way that we successfully since 9/11 have pushed the borders out as far as border security is concerned, likewise, I think we need to push airport security out past the checkpoint and long before a passenger approaches the airport.

Mr. KEATING. Yes, I am reminded when I was the district attorney there was a case just before I entered Congress where a 16-year-old boy just pierced through all the security that is there or wasn't there. He stowed away on a commercial airline and tragically ended up being killed as the airplane elevated and his body dropped in our district.

They went back through all of the video and all of the security and had no trace of him. So can you imagine if somebody was doing a bank robbery and you knew the bank was going to be robbed and you are gonna go back and find out how they did it that you never even had a trace of the person?

This is how wide open it is and the other thing that—if anyone wants to comment—it is a big problem with homeland security, the pointing of the finger of the local—oh, this is the local airport municipality or the ownership of the airport or this is the local police and TSA is just saying it is not our job. Well, it is their job.

Mr. LEITER. Congressman, I would say not to minimize your concern at all, I think it is very appropriate. I think we have similar challenges along the perimeter of much of our critical infrastructure in this country whether it is oil and gas, electrical facilities, and the like.

Going to Mr. Henry's area of expertise, but one in which I also work, we should accept that we have adversaries from around the world who are already inside the perimeter of all of these institutions. It just happens to be in the cyber world.

If we don't look at the combined cyber and physical world together we will undoubtedly be burned by one or both.

Mr. KEATING. We are still recovering from the Wall Street meltdown yet if there is a cyber breach in one of the big five financial institutions, for even several hours, they go bankrupt and can you imagine the effect on our economy.

So you are absolutely right. I yield back my time, Mr. Chairman.

Mr. WALKER. Can I mention one other thing, Mr. Keating?

Mr. KEATING. Yes.

Mr. WALKER. First, I guess I would say to what extent are we using the same technologies that we use on the border of the United States for the perimeter of airports? I don't know the answer to that, but there are technologies that are used to provide border security. So you could argue that this is another potential application of those technologies.

Mr. KEATING. That airport—just to clarify a point—where that young man breached security I believe was the eighth-biggest hub of the country. So this isn't just small airports that this becomes a problem with.

I yield back, Mr. Chairman.

Chairman MCCAUL. Thank you, and point of personal privilege, I enjoyed sharing the Chair with Chairman King for a couple of minutes.

[Laughter.]

Chairman MCCAUL. The Chairman now recognizes the Vice Chair of the full committee, Mrs. Miller.

Mrs. MILLER. Thank you very much, Mr. Chairman. First I want to thank you for this great panel, for all of these great patriots, great Americans coming to testify before the committee.

Sort of a broad range of I think the vision of this committee; where we are going, whether it is border security or cybersecurity or terrorism. Mr. Walker talking about how the National debt is going to impact our ability to secure the homeland, so I say it is a very interesting panel and I am very appreciative of that.

As you mentioned, I am and again, I am very appreciative again to be the Chairperson in the 113th Congress of the Subcommittee on Border and Maritime Security and so I am going to be focusing most of my questions for Admiral Allen and I appreciated your testimony. I will also say I do want to recognize again your service to the Nation, particularly with the Deepwater.

The country has moved past that but we are never forgetting when you were tasked with that mission and when you arrived onsite and started pulling everybody together and just by the very—your presence and your determination, you really—that was a remarkable mission that accomplished so well. Thank you so much for that.

Admiral, you have talked about, you know, all of the various components that might go into operational control of a border; what that might look like. You know, I was interested in a report that came out a couple of years ago from the GAO that talked about the

percentage of operational control that we currently have at the Southern Border which is about, in the 40, low 40 percentile and the Northern Border in its single digits, 1-digit numerals and, you know, this is not the best position to be in, I think.

Whether or not Secretary Napolitano has mentioned that operational control is an antiquated term, but we have to have some sort of metrics. How do you actually measure that?

Our committee is actually going to be—our subcommittee is actually going to be having a hearing just asking the Department: "What does a secure border look like to you, at the Department?" I would ask you, sir, if you were sitting there, what does a secure border actually look like?

Admiral ALLEN. Thank you for the question, ma'am. If I could start off with a metaphor related to the oil spill. I get asked all the time if there is any way to safely extract hydrocarbons in deep water drilling I tell everybody there is no risk-free way to extract hydrocarbons and we are going to go to another generation of energy development before we are going to have to move away from dependence on that.

So the question is: What is an acceptable level of risk to carry out those activities? I would tell you just the same as in deep water drilling, it depends on where you are at, the local region, the particular characteristics related to that, and frankly, the political sensitivities and some of the political perspectives and culture in the region.

The reason operational control of the border is such a vexing term is some cases you can effectively control the border with a 1-mile offense in a downtown municipal area like Juárez or Otay Mesa.

In other areas, sensors, integrated fixed towers can give you enough situational awareness where you can react if something does occur before it becomes a threat inside the United States.

In other places, they are such a remote area in the big bang country of Texas where it is going to take you an hour or 2 hours to get to the nearest crossroad. So the question is: What is deployed there that can respond to the threat?

I think what is needed is an integrated assessment of the areas of the border focusing on regional risk and vulnerabilities and what constitutes the greatest threat. There were conversations earlier about improvised explosive devices and nuclear devices in relation to high-population areas.

I think we need to look at the vulnerabilities that are out there and where we best mitigate risk, understanding that there are places where we will have to respond in some period of time.

That is the reason when people say operational control of the border or border security, I kind of cringe because I used to tell people if you can explain what that is, you have just proved you don't know it.

I think what we have to have is a comprehensive assessment and what happens in one port or one area of the border needs to be specifically—criteria that is equally applied in each area that will produce a different outcome on the type of resources, personnel, sensors that you need, but ultimately, all of that needs to come

back someplace to create common operating picture to direct responses from.

Mrs. MILLER. Well, I appreciate that and just one other question then. Following up on that, talking about the Southern Border, the Northern Border, if you think about the Maritime Border as well and with your background, the Ranking Member asked a question about the percentage of scanning, you know, the Congress saying we are going to have 100 percent scanning.

I would agree with your assessment that that is not possible. We are really only right now at 3 or 4 percent, scanning 3 or 4 percent of all the cargo that is coming.

So as we look at the outer ring of border security particularly from a maritime environment at our ports, et cetera—excuse me—what again, what kinds of things, you know, we talk about some of the—looking at our partners at some of the point of debarkation for some of the cargo, et cetera.

How could we do a better job and again how do you even measure those kinds of things?

Admiral ALLEN. Well, if I could just reiterate on the container situation, I think the best way to reduce that risk as low as we can is to look at technologies that actually allow those containers to be interrogated with sensors while they are being moved and the devices that lift them and that is a technology that has not matured, but I think that is where we ought to be looking there because we are never gonna be able to drive that risk to zero.

We made tremendous strides in the last 10 years in maritime domain awareness in terms of automated identification systems, devices that are required to be carried and transmitted by vessels of a certain length, and long-range tracking devices that are required by the International Maritime Organization when vessels have declared their intent to enter into a country.

It is not 100 percent. We need to continue to evolve this because the more we can identify the traffic that is out there and separate legitimate from illegitimate or dark traffic that is not identifying themselves, then we can funnel those resources where they can best be used to address those threats.

I think building out a robust National automated identification system for the country, which has struggled to get funding and support over the years, and create that maritime domain awareness is the best thing we can do in the maritime domain and that is consistent with international treaties and sharing agreements on trying to track and basically create more transparency out there on the ships that are moving on the ocean.

Mrs. MILLER. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAUL. Admiral, I appreciate your reference to Texas as a "big country."

[Laughter.]

Chairman MCCAUL. The Chairman now recognizes the Ranking Member of the Emergency Preparedness Response Committee, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. Ervin, following up on what Mr. King asked about mass transit, and as you know I am in Newark, New Jersey right across

the river from New York and a lot of our mass transit systems are shared.

Could you be more specific about what security measures should be taken? Does it look like airport security, the screening of the bags, passengers? Does it involve more targeted screening through human observation?

Mr. ERVIN. Thank you for that, Mr. Payne. Well, I think it is really all those things and as I mentioned, New York City I think is a very good incubator in this regard for other relevant cities in the country to emulate. It is a combination of personnel.

In New York you have these Viper teams for example, which are, you know, for want of a better word, multidisciplinary teams of police officers who have a variety of skills who deploy en masse occasionally unprovoked at mass transit stations.

It serves to deter terrorists who are casing mass transit facilities to see what the vulnerabilities are. I think there should be greater deployment of cameras for example. There are smart cameras that can spot anomalies and call those anomalies to the attention of those who are monitoring those cameras at police headquarters and otherwise.

There are sensors that can be deployed that detect the presence of chemical agents in the air and there are also random bag searches. In New York City there was a lawsuit, I think, is correct that the ACLU brought and the city won that lawsuit.

So I would urge the adoption of measures like that in cities across the country and I recognize as I said that financing is a problem especially now at the Federal level and at the State and local level, but this is a major threat and eventually the threat is going to catch up to us if we don't do something to address it not just at the time of the headline but on an on-going basis.

Mr. PAYNE. Just a follow-up on that. What would you think would be an appropriate time line for this transit security that is needed?

Mr. ERVIN. Well, you know, that is difficult to say. I think of the fierce urgency of now, to use that phrase.

I really don't think we have a moment to waste. You know, the principal point of my testimony, and I think Mr. Leiter made the same point, is that we cannot allow ourselves to think that the terrorism threat has receded.

In part I think we are a potential victim of our own success because we have done such a good job over the years in securing the aviation sector. I think that opens up terrorists' eyes to the vulnerabilities that remain with regard to mass transit, with regard to maritime, and also with regard to soft targets.

We haven't talked about soft targets today during the course of the hearing, and I think that you know as devastating as an attack was on the aviation sector, as devastating as an attack would be on the mass transit sector, an attack on a movie theater, on a shopping mall, and not just in New York City or Washington, DC, but in Clute, Texas or in, you know, Nebraska or Idaho would have a huge psychological, political impact in this country. So we have got a huge job to do and fewer resources than ever with which to do it.

Mr. LEITER. Congressman, if I may just add to that. I agree with everything that Clarke has said, but I think it is a mistake to try to only think about this in defensive measures, because we can't defend all of the sites, whether it is mass transit or City Hall or whatever it is. It is simply impossible.

In my view, intelligence is the key here and we have to understand these networks and find the people before they go out and actually launch the attacks. Now, we are not going to be perfect there either; that is critical

From this committee's perspective, I think one of the areas where we have to find efficiencies and improve our capabilities simultaneously is a greater rationalization of responsibilities between DHS-funded State and local fusion centers and FBI joint terrorism task forces.

We have spent a lot of money on this over the past 12 years. They do serve different purposes, but in my view we could rationalize a relationship between those organizations, have just as much safety, and save money.

Mr. PAYNE. Thank you.

I yield back.

Chairman MCCAUL. The Chairman now recognizes the Chairman of the Subcommittee on Cybersecurity, Intelligence, and Security Technologies, Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman, and I want to express my appreciation to the Chairman for his confidence in allowing me the distinct honor of chairing the Subcommittee on Cybersecurity, Intelligence, and Security Technologies coming into this new Congress here on this committee.

I also want to express my deep appreciation to this very distinguished panel not just for your presence here today, but for your long record of service and attention to the multiple issues before us. We watch this morph, but a couple of times this issue has been raised, the word "fatigue" has been identified.

Mr. Leiter, I think you spoke to it quite eloquently and now an aspect of that fatigue includes sort of a sense of complacency and built because of the successes that have been realized by many of the people who have worked alongside of you and your colleagues.

One of the challenges that I face as I look at this and I just left a week of visits throughout New York with many members of the banking community and others that have been most recently victimized by the scope of the attacks. Cyber—how real is this threat, Mr. Leiter?

Mr. LEITER. I think this is far more real than almost anyone understands. We have state-sponsored threats, principally China and Iran and Russia.

In the case of China, stealing absolutely billions of dollars and targeting not just traditional government, not just traditional military, but targeting every sector of our economy; agriculture, advanced manufacturing, clean energy, the law firms that support these worlds, our information service providers, all of them are being penetrated.

The best organizations at this, organizations like BAE who sell cyber defenses, have had these intruders in their networks for 18 months before they even know it.

In the case of Iran, we have seen destructive Iranian cyber attacks on Saudi Aramco and RasGas and if anyone thinks that you can't go from stealing data to destroying data and disrupting critical infrastructure, they simply don't understand the technology.

It is changing a few zeros and ones and that intrusion becomes an attack. So in my view, the scope of economic loss and the potential for physical destruction is very, very real.

Mr. MEEHAN. Well thank you. I think you framed it well.

Mr. Henry, we had the good privilege of working together during your days in the FBI and I appreciated your expertise, but you are one who works exclusively in this area of cybersecurity and I was struck—I mentioned I was in New York and I had been preceded just a few weeks earlier by Mr. Panetta and he used the word a "Cyber Pearl Harbor" talking about trains being diverted off of tracks with chemical weapons and the shutdown of our electrical grid.

But at the same time, how does the average American appreciate that they are affected by what is going on today in the cyber world, they have got a role, and that we have got to be responsive to this threat?

Mr. HENRY. I think that your recognition of that is key here. It is very, very difficult for the average American to see this because it is, to some of them, many of them it is very amorphous.

You can't actually see many of the impacts of this and I think that it may take unfortunately the digital equivalent of planes flying into buildings for people to take this seriously, until they can actually see it.

I have used an example before. If I were to say that there was a bomb under this table, everybody here would get up and run out of the room because everybody knows what it looks like when that bomb goes off. We have seen the news footage. We have seen the movies. We know what that means if there is a bomb under the table.

But if I say to that same audience that there is a foreign adversary in your computer network right now, they are stealing your most sensitive information, your most important research and development, that same group of people looks back at me and smiles like I am telling a joke because it doesn't resonate with them. It is not real to them, and that is very unfortunate.

I think the way we do that is through hearings like this, through committees, through some of the media attention to some of the real impacts.

When Mr. Leiter talks about some of the critical infrastructure that has been damaged, that needs to be highlighted for people for them to understand what the real risk is to their organizations, to our society as a whole going forward.

Mr. MEEHAN. I appreciate your framing it that way as well. One of the recognitions, 90 percent of this internet in which all of our commerce really today is built around, is in the hands of private entities.

Now we have got a real challenge tying together the intelligence resources that we are able to generate but working simultaneously with the private sector and information sharing.

It includes a variety of things, not only how we move that information, but how we protect privacy and other things too. How do we get people comfortable with the idea that we need to be working together while simultaneously being able to protect the individuals concerned about intrusions on thier privacy?

Mr. HENRY. Well, the, again is very, very critical. I think that for people to understand what the risk is that they are willing to accept certain inconveniences that may be critical to securing the networks.

If on September 10, 2001, somebody came from, a Government official, and said from now on September 10, 2001, from now on, we recognize that there as a terrorism threat and we are going to ask everybody to take their shoes off when they come through, take your laptop out of the bag, take your jacket off, you can't carry any shampoo, people would be outraged.

We can't do this. This is an inconvenience. It infringes on people's privacy. But then the next day the world changed and all of a sudden everybody understands how significant the risk is and they are willing to accept the inconvenience.

I don't particularly care to do it, but I get it. I understand what the risk is, what the adversaries are trying to do to us, and I am willing to make those concessions.

I think in the cyberspace it is very, very similar. People need to understand the risk. I think we can balance privacy with security. That is gonna take some work and some effort and I think the committee has a huge role to play in that.

VOICE. Mr. Chairman——

Mr. WALKER. Very quickly I think there are three elements that you have to be able to make real to people, okay.

No. 1, self-preservation. That is the most fundamental in hierarchy of needs. So how can a cyber have an impact that could end up having loss of life?

Second, economic security. How might cyber affect their assets, their resources, their accounts, all right?

Third, personal privacy. Those are the three big elements, I think, and you have to make that real to people to help them understand it and appreciate it and then they will be, I think, more aware and concerned about it.

Mr. LEITER. Congressman, privacy considerations here are really enormous and I would offer at least two ways in which this committee can be of assistance on that.

One is making sure there is transparency about how when this information is shared with the U.S. Government and vice versa, how it is used. Narrowing the scope of how it is used is critical in my view.

Second, currently today, as much as the Department of Homeland Security has done to increase the skill of its workforce technically, it is still pale by comparison to the National Security Agency and the Department of Defense.

They don't have the people they need to do this job well. Hence we talk a lot about giving the National Security Agency and the Department of Defense a larger role in this than we might otherwise do.

In my view, we might have to do that at the beginning, but this committee is critical in providing DHS the management flexibility and personnel authority to bring in people that they won't normally get so they can actually build up that expertise.

Hiring and firing people in the Federal Government is impossible. If you give DHS flexibility to bring in people through private sector for short-term tours at DHS they can build up that capacity much, much faster and then there is less of an operational impetus to share all of the staff all the time with the National Security Agency and Department of Defense.

Mr. MEEHAN. Well, thank you. My time's expired, but I look forward to working with each of you as we move forward in the year on this very challenging issue.

Chairman MCCAUL. Yes, and thank you for your testimony, Mr. Leiter, in terms of, I think, building the capability and credibility—excuse me—of the cyber workforce within DHS will be a priority as well.

The gentleman from Texas, Mr. O'Rourke, is recognized.

Mr. O'ROURKE. Thank you, Mr. Chairman.

I would ask for unanimous consent to submit two articles both published this week—one by our county judge in El Paso, Veronica Escobar, the other by Eric Olsen and Chris Wilson of the Wilson Institute—both dealing with the dynamic on the U.S.-Mexico border and the need to secure our border without sacrificing our way of life, trade, mobility, and our economy.

Chairman MCCAUL. Without objection, so ordered.

[The information follows:]

ARTICLE SUBMITTED FOR THE RECORD BY HON. BETO O'ROURKE

FEBRUARY 10, 2013

GRIDLOCK ON THE RIO GRANDE

By Veronica Escobar, El Paso.

Talk of comprehensive immigration reform is welcome news—especially because it could offer a possible path for citizenship for undocumented immigrants and more visas for highly-skilled workers.

But the debate's focus on enforcement is ill-advised and its approach is still too narrow. By emphasizing enforcement, Federal resources won't go where they are truly needed: America's international ports of entry, where millions of dollars in goods enter and leave the country each day.

These ports are overburdened and underfinanced. While billions are spent on walls and drones, the movement of people and goods is choked. Instead of further militarization of our Southern Border, we need to invest in the movement of people and goods through our land ports. The El Paso area's five ports of entry handle tremendous traffic: In the 2011 fiscal year, they had 6.8 million pedestrian crossings, 811,000 truck crossings, and almost 11 million car crossings, which translated into $80 billion in trade.

Much of that trade arrives in the form of trucks that go on to points deep inside the country. But a substantial amount stays in El Paso: Some 350,000 visitors walk across the Paso del Norte bridge into downtown every month.

But these ports haven't received significant Federal investment in personnel or technology for years. Facilities are outdated and understaffed. A Texas Department of Transportation assessment found that two were already at "operational failure," with average peak wait times of more than an hour for commercial traffic and 2 hours for passenger traffic.

One has only to view the rush hour between El Paso and Ciudad Juárez, its Mexican counterpart: Long lines of idling vehicles and exasperated pedestrians, infuriating at best, hazardous—during sweltering summer months—at worst.

Last year Steve Ortega, an El Paso City Council member, frustrated by the lack of meaningful response to the long wait times, drove repeatedly across the border to experience the process himself. Each morning he waited at least twice as long as what was being reported, mainly because most of the available lanes were closed for lack of staff.

El Paso isn't alone; ports of entry all along the border need investment. But for too long, policy makers, including the Obama administration, have fixated on security and enforcement to the exclusion of all else.

The result is a significant and chronic loss of jobs and trade on both sides of the border. But long waits could be eliminated if the Federal Government would aggressively invest in personnel, port infrastructure, and technology.

El Paso County is building a new port of entry, but the Federal Government has to pay for its personnel. Will it be another clogged artery in a country that fails to recognize the enormous benefits of cross-border movement, or will it be adequately staffed through more rational immigration reform?

When Government prioritizes enforcement and minimizes the benefits of the people and goods flowing through those ports, it does so at its own peril. Just as a path to citizenship for the undocumented would create millions of new taxpayers, a smoother path through our ports would create stronger economies.

Veronica Escobar, a Democrat, is the county judge in El Paso.

POLITICO ARTICLE SUBMITTED FOR THE RECORD BY HON. BETO O'ROURKE

DEFINING BORDER SECURITY

By: Eric Olson and Christopher Wilson

February 10, 2013, 08:48 PM EST.

The recent announcements by President Barack Obama and a bipartisan group of senators outlining broad principles for immigration reform are very welcome. While the specifics of any reform will be hotly debated, a major advance has been made with the emergence of a broad political consensus, from left to right, that the current system is broken and in need of major repair.

It would be troubling, then, if this golden opportunity to fix a broken system falls victim to the very same trap that has ensnared other reform efforts. By conditioning reforms on achieving a poorly defined and much misunderstood notion of "securing the border," the whole effort is at risk of unraveling.

It has never been clear what precisely is meant by the term, but billions have nevertheless been spent on fences and sophisticated technology, and the Border Patrol is now more than five times larger than it was two decades ago. Has the border been secured? Hard to say since there is no agreement on the metrics for measuring border security.

In the post-Sept. 11 era, border security has largely been thought of in terms of terrorist threats, "spillover" violence from drug-trafficking organizations operating in Mexico, and the risks associated with undocumented migrants. The top priority for border law enforcement has been denying entry into the United States to would-be terrorists. To this end, enforcement has been quite effective: There are no reported cases of a terrorist attack in the United States that involved passage over our Southern Border.

While drug-trafficking-related violence in Mexico has increased dramatically in recent years, violence has largely stayed in Mexico. Illegal drugs continue to flow in significant amounts, but crime data suggest that it has not contributed to a significant increase in crime or violence in the United States. There are exceptions to this, such as the 2009 kidnapping of a suspected drug trafficker in West Texas, but these are exceptional cases, not a trend, and communities near the border have, on average, rates of murder and violent crime that are lower than the rest of the Nation. San Diego and El Paso, the two largest cities on the border, are among the safest in the country.

Protecting the United States from the unauthorized entry of migrants often becomes the default criterion for establishing border security. Counting illegal crossings is inherently difficult, but we do know that unauthorized crossings are at their lowest point in 40 years, and the Pew Hispanic Center believes there are now as many Mexicans leaving the United States as entering. Studies have also dispelled the myth that immigration and crime are linked; in fact, the presence of a large immigrant population appears to actually help make a city safer.

All of this is to say that defining border security is actually quite complicated. The Department of Homeland Security has been wrestling with this concept for some time, and is currently working to revise its definition and measures of success.

In the absence of a clear definition and diagnostic of border security to help focus their strategy, Congress and the past two administrations have responded to border security concerns by dramatically increasing spending on technology and personnel on the border. The focus of these efforts has been the vast empty areas between the official ports of entry. Yet nearly half of all unauthorized immigrants in the United States entered through our ports of entry with legitimate visas but failed to leave when their visas expired, and most hard drugs like cocaine and methamphetamine likewise enter via official crossing points. While the Border Patrol does appear to be apprehending more unauthorized crossers, migrants are taking ever-greater risks by heading farther into the desert, with hundreds dying each year as a result.

The relative lack of attention on the official crossing points is also getting in the way of business. Wait times at the border for cargo and individuals have increased, resulting in new costs to manufacturers and shrinking the number of customers who enter the United States each day to shop. This same congestion can actually facilitate illegal crossing and trafficking rather than decrease it.

So before Congress and the Obama administration fall into the reflexive pattern of conditioning immigration reform on border security and spending additional money to further beef up the Border Patrol, we suggest they take a close look at what has already been done and whether more of the same is really the answer. As Homeland Security Secretary Janet Napolitano recently said at the Wilson Center, "We're getting to the point of diminishing marginal returns. What would really help us is if we could improve the legal migration system so that people come through our ports of entry."

Instead of making another border buildup a pre-condition for immigration reform, border security should be addressed in a way complementary to immigration reform. To do so, two things are needed. First, clearer metrics for border security must be established so we can ensure limited resources are directed to where they can best protect the Nation. Second, rather than more border security, we need better border management. Creating more legal avenues for workers to enter and depart the United States in an orderly fashion also serves as a disincentive to illegal immigration and allows law enforcement to focus its energy on more dangerous traffic. Similarly, at official border crossings, techniques to expedite known, safe travelers and shipments can free up resources to search for and deny entry to criminals and contraband.

Eric Olson is associate director of the Latin American Program at the Wilson Center and an expert on regional security and organized crime. Christopher Wilson is an associate with the Wilson Center's Mexico Institute and an expert on U.S.-Mexico trade and border management.

Mr. O'ROURKE. For Mr. Walker, you know, in your testimony I was, I was very pleased to hear you talk about doing more with less and for your request that we adopt efficiency, effectiveness, economy, and credibility as the watchwords for DHS going forward.

For a little bit of context for my question, I represent most of El Paso, Texas, which with Ciudad Juárez forms one of the largest binational communities in the world. We have five land crossings connecting the two communities and two countries over which pass $80 billion in trade every year.

In addition to that, there are millions of pedestrians and auto crossings every year in El Paso and those crossing north spend upwards of $2 billion in our economy, and the trade and retail activities alone support about 50,000 jobs in my community.

At the same time, we have 2-, 3-, even 4-hour wait times to cross those bridges—up to 9 hours for trade—and so with the over doubling of the Border Patrol force that we have seen in the last 10 years, billions of dollars spent on border walls, and the adoption of new technologies like drones to man the border, how do we do more with less?

How do we prioritize our ports of entry and the legitimate legal crossings taking place there and not sacrifice the economies of com-

munities like El Paso, the economies of the State of Texas—Mexico is our largest trading partner—and the economy of the United States; 6 million jobs are dependent on U.S.-Mexico trade?

Mr. WALKER. Well, first, I have been to El Paso several times so I know exactly what you are talking about. Look, I think we are all recognizing that the threats are real and they are diverse. I think we are also recognizing that the resources are constrained and are likely to get more constrained as time goes on.

There is no such thing as zero risk and therefore I think what it means is that we not only have to develop a comprehensive integrated strategy but we have to work with our partners, in this case, Mexico and if we are talking about freight that is coming from Europe, or Asia or whatever, we have to work more productively with our partners to be able to figure out what can be done elsewhere but before you get to the border, to keep able to use technology to a greater extent, and to, you know, have human intervention on a more limited basis in circumstances where we think there may be a credible threat or there is something unusual, alright?

So there is clearly an opportunity to make more progress there. Quite frankly, we are going to have to make more progress there given that we can't mitigate all the risk and given that we want the flow of people and we want the flow of goods and given that resources are going to become more constrained as time goes on.

Admiral ALLEN. Sir, could I make a comment?

Mr. O'ROURKE. Please.

Admiral ALLEN. When I was commandant I served as the chairman of the interdiction committee for 4 years and made several trips to El Paso, and in the middle of 1970s I was one of the people that set up the maritime program with the El Paso Intelligence Ccenter. So I am familiar with El Paso.

I would like to focus a little on some of the challenges the CBP has related to border operations and I think it is really important to understand this. The inspections that take place at ports of entry are done by the Office of Field Operations and the Border Patrol's mission is between ports of entry.

When you are looking at how to effectively—and I am really cognizant of the trade issue down there. I recently did a panel with Nelson Balido of the Border Trade Alliance looking at how we could do this better and also Mr. Winkowski who is the acting Customs Commissioner.

We need to look at the actual organic operation of the ports of entry, how they are staffed, how they are resourced, and we also need to look at how CBP is resourced to carry out these missions.

They are still dealing with a legacy appropriation structure that looks at fees that go back to when agriculture, customs, and INS were actually separate inspections.

They have problems with their human resource structure over time, how they handle their workforce, and it really restricts their agility and flexibility on how they apply inspection operations at ports of entry.

Likewise, I think we need to look at queuing on the Mexican side of the border, how we handle truck traffic, which you know there is a large amount of, agricultural products that come across. Most

of the offloads by trucks on the Southwest Border are done for agricultural purposes.

I think, I try to bring all of these things together and look at them as a system, and I look at the resource structure that supports those in terms of the human resource practices that are going on inside of CBP and how they have to fund their personnel overtime and so forth is something that desperately needs to be looked at.

Mr. O'ROURKE. Very quickly, Admiral Allen, I was pleased to hear you talk about the consequences of zero risk; one of which would be zero trade to paraphrase what you said. I want to commend and thank the Chairman and many others for their remarks about the need to set defined goals, metrics that will chart our progress towards those goals because right now, border security can mean many different things to many different people, and I am afraid that any more border security in areas like El Paso will crush our economy, our way of life, and threaten the National economy as well. So I appreciate your testimony.

Chairman MCCAUL. The Chairman now recognizes the Chairman of the Oversight and Management Efficiency Subcommittee, Mr. Duncan.

Mr. DUNCAN. Thank you, Mr. Chairman, and thanks for your confidence in me to handle the committee that you led so well in the last Congress.

I want to thank the members of the panel for your service to our great Nation in your various roles.

Specifically, Mr. Walker, and continuing, I will raise awareness about the Nation's debt and our fiscal situation and its threat to our National security.

If you followed the last Congress, you will understand that one of the areas of emphasis that I had was Iran and the threat that Iran and its proxies posed to the security of the United States.

Mr. Leitner, if you could provide, I am gonna ask you to provide in writing to the committee and myself, your thoughts on Iran and specifically the Caracas-Tehran nexus in a post-Chávez Venezuela.

That is an in-depth issue I know and so for my oversight role, what I would like to ask you guys independent of that, given the fact that the Department of Homeland Security has a $59 billion budget, 225,000-plus employees—and I will start with Mr. Walker—if you were named Secretary of the Department, where would you direct the resources to meet your mission or the mission of the Department?

Mr. WALKER. Well, that is getting down to the detail. I guess what I would say is I would come back to what I said. I think that you have to have three things to effectively manage any entity. You have to have a strategic and integrated plan that is forward-looking, threat/risk/opportunity-oriented, resource-constrained.

Second, you have to define specific goals and objectives. What are you trying to achieve? How do you measure success?

Third, you have to have outcome-based performance metrics. How can you end up measuring whether or not you are being successful? Are you getting better or worse? How do you compare to others on an outcome basis?

Third, you have to allocate your limited resources to be able to maximize value, mitigate risk within current and available resource levels.

That means: Do they have all of those? They don't have all of that to the extent that they need to. Second: Who is going to execute on this? Who is going to make sure that the systems and the processes are in place and that you have continuous improvement in order to be able to execute on these things? I am talking about the—I am not talking about the operators, but I am talking about the management aspects and support mechanisms.

That is why I come back to a chief operating officer who is focused full-time on these types of things because the fact is, is that we have too much turnover in those critical roles that, you know, very good political appointees are appointed, but they don't necessarily have the right background. They don't necessarily stay there long enough in order to effectively do what needs to be done.

So, I mean, I would give you—that is what I think needs to be done rather than saying I would give more money in this particular area versus another because it would be, I think, I don't have that data to be able to give you an intelligent answer there.

Mr. DUNCAN. Okay. I am going to ask the admiral to comment on that and then I am gonna come back to Mr. Ervin. How would you allocate those resources to meet the mission?

Admiral ALLEN. Frankly, sir, I would go with the current financial structure of the Department and start there. You need to be able to enable mission execution with a mission support organization and that is not completely integrated in the Department now.

There have been great strides that have been made in the last 10 years, but attempts to establish a core financial accounting system and a standard human resource system have not been successful.

One of the problems I think exists if you want to get right to the bottom of it is that the appropriations structures for each of the components is not the same.

It is not possible to compare personnel costs, operating costs, and capital expenditures across the components. Because of that, it is not possible to come up with future-years homeland security plan very similar to the future-year defense plan that allows consistency in planning, especially in capital investment.

I believe that the first step towards getting our arms around this would be to standardize the appropriation structure—and this gets back to the comments I made about CBP's having a legacy structure of fees that date back to their legacy departments that have never been rationalized—so it makes it almost impossible to estimate personnel costs.

This is like blocking and tackling of management. Without that structure below you it is going to be very hard to do that. I would start with the financial management structure of the Department.

Mr. DUNCAN. Okay.

Mr. Ervin, how would you allocate the resources?

Mr. ERVIN. Well, sir, I guess I would make a—one quick overarching comment and then give a couple of items of detail.

I guess my overarching comment is I think the bulk of the DHS' resources should be deployed on the counterterrorism given the im-

portance of that mission to the Department and the genesis of the Department.

To be a bit more detailed about that, given this budget environment, I think the DHS should look hard and I think this committee can be helpful in this regard and I think, to be fair, DHS is beginning to look hard. It needs to look harder.

Among the missions it performs, even within the counterterrorism space: What is it that DHS can perform uniquely that other agencies either literally cannot perform or can't perform as well as DHS? I will give you two examples.

One is the Intelligence and Analysis, I&A unit, at DHS. There are lots of other intelligence agencies, some 15 others within the United States Government, but of all the multiple intelligence missions out there, the one it seems to me that DHS uniquely can play is to take the intelligence that the rest of the community collects and analyze this and then make sure that that intelligence is then shared with the private sector that owns and operates the bulk of critical infrastructure and State and local governments in a nonclassified way, but in an actionable way, in enough detail such that action can be taken on it when action needs to be taken, and I don't know that DHS has focused on that enough.

The second area that I would highlight is S&T. There are lots of other S&T R&D components elsewhere in the United States Government; DOD comes immediately to mind and that is the case as well in the intelligence community.

It seems to me that S&T should do a better job of piggybacking onto those research and development advances that other agencies have developed and deployed, and then focus on what it is uniquely that either DHS should develop or should adapt for the unique purposes of the homeland security mission.

I think if that mindset is brought to bear we can see huge economies, huge efficiencies, and a more effective security for the Nation.

Mr. DUNCAN. Okay.

Thank you, gentlemen.

I yield back.

Chairman MCCAUL. The Chairman now recognizes the gentleman from Texas, Mr. Vela.

Mr. VELA. Thank you, Mr. Chairman.

I, like Mr. O'Rourke, represent a border region in Texas. I represent the most southern border region beginning in Brownsville, and I just have a few questions.

Mr. Walker, you have on a few occasions mentioned the difficulty in mitigation of risk, and I was curious if you could expound on that.

Mr. WALKER. I think my point is that we are never going to fully protect the border. We are never going to fully protect the air system. Just recognize reality. That is not going to be the case.

It is an impossible task and therefore we also have to recognize that we have got limited resources that are going to become more limited and that is why it is so important to be able to create this comprehensive integrative plan that focuses on risk. There are certain areas of the country that are higher risk than others.

There are certain modes of transportation that are higher risk than others. There are certain areas of the country that quite

frankly where you don't have, you know, a large population and you can use technology to be able to help scan the border, but if somebody crosses the border, which they easily can, you are going to have to have a system to be able to get them within 100 miles or something of that nature in order to be able to deal with it.

So we have to recognize there is no such thing as zero risk. We have to mitigate risk. It will never be zero and we need to mitigate it in an intelligent way where we are trying to protect as many people as possible and as much assets as possible given the resources we have.

Mr. VELA. Of course like Mr. O'Rourke, we have a significant interest in our Texas border on the facilitation of trade, so I share many of the same concerns that he has.

Admiral Allen, one of the questions I have for you is, I was curious as to your thoughts on the significance and impact of security in Mexico on the safety of citizens on our side of the border.

Admiral ALLEN. Let me start with an overarching statement. I believe the most significant security issue that Mexico has to deal with is their southern border and their ability to control illicit trafficking, movement of people.

Once either people or contraband moves into Mexico, we are dealing with our own ports of entry. So I think as a general statement, working with Mexico to enable them to do a better job on their southern border is in everybody's best interest.

They have had tremendous challenges there; the new administration coming into place has some ideas about what to do with the national gendarme, if you will. They have been effective in the past by using their naval forces and their Marines as a special operation forces, if you will, to be effective against the drug cartels.

We exchange information with Mexico. We are improving daily on that. I think there has to be a shared common purpose on the border related to exchange of information. There are some barriers. Those barriers are starting to be dropped down, but I think in the long run it is in our best interest to enable our Mexican partners to deal with their southern border first and then look at the art of the possible in dealing with our borders as far as managing risk.

That includes things like taking advantage of high-performance computing and data analysis to look at license plate reader data, and other things out there that we can't put into a data link or data cloud and do analytics on them to look at trends and anomalies that would allow us to be able to attack the areas of highest risk.

Mr. VELA. What is the state of affairs, so to say, of Mexico's efforts on their southern border?

Admiral ALLEN. I might defer to other panel members here if they have any information on that because I am a little time late being out of the Coast Guard at this point.

I do know initiatives like the America Initiative may have been put in place to give them resources and create capability and capacity to allow them to manage those issues on their southern border.

I believe that this is a regional issue. It is not just a Mexican issue. The Central American countries that are suffering the corrosive effects of drug movements that are now moved into the littoral

areas in mainland because of our successes offshore are producing a regional risk down there.

I think the more that we can encourage regional approaches to their southern border the better off we will be, but I think anything that empowers them to have a better situational awareness, to be able to move resources, and attack those threat vectors that are crossing the southern border should be our goal.

Mr. VELA. So do any of the other witnesses have that information with respect to the current state of affairs of Mexico's efforts on the southern border or is that something left for maybe another witness?

Admiral ALLEN. I would defer to our current colleagues that are in Government right now and potentially probably a classified briefing.

Mr. VELA. Okay.

Thank you, Mr. Chairman.

Chairman MCCAUL. Thank you. The Chairman now recognizes the gentleman from Utah, Mr. Stewart.

Mr. STEWART. Thank you, Mr. Chairman.

To the witnesses, thank you for being here today and thank you, each of you, for a lifetime of service to your Nation.

This committee has broad responsibilities. We have touched on some of those responsibilities today even if only briefly—border security, anti-terrorism training and efforts, WMDs, cybersecurity—I mean, the list is long.

I am a former Air Force pilot. Many years we were trained to be effective; we had to analyze the threat. We had to prioritize the threat in order to effectively defeat that and I would ask you to kind of take a—you know—again an Air Force analogy; a 30,000-foot view here.

Is there, with your various backgrounds and your areas of expertise, is there a consensus at all about what our priority should be? Our No. 1 priority?

If there is not a consensus, would you individually answer the question? If you were king for the day, what would you do? What would be the one thing that you would do in order to, you know, most greatly enhance our security; the thing were all striving to do?

Admiral, we will start with you if you don't mind.

Admiral ALLEN. Let me echo what was said earlier and I quote my very good friend, Mike Mullen, past chairman of the Joint Chiefs of Staff. I don't think it can be overstated enough the current risk that the current budgeting situation, continuing resolution, sequestration, and the uncertainty associated with that has on National security.

Moving to actual threats themselves, I would place cybersecurity at the top.

Mr. STEWART. Okay.

Admiral ALLEN. I think one of the challenges associated with cybersecurity is that it manifests itself differently; the different infrastructure sectors and with privacy. I think somewhere we need to divide that out and then talk about what an inherent Governmental role is within the regulatory frameworks of each of those

sectors, and find out where that places where we can exchange the information that was alluded to moving forward.

I think after that, we need to look at how we functionally manage our borders—not just at a port of entry or between or Border Patrol or field operations or Coast Guard does. We need to look at the border as a holistic framework and how we are going to minimize risk by, in my view what is underutilized right now is bringing the various sets of data that are resident in the components and taking advantage of high-performance computing and data analytics to be more aware of anomalies and where we ought to be putting our forces.

Mr. STEWART. So Admiral, just making sure I understand, your No. 1 would be, focus would be, cybersecurity then?

Admiral ALLEN. Right now, yes.

Mr. STEWART. Okay. Yes.

Mr. Henry.

Mr. HENRY. Well, I will follow on then on the admiral and concur as well on cybersecurity. Although as a taxpayer and a former Government employee working in the budget, certainly our budget deficit is a significant concern to me for a lot of different reasons that have been articulated here.

I think from the cybersecurity perspective, what we need to do, king for a day, what is the one thing you need to do, I think it really is defining the red lines and communicating those red lines to our adversaries, so they know very clearly what the repercussions are for attacking the United States of America whether it be stealing intellectual property or impacting our critical infrastructure.

That has got to be key, and again, we cannot just merely try to reduce the vulnerabilities. That is important, but we have to thwart the adversary. They have to know that they cannot attack us.

There are so many comments that have been made here today by each of the distinguished witnesses regarding counterterrorism and protecting the border, all of those things that they said absolutely apply right here to this space, to cyber, it is a direct parallel.

Mr. Leiter talked about——

Mr. STEWART. Mr. Henry, could I, could I just add, follow-on before you move on? It seems to me that they don't pay a great price right now that to some degree they work with some impunity towards us. Would you agree with that?

Mr. HENRY. There is no risk to the adversary. The return on their investment is tremendous.

Mr. STEWART. Yes.

Mr. HENRY. They are stealing billions of dollars, and there is no risk because nobody is telling then, "Stop."

Mr. STEWART. Yes.

Mr. HENRY. Nobody—there is no penalty and until the penalty and the threat to them, the risks to them, outweighs the game, you are absolutely right, Congressman, there will be no stopping this threat.

Mr. STEWART. Okay.

Admiral ALLEN. There is no barrier to entry.

Mr. STEWART. Yes.

Mr. LEITER. Congressman, with the caveat that I am a formal naval aviator, so you might choose to dismiss everything I say.

Mr. STEWART. You are a bigger man than I am, if you have landed on a carrier.

Mr. LEITER. Just close your eyes and pray. Congressman, I would say two mission areas that I simply can't say one is more important than the other; counterterrorism and cyber.

But on counterterrorism I am going to caveat that with we can not aim to stop every small attack and we have to really defend and prioritize the catastrophic event.

But there is a different priority that I would take which is not mission-focused, it is following on what Mr. Walker and Admiral Allen said. If I was king for a day, I would spend 75 percent of my time striving for true coordination and cohesiveness across the Department, and then making sure that the Department is really only doing those things that other departments and agencies can't do in the rest of the Federal Government.

By doing that, I am going to have a lot more capability and resources to cover all of my other mission-focused priorities.

Mr. STEWART. Okay, thank you.

Mr. WALKER. If you don't put your finances in order, everybody will suffer to differing degrees over time and every function of Government will suffer to differing degrees over time.

Second, I do agree that we need to focus on, you know, a more comprehensive and integrated approach, a more risk management approach, focus on core competencies and comparative advantage, which is I think what is being said. What can they do uniquely?

Then last, cyber and border. I think, my personal view is we are wasting a hell of a lot of money on what TSA is doing domestically with regard to airport security.

You know what TSA stands for, right? The acronym? Yes, okay.

Mr. ERVIN. I associate myself with everything my colleagues said. I particularly agree with Mr. Leiter. He said exactly what I would say about where to focus.

You know, I think it is very tough to distinguish between the degree of threat posed by cyber and terrorism. I think they are essentially equal within terrorism.

I would agree with Mr. Leiter what he said earlier that we need to focus most on events that are low-probability but high-consequence, namely the threat of terrorists with the weapons of mass destruction.

In terms of what to do about it, again I agree with my colleagues. One thing that hasn't been said that I think is important is that, you know, I think the figure of $100 billion was used by Mr. Leiter earlier as the total amount of money that has been spent since 9/11 to secure our country against the threat of terrorism. It is something like that—yearly, annually. So it is a huge amount of money needless to say.

But we don't have an integrated approach, a strategic approach to the expenditure of that money. There is a lot of duplication within DHS across agencies with regard to that and I don't think—for example, part of the strategy is how much of the total money spent is focused on preventing terrorism? Countering violent extremism?

To what degree is that integrated across governments? So I think greater attention needs to be paid to that and I think it would yield outsize dividends if we were to.

Mr. STEWART. Thank you, all.

Mr. Chairman, I yield back.

Chairman MCCAUL. Thank you.

The Chairman recognizes the gentleman from Nevada, Mr. Horsford.

Mr. HORSFORD. Thank you, Mr. Chairman.

I look forward to working with my colleagues on this committee.

My district includes a portion of Las Vegas and our airport there, the McCarran Airport, is the fifth-busiest airport in the country; nearly 40 million people fly through that airport on an annualized basis.

So listening to the testimony today, clearly security, technology, innovation is at the forefront and I appreciate the explanation while also balancing the interests of civil liberties and protecting the privacy of individuals.

My question is: What are the processes in place to share the best practices that we have learned over the last few years in airport security, particularly in large airports like McCarran, and how do we share that with other airports that aren't yet at that level? And for airports that are at the cutting edge, how do we make sure that they are staying at the cutting edge?

Mr. ERVIN. Well, I guess I will start there—start with it. I think it is a very good question. I don't know frankly the extent of which TSA focuses on best practices among airports. You know, there certainly is a degree of variation among them.

There are differing degrees of effectiveness, differing degrees of efficiency, differing degrees of innovation as you said. I don't know that there is an organized way to do that, but there certainly should be. I agree with that.

Mr. WALKER. I fly multiple times every week all over the country. I have been to all 50 States. I have been to 100 countries. I think that is a great question to ask the administrator at TSA because it is a very clear to me they are not consistent. They are not consistent and there are clearly opportunities to share best practices and lessons learned, if you will.

Mr. LEITER. Congressman, I am not sure of the best practices, but I would say one thing for this committee to consider how TSA and the Department of Homeland Security can accelerate those programs that we all know work well, which are real risk-based approaches, in particular global entry and TSA PreCheck.

These are ways of focusing on the people you have to focus on and not focusing on the people that you have already done background investigations as a matter of intelligence are far lesser threats.

Admiral ALLEN. Just to follow up, if you look at the risk-based, screening is probably what you want to do. I don't think there is any legal requirement to run people through scanners. That is the technology or that is the process that is being used right now even with the new advanced imaging technology.

I think the more you can understand about people and the threat posed by that and the more you understand about them in advance

related to prescreening, the better off you are going to be, but I would encourage TSA very much to go to risk-based screening, to look at other areas other than just—and Clarke already mentioned this—you know, just screening for anomalies is not going to reduce risk to zero.

But to allow them to understand more about passengers, to understand about behaviors, behavioral detection officers is being deployed, and things that don't negatively impact the queues.

Mr. HORSFORD. Mr. Chairman, just a follow-up briefly.

On the counterterror-attack funding—I think one of you mentioned that earlier—I know that there have been issues in the past where communities like ours that have a higher tourism base aren't always taken into account in that methodology. Can one of you touch on the need for that in various areas?

Mr. ERVIN. Yes sir, I think I am the one who mentioned it, but I am sure we would all agree with that. As you know, over the course of the, you know, decade or so of post-9/11, DHS's history, there has been a constant struggle over how counterterrorism—scarce even then and even scarcer now—counterterrorism dollars should be allocated.

You know, my argument is that, you know, perhaps there is a role for pork barrel programs, one can argue about that, but if there is, there certainly isn't a role for pork with regard to counterterrorism dollars in particular in this time.

So I think on a bipartisan, bicameral basis, there needs to be a consensus about the obvious that certain—the larger a city is, the more iconic it is, like Los Angeles being a tourism mecca, Las Vegas and—and I believe that there was some interaction with the 9/11 hijackers in Las Vegas as a matter of fact—the more likely it is that they continue, those cities continued to—localities generally speaking—continue to be in terrorists' crosshairs. So we have got to direct those counterterrorism dollars to cities and localities most at risk.

Chairman MCCAUL. Thank you.

The Chairman now recognizes the gentleman from Pennsylvania, Mr. Rothfus.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Admiral Allen, I appreciated the interchange with Representative Miller about the operational control of the border issue.

You know, we are going to be taking a look at immigration and one of the measures that they are going to be looking at is securing the border and I think part of the discussion was there is going to be maybe a commission that would certify that the border is secure.

You know, what are going to be the criteria? Are there objective criteria by which we can judge whether the border is secure? What would we be looking for?

Admiral ALLEN. Well, it gets back to the comments I made about the oil spill. These are sometimes subjective evaluation of what is acceptable risk because the risk can never be driven to zero.

But what it needs to be is an acceptance of risk that is openly arrived at, transparent, and the criteria that is supplied in the discussion needs to be universally understood, recognized, and accepted.

That will be different in different parts of the border. It is a far different border in Ciudad Juárez and El Paso than it is in Detroit where you have got an international border there with Canada.

I think what we need to strive for are criteria that we can apply to a certain area that will produce different outcomes depending on the geography and everything else.

Mr. ROTHFUS. What kind of criteria would we be looking for?

Admiral ALLEN. Well, the physical nature of the border itself. Is there a land border? Is there a water border? The type of access, the terrain.

The population density, the amount of cargo in traffic that moves through it. How much of that is related to trade? How much is foot traffic?

All of those are different dimensions——

Mr. ROTHFUS. So if it is a land border for example, are we looking at a fencing issue, I mean looking at, you know, remoteness——

Admiral ALLEN. Well, I think you——

Mr. ROTHFUS [continuing]. If it is a water border, are we looking at certain either drones or cameras or something watching?

Admiral ALLEN. If you look at a highly densely-populated area, you can extend fencing out several miles either way and you have not reduced the risk to zero but you have channeled the threat to places where it can be more adequately dealt with.

There are places where fences aren't going to do you any good, out in the middle of nowhere. Where you have a river or some other natural barrier, that needs to be considered.

I guess what I am saying is we need to come up with a universally recognized and accepted set of criteria that will allow us to make it the best assessment of risk and then accept that in terms of what constitutes adequate border security knowing that it will never be driven to zero and if we wait for that we will never—if we drive it to zero, we will have no trade in this country and you will never see immigration reform.

Mr. ROTHFUS. As far as establishing those criteria, I guess it is to policymakers in this House and looking to the people in the administration who would be suggesting things also?

Admiral ALLEN. I believe, and this gets back to my experience in environmental issues and the oil spill, there is a much different view of what constitutes an acceptable level of risk in the Gulf of Mexico say than there might be off southern California or off the North Slope of the Arctic.

These are local issues that that need to be—that need to be taken into account the concerns and the equities of those communities, but I think from a National standpoint, we have to come up with a set of criteria where we equally apply those to areas knowing they will be different outcomes because as one of my predecessors said, "If you have seen one port, you have seen one port."

That doesn't mean you can't apply criteria to each port. It might produce a different outcome, but then you have a standard way to assess risk and know what kind of risk you are accepting.

Mr. ROTHFUS. Thank you.

Mr. Henry, on cybersecurity, you know, taking a look at the organization of the Department, we have an office in the National pre-

paredness—it used to be preparedness—the programs and—NPPD directorate. There is an office of cybersecurity there.

We also have cybersecurity elements in other components of the Department. Is this the optimal organization for cybersecurity issues at the Department? Should we be—we are two levels down from the Secretary that I can see anyway on handling cybersecurity issues.

Can you comment on the how the assets of the Department are deployed with respect to cybersecurity?

Mr. HENRY. Yes, let me first say that when we are talking about cyber, we are talking about espionage, we are talking about terrorism, we are talking about criminality. Cyber is actually the tool.

So that is why so many of the things that we have talked about here and other areas, border protection, counterterrorism, et cetera are absolutely relevant in this space. That is important to get out.

As it relates to DHS, I think that you need to have visibility into this at the senior levels. I think that executives have to be part and parcel of this. This is a whole-of-Government response and a whole-of-agency response, and there is a lot of overlap and many gaps and not enough comprehensive review of this at the and in the departments and agencies and writ large, the Government writ large, so I think that that has got to be considered and look across the agency and bring it, consolidate it into one particular area with the leadership of the executives directly involved.

Admiral ALLEN. I might suggest there are three roles inside the DHS related to cyber, and I am going to go functional not related to the threat that Mr. Henry talked about.

The first is the Department has to protect its own network. The second: There is a role right now for the Department in coordinating across the dot-gov domain, in terms of continuous diagnostics and monitoring, to bring them in compliance with the administrative directive regarding how the entire Government will defend its networks.

Third is the external requirement that we have discussed here today to interact with the private sector, especially regarding infrastructure protection and how those sectors will be protected, and that is a work in progress impacted by the Executive Order that was signed by the President yesterday and hopefully will be codified and have legal ambiguities removed through legislation that is passed by Congress.

So if you look at those tiering, it is easy to kind of break out who in the Department is doing what. For internal network security you are talking about the CIO. When you are talking about their role in relation to the dot-gov domain and the private sector, then you are talking about NPPD, but there also is a role for Intelligence and Analysis that are related to how they are dealing with the State and local governments in the critical infrastructure sectors as well.

Mr. ROTHFUS. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAUL. The Chairman now recognizes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

I thank the Ranking Member.

I thank all of you who have testified before us today, and I am going to be a little bit more provocative than some of my other colleagues because I truly believe that while we all have good intentions when it comes to homeland security, we are really playing at homeland security, we are not doing homeland security.

I say that in the light of the fact that when you look at our armed services and the role that they play in securing our Nation, if we treated our armed services the way we treat homeland security, other nations would be eating our lunch. Other nations would be eating our lunch.

The title of today's hearing was "A New Perspective on the Threats to Homeland," and as a New Yorker I am extremely sensitized to it having lived and currently living in New York City; I am extremely sensitized to it.

But when I have CBP officers or, come to my office to tell me how at any moment in time something really bad can happen because they are doing double, triple shifts because assets have been moved to the Southern Border and we are not looking at the whole matrix of what needs to be done to actually have the FTEs in place to protect our Nation, I get concerned.

I get extremely concerned, and when we talk about cybersecurity for instance, we know what the vulnerabilities are. It is not a matter of, you know, how it is going to happen, it is—it is like, when is it going to happen, at this stage.

So my concern is that while yes we are trying to do more with less, why are we playing with homeland security? Why is it that everyone is so ambivalent to talk about what is really required to secure the homeland?

I am really intrigued at the fact that were this the Marines, the Air Force, the Navy, the Coast Guard, that we would not have the same posture about it.

So I want to raise a question because we are talking about threats to the homeland and when you have a situation where ports of entry for instance like JFK Airport has far fewer workers, CBP officers, than they had prior to 9/11 working on a given shift. You have hundreds if not thousands of people coming through customs. They are waiting in a very—about the size of this room, maybe a little bit bigger, to go through and be documented and be screened.

You have people waiting there for 2 and 3 hours and mayhem breaks out and you have got like four guys sitting there. Is that not a threat? Does not that—something like that—pose a problem for us as a Nation and how do we bring efficiency, how do we bring balance to what we are looking at?

When people are able to walk around a CBP officer and leave undetected the airport and then we find out that, you know, there is a superhighway within our communities of drug flow, of gun flow.

Isn't there some connection that we should be looking at in terms of threats to the homeland? I am raising this because I am a bit concerned—I have heard all of you speak to the threat of terrorism but terrorism is one aspect of homeland security and we are so fixed on it as we should—listen—well, I have been through two terrorist attacks.

My father worked for the Port Authority, so I am not looking at this as someone who doesn't understand what terrorism is, but I have also been in City Hall when my colleague was gunned down. So I know what illegal handguns can do.

How do we look at this comprehensively and how do we raise, stand up this agency, so that it does what it needs to do without excuse, without equivocation?

Because what I am hearing here today is that well we are going to do more with less. Well, you know what, we invested in IC about one, two, three, four, five, six technology deployments for the Southern Border at the cost of billions of dollars that never worked, that never worked.

Yet my airport is a powder keg ready to explode. I am putting this out there just a little frustration. I wanted to raise it with you because I wanted to get a sense from you of, you know, what do we really see as the role of CBP?

If they are not the first line of defense than who is? That is one question. I will have you answer that and then I will come back with my next.

Admiral ALLEN. I will take a stab——

Ms. CLARKE. But if you can just share with me your——

Admiral ALLEN. If I could maybe provide a little context. What you are talking about, terrorism, drug trafficking, trafficking human beings, trafficking and guns, what you are really talking about is illicit trafficking that produces financial resources that perpetuate criminal activity. Now I would classify terrorists as political criminals.

All of these networks require money to continue to operate and I didn't discuss it specifically, but I think one of the challenges facing the Department and the country right now is how to deal with these criminal networks by attacking a network with a network.

When we talk about cyber, we talk about defending a network with a network. I think we need to understand that these threats start to pass organizational boundaries that a lot of our traditional law enforcement agencies are created for one specific threat; DEA in drugs; ATF in guns, and so forth.

What we need to understand is moving ahead in this country and dealing with either criminal activity, terrorist activity—we have got to start breaking down the barriers between agencies that are being constructed to attack one problem, put the information together, and attack a network with a network.

Ms. CLARKE. Isn't that what DHS does? Isn't that their role?

Admiral ALLEN. That gets back to the high-performance computing data analysis, information sharing, breaking down IT stovepipes, coming up with a common operating, common intelligence picture. I think it is a major challenge for the Department.

Mr. LEITER. Congresswoman, I will be a bit provocative back. Without disagreeing with you that you of course have to have adequate staffing to deal with whatever threat you see, first of all, we shouldn't be looking at the Department as having counterterrorism resources. I agree with you. They have border protection and security resources and those should be applied equally across different missions.

In most cases, not many things are actually specialized and cut down one mission area. You can work all of these security threats, but the place where I will be a bit more provocative is I think you have very little sense of whether or not security at Kennedy Airport has been increased because there are four people or eight people there at the border.

What we learned in the case of Umar Farouk Abdulmutallab on Christmas day in 2009, is that if we are waiting to screen these people once they get to JFK, we have probably already lost the fight.

So I would go to Admiral Allen's point. The question is: How is the National Targeting Center for CBP doing in screening these travelers before they even get there, either stopping them from getting on a plane and arriving at JFK or knowing which ones they have to screen additionally?

So I do think it is more than a uni-dimensional look at the number of people that are at that airport.

Mr. WALKER. Yes. I would say don't focus on how many people they have and how big the budget is because that is not necessarily indicative of outcome-based results. I will give you some examples.

We spent two-and-a-half times per person for health care. We spent two-and-a-half times per person for K–12 education, and we get poor results. We are not top 25 in the world, okay.

If you look at the Defense Department, I can assure you that the Defense Department has a huge amount of waste, a huge amount of waste, and they are going to have to be cut too.

But it comes back to what a lot of us have been saying. You need a plan, you need a comprehensive and integrated plan. You need to define risk and measure risk. You need to determine what are you trying to accomplish and how do you measure success in that regard, and you have to allocate your limited resources, whatever they are, to try to accomplish the most with what you have; focus on outcomes. I think there is clearly room for improvement there.

Ms. CLARKE. Thank you, Mr. Chairman.

Chairman MCCAUL. I thank the witnesses for their valuable testimony.

The record will stay open for 10 days pursuant to the rule.

Without objection, this committee stands adjourned.

[Whereupon, at 12:27 p.m., the committee was adjourned.]

○