AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DEPARTMENT OF HOMELAND SECURITY INTELLIGENCE AND BORDER SECURITY: DELIVERING OPERATIONAL INTELLIGENCE

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 28, 2006

Serial No. 109-89

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

34-854 WASHINGTON : 2007

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

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, NEW YORK *(Ex Officio)*

ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENT

The Honorable Rob Simmons, a Representative in Congress For the State of Connecticut, and Chairman, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment 1
The Honorable Zoe Lofgren, a Representative in Congress For the State of California and Ranking Member, Subcommittee on Intelligence, Informaton Sharing, and Terrorism Risk Assessment 2
The Honorable Bennie G. Thompson, a Representative in Congress For the State of Mississippi, (ex officio) 4
The Honorable Mark E. Souder, a Representative in Congress For the State of Indiana 12
The Honorable Jim Gibbons, a Representative in Congress For the State of Nevada 16
The Honorable Jane Harman, a Representative in Congress For the State of California 20
The Honorable Nita M. Lowey, a Representative in Congress For the State of New York 38

WITNESSES

PANEL I

Mr. Charles E. Allen, Chief Intelligence Officer, Office of Intelligence and Analysis, U.S. Department of Homeland Security:
Oral Statement 6
Prepared Statement 7

PANEL II

Mr. L. Thomas Bortmes, Director, Office of Intelligence, Customs and Border Protection, U.S. Department of Homeland Security:
Oral Statement 31
Prepared Statement 33
Ms. Cynthia O'Connell, Acting Director, Office of Intelligence, Immigration and Customs Enforcement, U.S. Department of Homeland Security:
Oral Statement 27
Prepared Statement 29
Mr. James Sloan, Assistant Commandant for Intelligence, U.S. Coast Guard, U.S. Department of Homeland Security:
Oral Statement 22
Prepared Statement 23

PANEL III

Mr. Michael W. Cutler, Fellow Center for Immigration Studies:
Oral Staement 44
Prepared Statement 46
Mr. Michael O'Hanlon, Senior in Foreign Policy Studies, Brookings Institution:
Oral Statement 48
Prepared Statement 49

Page

QUESTIONS FOR THE RECORD

Questions from Representative Rob Simmons for Assistant Secretary Charles Allen 60

DHS INTELLIGENCE AND BORDER SECURITY: DELIVERING OPERATIONAL INTELLIGENCE

Wednesday, June 28, 2006

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

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Souder, Gibbons, Dent, Lofgren, Harman, Lowey and Thompson (ex officio).

Mr. SIMMONS. A quorum being present, the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment will come to order.

Today the subcommittee meets to hear testimony on the Department of Homeland Security's border security intelligence operations. One of the Department's primary jobs is to secure the homeland against the illegal entry of people, goods and illicit materials. The 9/11 Commission wrote in their comprehensive study, and I quote, targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations and law enforcement in a strategy to intercept terrorists, fine terrorist travel facilitators and constrain terrorist mobility.

DHS works to do this through the hard work of people, through U.S. Customs and Border Protection, Immigration and Customs Enforcement and the United States Coast Guard, among others in the intelligence and law enforcement communities. But as we all know, thousands of people illegally stream across our international borders.

The 9/11 Commission estimated that annually approximately 500,000 people enter this country illegally, without inspection, and overstay their legal welcome. Many come for opportunities that America provides, and we understand that, but others have a more sinister intent. In order to better protect our borders, we need to know who is attempting to cross, and what are they bringing into this country, and why.

Our border immigration and Coast Guard officials protect more than 5,000 miles of the border with Canada, 1,900 miles of border with Mexico, and approximately 12,400 miles of shoreline east and west. To protect this vast international border, intelligence-driven

operations will be the key to targeting and interdicting these threats before their arrival.

On a typical day Federal officials will apprehend over 3,000 people trying to cross between ports of entry, and on a typical day will intercept one person for terrorism or national security-related reasons. These apprehensions net fraudulent documents and seemingly innocuous pocket litter, both of which can have tremendous intelligence value. Therefore, DES frontline operators must have the tools, the training, capability and processes in place to weave the information from these everyday encounters into a comprehensive intelligence picture.

In addition to those who try to cross our borders illegally, on a typical day approximately 1,200,000 people and passengers arrive at our ports of entry, and approximately 80,000 shipments of goods arrive for approved entry. Nothing wrong with this, we want to encourage this. And we must make sure that this lawful travel and lawful commercial activity proceeds efficiently, without undue delay, while focusing again on those who deserve additional scrutiny. It is a daunting but necessary task.

Today we will hear from Charlie Allen, the Chief Intelligence Officer of the Department of Homeland Security, who will give an overall perspective of the Department's strategic intelligence efforts and his support to DHS operational components. Again, welcome, Mr. Allen. This task is a huge task and a new task for United States as Americans.

Next we will hear from the Coast Guard, the Customs and Border Patrol and the ICE on how they incorporate intelligence into their operations, and on how the Office of Intelligence and Analysis is supporting their efforts.

And then finally, our third panel will consistent of Mr. Michael W. Cutler from the Center for Immigration Studies, and Mr. Michael O'Hanlon from the Brookings Institute, who will provide the subcommittee with their perspective on how intelligence can best be used to secure and control America's borders.

Mr. SIMMONS. The Chair is now happy to recognize the Ranking Member of the subcommittee, the gentlelady from California, Ms. Lofgren for her opening statement.

Ms. LOFGREN. Thank you, Mr. Chairman.

While I am pleased that we are finally turning our attention today to the question of intelligence and border security, I must say, Mr. Chairman, this hearing and other hearings the Republican leadership has scheduled in the next few months are a day late and dollar short—correction, we are 6 years late and millions of dollars short.

President Bush took office in 2001, and this Congress has been controlled by Republicans since 1995. The Senate, with one exception, has had a majority of Republicans since 1995. The Federal Government, charged with making and enforcing the laws of this Nation, have been under the sole control of Republicans for the last 6 years.

With complete control of legislation and enforcement of the law for 6 years, you would think that a party that now calls so vigorously for border security and enforcement of immigration law could have solved the problem of illegal immigration by now, but, Mr.

Chairman, the Republican Party seems to be all talk on this subject.

Here is just a partial list of the failures presided over by the Republican majority on illegal immigration.

Since 1996, when the Senate and the House were taken over by the Republican Party, 5.3 million undocumented immigrants came to the United States. Since 2003, when President Bush came to power, over 2 million undocumented immigrants have entered the United States.

In 2004, Congress enacted the Intelligence Reform Act, or the 9/11 Act, which mandated an additional 2,000 Border Patrol agents being hired over each of the next 5 years. But the President's subsequent budgets and Congress have failed to include adequate resources to implement the act. Indeed, the President's fiscal year 2006 budget called for only 210 additional Border Patrol agents. In fiscal year 2006, the Congress, with both House and Senate controlled by Republicans, eventually funded only 1,000 additional agents.

The 9/11 Act also mandated an additional 800 immigration enforcement agents over each of the next 5 years, and yet for fiscal year 2006, the Congress funded only 350 additional agents. The act also mandated an additional 8,000 detention beds, but for fiscal year 2006, the Congress funded only 1,800 additional detention beds.

President Bush and the House Republicans continue to underfund the Border Patrol. The President's fiscal year 2007 budget does not fully fund the authorized levels for the Border Patrol.

During the Bush administration, Catch and Release has been rampant, a program under which 12,000 undocumented immigrants each month are apprehended from countries other than Mexico and are released and allowed to live in the United States while awaiting a deportation hearing, yet the Federal Government, which is completely controlled by Republicans, 70 percent of the OTMs are released into the interior with notices to appear at a later date and are never heard from again.

According to the Washington Post, between 1999 and 2003, worksite enforcement operations were scaled back 95 percent by the Immigration and Naturalization Service. The number of employers prosecuted for unlawfully employing immigrants dropped from 182 in 1999 to only 4 in 2003. And fines collected declined from $3.6 million to 212,000. In 1999, the United States initiated fines against 417 companies; in 2004, it issued fine notices to only three.

Next to nothing has been done to secure our northern border at a time when 17 suspected terrorists were arrested in Toronto, and there are reportedly 50 terrorist groups in Canada. The millennium bomber was arrested as he attempted to cross the northern border with explosives, and the Congressional Research Service says that Canada is, quote, "a favored destination for terrorist groups as a safe haven, transit point and place to raise funds."

While the Republican leadership in Congress focuses on the southern border, with 10,000 Border Patrol agents stationed along a 2,000-mile border with Mexico, only one-tenth of that amount is on the Canadian border, a border that is 2.5 times as long as the

Mexican border. Recent news stories state that people drive, walk, sail, ski and sled across the northern border all the time.

On December 16, 2005, all 219 House Republicans voting that day opposed a proposal, the Democratic motion to approve border security and immigration enforcement by fulfilling the 9/11 Commission's border security recommendations. The proposal would have hired more border guards; ended the Catch and Release practice by authorizing 100,000 additional detention beds; and incorporated state-of-the art technology, including cameras, sensors, radar satellites and unmanned aerial vehicles in order to ensure 100 percent border coverage.

In 2005, all but one Republican voted against a comprehensive Homeland Security proposal that would commit 41 billion to securing the Nation from terrorists, 6.9 million more than the President's budget. In 2005, all but two Republicans voted against an effort to add $284 million to an emergency spending bill for securing the Nation's borders.

Mr. Chairman, there has been a lot of talk about immigration these days, tough talk, but the pattern is talk and not action. And I say this because I have been made aware that there is a schedule—and this hearing, I think, is on that schedule, and I was on a hearing last week that was part of this schedule—to raise the issue of immigration, and I think the Republican leadership has made it a political issue. There was the hearing in the House Administration Committee last week; this hearing today; on July 5th, the hearing from the House International Relations subcommittee in San Diego, the Senate Majority is on it; July-h, another hearing in Laredo, Texas; mid-July a hearing, House Education and Workforce; August 14th, Government Reform and the like.

So I am quite skeptical that this hearing on border intelligence is more than talk. It seems to me this is just another long list of the hearings held and planned by the Republican-led Congress that does not lead to solutions to a problem that the American public cares about, and I thank the gentleman for recognizing me.

Mr. SIMMONS. Yes. And I think some of the items that you have listed in your opening statement are just the reason why we are having this hearing today, so that we can hear from our Chief Intelligence Officer how he is working to incorporate the various components of the Department of Homeland Security intelligence to better address this important issue. And I think we understand it is an important issue, and we look forward to their testimony, and hopefully their statement of progress in these difficult issues.

And now the Chair would like to recognize the distinguished Ranking Member of the full committee Mr. Thompson of Mississippi for any statement he would like to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman and Ranking Member. I appreciate the opportunity to participate in this hearing.

Always nice to see my friend Charlie Allen. First day of work he came by, and it has been a good relationship so far. I appreciate you, Mr. Allen.

But for the sake of this hearing today, Mr. Chairman, we really should have been talking about border intelligence 5 years ago

after 9/11. If we had conducted oversight and border intelligence during that time, we could focus legislation more adequately on what our problems are now. More importantly, it would have given us some meaningful starting point when taking up border security legislation.

Essentially we have a bill pending now that is not informed by what is known at the border. This Republican Congress passes bill after bill—and I have five different bills that we have passed on border security, Mr. Chairman—and nothing has happened with them. If we are going to do top-notch border intelligence, it is essential that we develop a risk-based approach to border security.

The United States has 216 airports, 143 seaports, and 115 land border crossings that are official ports of entry. Screening all the people and goods coming through these busy ports is already an enormous resource challenge for the men and women of the Department of Homeland Security. I have serious concerns that they lack the resources necessary to obtain true situational awareness at these locations, not to mention among the many hundreds of miles of unguarded rural and remote border locations.

As we know, the threat to our northern border was thrown into sharp relief with the arrest of an apparent terrorist sailor in Toronto. This administration has failed to adequately secure our northern border by the fact that the northern border is more than twice the length of the southern border, with only one-tenth of the agents.

State, local and tribal law enforcement is uniquely situated to help out with border intelligence where resources are stretched thin. What I am hearing from police and sheriffs' offices, however, worries me. When it comes to border security, the Department should have an all-hands-on-deck attitude. Instead, I hear CBP holds back information from local law enforcement because they view locals as competitors. Some local officers tell me that if they arrest someone coming over the border illegally, CBP headquarters sees it as a black eye for them.

Making matters worse, officers in northern border communities have told me that they often receive more specific and actionable information from their Canadian colleagues than they do from the Department. Add to this the fact that border security is a Federal responsibility, Mr. Chairman, and yet this administration has passed the buck to State and local authorities in some areas, relying on them to do its job, without providing adequate support.

Whether it is a turf issue, a resource issue or something else, this is unacceptable. CBP, ICE and the Coast Guard need to adopt common and consistent practices to share information with all their border security partners. While I had high hopes for the Homeland Security information network as a key way to communicate with State and locals, moreover, I am troubled about a Department report yesterday that found that most officers either don't trust it or don't think it contains much useful information.

This hearing, therefore, is both important and timely, Mr. Chairman. This administration has dropped the ball on border security by underfunding critical programs for recruiting Border Patrol agents, leaving large planks of our border vulnerable in not procuring sufficient detention beds. Constructive and thoughtful

Democratic amendments that seek to fill these critical gaps have been rejected time and again, and now we face a possible intelligence breakdown on our borders. How we proceed from here will have a big impact both on how we go about securing our border, and ensuring that our immigration laws are fully enforced.

I welcome all the witnesses and look forward to your thoughts on these critical issues. I yield back.

Mr. SIMMONS. I thank the Ranking Member for his comments, and I agree with him completely. I think this hearing is important, and I think it is timely. Other Members who are present know that they can submit opening statements for the record.

Mr. SIMMONS. We will move now to the first panel. The Chairman calls the first panel, which is assembled; recognizes Mr.Allen as our Chief Intelligence Officer of the Department—of the Office of Intelligence and Analysis, who reports directly to Secretary Chertoff. In this role, he is responsible for coordinating with the Intelligence Community and providing guidance on Homeland Security intelligence issues.

Mr. Allen has a long and distinguished career in the U.S. Intelligence Community, beginning in 1958, when he joined the Central Intelligence Agency. He has subsequently held assignments of increasing responsibility within that organization, within the Office of Secretary of Defense, and he has served his country in a variety of other capacities.

Mr. Allen, welcome. It is good to see you again. We look forward to your testimony.

STATEMENT OF CHARLES E. ALLEN, ASSISTANT SECRETARY FOR INTELLIGENCE AND ANALYSIS, CHIEF INTELLIGENCE OFFICER, DEPARTMENT OF HOMELAND SECURITY

Mr. ALLEN. Thank you, Mr. Chairman, Ranking Member Lofgren and members of the committee. I am very grateful for the invitation to speak to you today. I am also gratified to appear alongside my colleagues from the United States Coast Guard; Customs and Border Protection; and Immigration and Customs Enforcement. As members of the Homeland Security Intelligence Council, which I chair, they have been invaluable partners in realizing the Secretary's vision of an integrated Department of Homeland Security intelligence enterprise.

I have a very brief statement, and I would request that my full statement be submitted for the record.

Providing intelligence support to border security is a subject that I have devoted considerable time and energy during my relatively short time as Chief Intelligence Officer of the Department. One of my first actions was to launch an intelligence campaign plan for border security. We began this process last October by holding a border security intelligence conference that enabled us to gain inputs from a wide range of Department of Homeland Security and Intelligence Community partners.

Since then we have worked on two tracks. On one track, we have taken concrete measures to deliver discrete, actionable intelligence to the men and women securing our borders. And although the need to protect sensitive sources and methods precludes my discussing these measures in detail today, I can tell you that members

of my office have drawn on the extensive experience in the Intelligence Community to help the Department get full benefit from national collection assets, and that is a process that was not evident before I came. We have changed that substantially.

On the other track, we have been developing a phased framework for sustainable intelligence support to border security. Our overall approach is to bring national intelligence to bear on the border, while at the same time fusing intelligence from border and immigration activities into an integrated threat picture, at first within individual sectors, but eventually across the length of the borders. The approach is consistent with ongoing operational efforts to push the border outward and to build a layered defense extending into the U.S. Interior.

As befits an office with department-wide responsibilities, my office has focused its own staff resources on strategic efforts, including the development of a department-wide intelligence, surveillance and reconnaissance architecture; establishing a border security analysis branch; and working with interagency partners to coordinate and streamline Federal intelligence efforts on the border.

Some of our efforts have had an indirect but strong effect on the delivery of operational intelligence in support of border security. Our plan for supporting State and local fusion centers envisions deploying DHS personnel, including intelligence officers, in a way that is most responsive to each center's particular need, including augmenting border security intelligence capabilities, if required.

Our work on enhancing the Homeland Security Information Network, which will invigorate an important channel for sending intelligence to and receiving information from the State and local authorities.

Finally, my office's development of an information architecture for the Department's intelligence enterprise will promote faster information sharing and greater interoperability, improving the delivery of operational intelligence in support of border security.

In summary, my office has been an active and effective advocate of intelligence support to border security, deploying our department-wide perspective and authorities and the particular skills of our officers on behalf of the entire DHS intelligence enterprise.

Mr. Chairman, I look forward to your questions.

Mr. SIMMONS. Thank you for that testimony.

[The statement of Mr. Allen follows:]

PREPARED STATEMENT OF CHARLES E. ALLEN

Chairman Simmons, Ranking Member Lofgren, Members of the Subcommittee,

Thank you for inviting me to speak with you about my role in providing intelligence support to border security. The subject of today's hearing is one to which I have devoted considerable time and energy during my tenure as Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer of the Department. I am gratified to appear alongside my esteemed colleagues from the Coast Guard, Customs and Border Protection, and Immigration and Customs Enforcement. As members of the Homeland Security Intelligence Council, which I chair, they have been invaluable partners in realizing the Secretary's vision of an integrated DHS intelligence enterprise.

When I arrived last September, the Office of Intelligence and Analysis already was leading a working group on intelligence initiatives in support of the Secretary's Secure Borders Initiative, or SBI. One of my first acts was to launch an Intelligence Campaign Plan for Border Security, or ICP, which Deputy Secretary Jackson introduced to General Michael Hayden, then the Deputy Director for National Intel-

ligence, on Sept. 27, 2005. We kicked off our planning efforts by holding a DHS Border Security Intelligence Conference on 24-25 October, 2005. This conference, held in a secure facility, enabled us to gather inputs from a wide range of DHS and Intelligence Community partners. It proved highly valuable to our subsequent planning.

Among the needed improvements we identified as a result of the conference were greater focus on strategic analysis; coordination and integration of analytic efforts at both the tactical and strategic levels; inclusion of DHS agent and inspector insight in collection and exploitation activities; better-defined areas of responsibility for information sharing; and dissemination of-and identified repositories for-relevant information.

Since then, we have worked on two tracks. On one track, we have taken concrete measures to deliver discrete, actionable intelligence to the men and women securing our borders. I would be pleased to describe some of these measures in a closed hearing, but the need to protect sensitive sources and methods precludes my discussing them in detail in this setting. What I can tell you is that my officers have drawn on their extensive experience in the Intelligence Community to help ensure that DHS gets full benefit from national collection assets.

On the other track, we have been developing a phased framework for sustainable intelligence support to border security. Our overall approach is to bring national intelligence resources to bear on the border while at the same time fusing intelligence from DHS border and immigration activities into an integrated threat picture-at first within individual sectors, but eventually across the length of the border. This approach is consistent with ongoing operational efforts to push the border outward and build a layered defense extending into the US interior. In addition we are maintaining focus on all of our borders to include the Northern Border and maritime domain.

In the first phase of the ICP, covering fiscal years 2006 and 2007, we will develop and implement a comprehensive strategy for collection and analysis of border security intelligence. During this phase, we will apply our intelligence resources and analytic focus in areas of immediate need. Our research will be comprehensive covering a broad range of topics associated with cross border violence with subcategories of human, drug, weapons, contraband smuggling and trafficking, transnational gangs, documentation fraud, and the violence these topics spawn on the border. The research and assessments we produce will include all agencies with responsibilities in these areas of interest. We will start with the southwest border, progressing to all borders based on threat assessments. We will review lessons learned from the first phase and make any programmatic investments and structural changes that flow from these findings. Finally, we will be on a sustainable footing, allowing us to push the borders outward while supporting interior enforcement.

I should point out that even though our planning efforts pre-date the President's decision to deploy the National Guard to the border, we are taking this deployment into account. We plan to collaborate with the National Guard to ensure its intelligence capabilities are integrated with the overall intelligence enterprise at the border, filling in shortfalls and laying the foundation for the post-deployment period.

As befits an office with Department-wide responsibilities, my office has focused its own staff resources on strategic efforts. In the area of collection and requirements, we are leading the development of a Department-wide intelligence, surveillance, and reconnaissance (ISR) architecture that will serve as the central nervous system of DHS intelligence. In the area of analysis and production, we have created a border security branch that is focusing research and analysis on a number of topics relevant to the border, including alien smuggling, counter-narcotics, money laundering, transnational criminal gangs, and identity theft and benefit fraud using travel documents. Finally, we are deeply deeply engaged in efforts to coordinate and streamline interagency intelligence efforts on the border, notably in El Paso, where three valuable intelligence centers, run by elements of three different Cabinet agencies, are exploring new ways to work together on their common mission of securing the border.

I wish to highlight several efforts of the Office of Intelligence and Analysis that will have an indirect, but powerful, effect on the delivery of operational intelligence in support of border security. First, my office has led the Department's development of a plan to support state and local fusion centers across the country. Our plan envisions deploying DHS personnel, including intelligence officers, in a way that is most responsive to each center's particular need. If the fusion centers in states along the border tell us they want particular support in partnering with the federal government on border security, we stand ready to deliver. Second, we have taken on the responsibility for enhancing the Homeland Security Information Network, an important channel for sending intelligence to, and receiving information from, state and

local authorities. Third, we are developing an information architecture for the DHS intelligence enterprise in order to promote faster information sharing and greater interoperability-characteristics that undoubtedly will improve the delivery of operational intelligence in support of border security.

In conclusion, I believe we have been an active and effective advocate of intelligence support to border security, deploying our Department-wide perspective and authorities and the particular skills of our officers on behalf of the entire DHS intelligence enterprise. I look forward to answering your questions.

Mr. SIMMONS. And in my opening statement I made reference to the fact that we have a 5,000-mile border with Canada, an undefended or demilitarized border with Canada; 1,900 miles of border with Mexico, again, a demilitarized or undefended, in some respects, border with Mexico; 12,400 miles of shoreline. This geography presents a vast challenge.

I think back to my experience, my service in Asia, working on the Great Wall of China, thinking about the logistics and expense of creating such a great wall and then reflecting on the fact for all that effort, it actually did not work; it did not keep, if you will, the barbarian hordes from penetrating that country.

So my point of view has always been very simply stated. We need to be intelligent about how we control our border. We need to focus and target our intelligence assets so we are at the right place at the right time, doing the right things against the right people.

Some of my colleagues, as you have heard from their opening statements, give the impression that nothing has been done. Of course, in the Intelligence Community it is often best not to be on the front pages of the New York Times; I think we understand that. But from your perspective, how have we been focusing our intelligence assets to this problem, and what successes do you feel that we have had over the last several years—or at least since you have been in office, which is a relatively short time?

Mr. ALLEN. Yes, Mr. Chairman. That is an excellent question because this is a very difficult, multifaceted, multidimensional threat, and trying to secure all those lengthy borders is a very large challenge. But I think we have to do it in a couple of ways. And my colleagues, who will speak later, will speak on specific operational successes and programs on which they are engaged.

What I see has been lacking is a good intelligence analytic baseline to understand the threat thoroughly, to look at the border holistically. We cannot break it into simply the legal movement of goods and people, narcotics, human smuggling, trafficking, contraband, potential of WMD being smuggled across the border, terrorism, and illegal immigration. We have to look at a secure border process.

Under the Homeland Security Act, the Secretary of Homeland Security is charged with developing secure borders, and I think we have to look at it in a way that we have not looked before. One of the things that I have done since we have arrived is establish a border security branch that is going to be quite substantial in order to understand the threat, the drug smuggling, the alien smuggling, and the financial transactions, including money laundering. So we are going to have to take a very strategic look at this problem that we have not done previously.

The other issues that we have to bring to bear is all of the capabilities of the national Intelligence Community on to this problem. And there is a lot that can be done through the various intelligence

collection capabilities. I don't have the power to collect intelligence, as the Chief Intelligence Officer, although the DHS operating components can collect information as part of their operational and law enforcement duties. But I do have the right to develop the collection requirements and priorities, which we are doing, and for the first time we have a set of priorities which we would be happy to talk about in a closed session.

We also are developing new capabilities within the GEOINT. General Clapper, who just left NGA; there are things we have done that are totally unprecedented within the area of other intelligence collection capabilities. As I said in my opening comments, we are developing an intelligence, surveillance, and reconnaissance plan to deal with border security, and working very closely with General Maples over in the Department of Defense, and General Cartwright at the Strategic Air Command. All of these things we have done in the last 3 or 4 months. And as I said, when I came in, we did not have an intelligence campaign plan against the border. The Secretary and Deputy Secretary of Homeland Security directed me to do so. And I think we are in the opening stages of developing that overall strategic picture and landscape. My colleagues will talk to you in specific terms of successful operations.

I agree with you that we should have done more earlier, but we are not at this vigorously. I have a weekly stand-up, and believe me, those are rough stand-ups. Of all of my people—

Mr. SIMMONS. Mr. Allen, before my time runs out, in all of these activities are you preserving and protecting civil liberties and rights of people across our borders?

Mr. ALLEN. Absolutely. This is something of which we are very concerned. Civil liberties and civil rights, privacies are all taken carefully into account. Everything we are doing were done under the careful scrutiny of my legal staff as well as—and my colleagues can talk about their lawful activities. But everything we do is absolutely lawful. And we certainly are looking at special interest aliens from certain countries that could have not only just alien smuggling, but perhaps terrorism connections.

Mr. SIMMONS. The Chair now recognizes the Ranking Member.

Ms. LOFGREN. Thank you, Mr. Chairman.

And it is good to see you, Mr. Allen. Certainly your reputation in the Intelligence Community is a sterling one, and I am glad that you are in the job that you have. However, as you have only been there a short period of time, as we all know, so would it be accurate to say that you have—obviously no plan is ever completely done. Even when the plan is done, it must be continuously updated, but would it be accurate to say that you have completed the comprehensive DHS border intelligence plan, including CBP, ICE and the Coast Guard, or is that in progress still?

Mr. ALLEN. Congresswoman, that is still in progress. We are still—in my view, we are only in midstream in getting that overall plan together. I have seen a lot of vigor on the part of the individual operating components, but we have to work this as an integrated process. As you know, there are a number of initiatives. There is a Southwest Counternarcotics Border Strategy in which we are participating. It is a very layered approach.

One of the things we are looking at is the information flows and trying to ensure that as we acquire information, we provide the information to the border—to the Customs and Border Protection. And we obviously have to improve those connectivities and the flow of information. We have a good deal to do, but I have some good ideas on how to get this done.

Ms. LOFGREN. I am sure that you do. Can you tell us, if you know, why this wasn't done before you got here?

Mr. ALLEN. Well, I think the real issue is bringing the Department together, bringing all these various agencies and operating components together, many of which have somewhat overlapping roles, but never ensuring there is a close collaboration, integration. I meet every week with the gentlemen and ladies who will be speaking later from the operating components, and we have 2 hours of just talking about how we can integrate our efforts toward the borders and towards training together, developing our analytic expertise together. And these are very tough sessions, but we are getting things done.

Ms. LOFGREN. As you know, 17 suspected terrorists were recently arrested in Toronto, and there are reported—I don't know if it is accurate—at least 50 terrorist groups in Canada. And we know that the only reported terrorist caught at the border was the millennium bomber arrested at the northern border as he was—with explosives, and a Congressional Research Service says that Canada is the favored destination for terrorist groups as a safe haven, transit point and place to raise funds.

Now, we have gone over that there are 10,000 Border Patrol agents stationed along the 2,000-mile border with Mexico, and we still have problems with illegal immigration with that level of patrol, but only one-tenth of that amount is on the Canadian border. That border is 2.5 times as long as the Mexican border. And I know it would be incorrect to assume that those 1,000 agents are really on the job because it is a post position. If you look at 24 hours a day, at any given time you have got between 200 and 300 people on that whole border. And we have had reports that people drive, walk, sail, ski, sled, crawl—and probably a few other things—across the border with impunity.

Does the comprehensive border plan that you are putting together address that gaping hole in border and national security?

Mr. ALLEN. Yes. Our intelligence campaign plan would also include our northern border. We are very much concerned about our northern border. I believe that Ambassador Negroponte spoke indirectly to it in his hearing in front of the Senate Select Committee on Intelligence when he did his worldwide threat. I just met with Ambassador Negroponte and Stockwell Day, the Minister of Public Safety up in Canada. We certainly have some common interests. We are very impressed with what the Canadians have done in dealing with extremism. But this is an issue, and any nexus with the United States is of great concern to us. We obviously need to ensure that we work at this much harder.

I just met with the head of the Border Patrol of Canada. We and—the head of the Border Patrol is a woman. We have agreed that we will work harder to look at issues where we should do common cause to better secure our border.

The northern border is very different from the southern border, and we need new tools, techniques and methods to help make the border more secure.

Ms. LOFGREN. Just before my time is up, do you think 200 Border Patrol agents on a 5,000-mile-long border is sufficient?

Mr. ALLEN. I think we need substantial resources on all our land borders. And I am very impressed with what our U.S. Coast Guards have done with our maritime borders. We obviously have to spend a great deal of time and attention with our northern border as well as our southern border.

I have spent time with our southern borders. I have just made a very good trip to Mexico City where we had some very strong discussions on how to work harder on particularly special-interest aliens, people who might be involved in terrorism, and we are getting good cooperation in the south.

Ms. LOFGREN. Thank you, Mr. Chairman. My time is up.

Mr. SIMMONS. The Chair recognizes the gentleman from Indiana Mr. Souder.

Mr. SOUDER. First I would like to make a couple of brief comments on the northern border. Clearly, coming from the Midwest, I am concerned about the northern border, but it is a little bit different than the southern border. One thing is we work with the Canadians on harmonization of immigrationwise. I have met teams along the border. They are taking down groups in Canada, the millennium bomber himself, and working with the RCMP.

We have had open testimony in this committee from Mr. Garcia about the 10- to 12,000 that it usually takes to smuggle a Hispanic across the southern border, and that there are areas along the southern border where it is 30—to 35,000 to smuggle a Middle Easterner. But since we have no real knowledge of what is coming into Mexico, east, west or from the south, and they don't have functional control of their country, and we don't have functional control of our south border, that is partly why we focus so much on the south border. We do need attention in the north border, in fact, because so many Middle Eastern natives in Canada and citizens of the U.S. live in Detroit and Buffalo, Toronto and Montreal. That is clearly a pressure zone, but it is not exactly the same as the south border.

I had a couple of questions. One is kind of simplistic, but it has been an increasing frustration of mine. It seems like often our agencies are spending more time meeting with each other to try to coordinate their intelligence than trying to figure out who the bad guys are.

I have a very simple question: Given that we will probably never eliminate all stovepiping, and given the fact that so many of the different intelligence subgroups have somewhat different goals, in addition to terrorism they have a multiplicity of goals and focusing on different things, what I am wondering is if you are a border agent at any of the official border crossings, and you have an ID and the name comes up, is there a pop-up, just a signal? If the Department of Defense doesn't want to share certain intelligence, if the CIA doesn't want to share certain intelligence, if different parts of DHS have different intelligence in all this that pops up and says this is a person of interest, do we have enough harmonization of

our intelligence agencies that even if they don't want to share the information, that if a name hits the border system, a pop-up occurs?

Mr. ALLEN. I think—and I will let Customs and Border Protection, Captain Bortmes, speak to that later, but I, having visited the Border Patrol and spent time with it in two sectors and traveled with Congressman Reyes to El Paso, I am convinced that databases, as names are checked, those are done very quickly and very efficiently. And believe me, having come from the Central Intelligence Agency, there is no information if it involves the security of the United States that can be withheld by CIA or anyone else in getting that information. If it needs to be sanitized and declassified, that can be done if it deals with personalities of interest to the Border Patrol.

Mr. SOUDER. So you are saying that you are confident that—because I ran into a case in my area that we have. It was a new category of people we are watching as opposed to our watch list; in other words, they haven't done anything wrong, they are not even a suspect, but they are doing certain behaviors. You are confident that each branch of the government, that if they have someone that they have some interest in, they may not have an arrest warrant out, they may just be trying to trap them, that all those names are in a system, in a computer system, that if that person crosses a border entry, that some warning will come up to say hold this person, here is the agency you contact.

Mr. ALLEN. I am not confident that every database that has a potential person of interest would be immediately available to the Border Patrol. But the Border Patrol does have an ability to check to see if there is a potential record that would indicate that individual has engaged in something nefarious or has connections with terrorism.

I think they do a good job. There are people turned away every day at our borders. I am sure Mr. Bortmes can speak more directly about this, but I do believe that this is improving. Database management is a very hard problem for the U.S. Government, and particularly for the U.S. Intelligence Community.

Mr. SOUDER. Because this isn't a question of whether the Border Patrol is doing their job, or CBP, this is a question about is the information getting to them with which to do this job, which I know we are pushing towards, but it is really hard to get all these agencies to share complete information, and if they won't share it, if they would at least share the name so that people can get back to them.

I have one other question. How do you see AMO fitting in Riverside? The maritime center.

Mr. ALLEN. Out in California?

Mr. SOUDER. Yes.

Mr. ALLEN. Well, we are working closely with AMOC, that is a center there. We are providing them with strategic information. Through our initiatives and building requirements, we have provided them with data that they have never received in the last 2 months. In fact, they say they are inundated with some of the information that using national NTM systems that they never had

access before. So we are starting to make progress. We are not where we should be, sir, but I am pushing it every week.

Mr. SOUDER. Thank you. Because it is clear that the area you are working in is the underpinnings of everything else we do, because good intelligence and actionable intelligence is how we are going to prevent things. Thank you for your work.

Mr. SIMMONS. I believe I just got a call for a vote, but we have time for an additional—a couple of sets of questions, I believe.

The Chair recognizes the Ranking Member Mr. Thompson.

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

Mr. Allen, are you aware of CBP being accused of holding back information to local law enforcement agencies?

Mr. ALLEN. No, sir, I am not. And I would—I will let Mr. Bortmes answer that question when he appears on the second panel. Unless it is for some reason sensitive law enforcement case—investigative case information, one would think that information would not necessarily be held back in ways that would not be effective.

Mr. THOMPSON. So you would agree that the sharing of information between agencies is a must, from an intelligence standpoint.

Mr. ALLEN. It absolutely is. That is where I am—as you know, Congressman Thompson, that is where I am spending a lot of my time. We are putting people—Secretary Chertoff has just approved my implementation plan for putting my officers out with State fusion centers—and, in fact, I want to put them out in every fusion center—in order to help both the sharing of information from the national Intelligence Community down at the lowest possible level to the local level.

Mr. THOMPSON. Can you give me our analysis of where CBP, ICE and the Coast Guard is with regard to the common sharing of intelligence with other State and local partners?

Mr. ALLEN. Well, I would defer to them, but we have become—for State and local fusion centers, we have become—my own office has become sort of the centerpiece, the executive agent for the Department for the flow of information down to State and local level. I am sure there is information shared at the local level by all the operating components, and I should let them speak directly to that.

Mr. THOMPSON. So your job will be to manage the fusion center?

Mr. ALLEN. To ensure that there is a flow of information down to the State fusion centers and to the major city fusion centers. We are in the process of doing that and in the process of deploying officers to those centers. We have deployed them to Los Angeles, New York, Louisiana, Maryland, and we are sending an officer to Georgia and to Virginia in the near future.

Mr. THOMPSON. And the goal of those centers is to have some common thread of intelligence available to all parties?

Mr. ALLEN. Yes, sir. Those are under State or city control. And our job is to coordinate the flow of Federal information down to those centers and to ensure that they have all the information that they need in case there is some risk or danger to that particular State or that particular city.

Mr. THOMPSON. Well, with respect to border intelligence, will we have CBP and ICE agents in those fusion centers also?

Mr. ALLEN. That is a decision I think that the head of the operating component must make. We certainly will have officers from DHS there. They obviously, and JTTS, the Joint Terrorism Task Force, that is managed by the FBI, and they are there in many places, and they do a tremendous job in working and sharing of information.

Mr. THOMPSON. If it was left up to you, would you have one there?

Mr. ALLEN. I am not sure. I think that if we have the right small number of officers there—and certainly officers from ICE or CBP could come down to a fusion center working for the Chief Intelligence Officers as part of his outreach to State and local governments. I would like that very much. The Secretary has designated me and my office as executive agent for the Department in the flow of information to State and local governments.

Mr. THOMPSON. Well, since we are talking about border intelligence—I will have some other questions, Mr. Chairman, I will submit for the record.

Mr. THOMPSON. But, Mr. Allen, the only other question I have for you is, are you aware of the IG report that came out yesterday with respect to the Homeland Security Information Network?

Mr. ALLEN. Yes, sir, I am aware of it. I have not read it. I have asked my information management officer to send it to me. The Homeland Security security network is run by the operations director at the Department.

Mr. THOMPSON. But you also—there was some—well, you have not seen it, but there are some weaknesses.

Mr. ALLEN. Yes. And one of the things that we have been doing—and let me just say on the classified side we are doing three things. One, on the Homeland Security Information Network I have put in an intelligence portal for sensitive but unclassified information to go to State and local governments. We have run some experiments, and we have gotten good reception on that.

Two, I took over a very broken Homeland Security Information Network system. We have fixed that to almost every State and fusion center.

And three, we are forming a Homeland Security data network, which will be a more robust—a more robust classified network. We are in the early stages of doing a pilot test on that. We have every intention of doing that.

Very candidly, Mr. Thompson, we have been behind in our information management, and I am not happy with it, and I know that the Secretary isn't either.

Mr. THOMPSON. I yield back, Mr. Chairman.

Mr. SIMMONS. I thank the gentleman.

For the record, we have a motion to adjourn on the floor. I will keep the hearing going. Ms. Harman is going to go vote and return. I think there is adequate time for the gentlelady from New York to ask her questions of Mr. Allen, and we will try to keep this moving along.

Mrs. LOWEY. Thank you very much, Mr. Chairman.

And I thank you, sir, for your presentation. And I particularly appreciate your focus on fusion centers.

I met with the head of the New York State Department of Homeland Security just last week, and one of the points he unfortunately shared with me is that the communication between the Federal Government and the local officials in New York is mediocre at best. So, number one, I would appreciate if you would comment on that and what is being done to improve upon it.

And secondly, there are three fusion centers, as you know, in New York. There is one in Albany, there is New York City Police Department, and there is one in Rockland County. I know Westchester is in the process of putting one together, but there isn't one now.

I am very pleased that you talked about placing your people in these fusion centers. Perhaps you can continue to expand on that. How fast is this moving? Are you getting support for doing that? Perhaps you can focus specifically on New York. I happen to have an interest in it; it happens to be my district. What is happening there? And if the New York State Department of Homeland Security said there is inadequate communication, what are you doing; what can you do; what will you do to improve upon it?

Mr. ALLEN. Well, I thank you for the question because New York City—New York State, and New York City in particular, has been a focus right from the moment I arrived. I will soon have three officers in New York City working with the Intelligence Division and with the Counterterrorism Division. I have a general liaison officer there now full time. We are going to send up two very experienced all-sourc intelligence officers to help in mentoring and teaching in New York City. Mr. David Cohen and Larry Sanchez are very strong on this.

Mrs. LOWEY. Didn't David originally come from New York?

Mr. ALLEN. Well, his wife is from Brooklyn. He came from Boston. He still has a Bostonian accent. But he is a New Yorker, he truly is. And up in Albany we have a UNYRIC where we work very closely. And I have a team in UNYRIC this week. I intend to put a full-time officer in UNYRIC, there is no question about that. My principal deputy, I have an outsider, Jack DiMaggio, who spends his full time working to get our officers out to the various fusion centers.

Albany—at this stage we do not have plans to put anyone in Rockland County, but we do have—we will put people in Albany. And I respect that Homeland Security advisor. We are going to improve our communications flows. When we have a threat into New York, we always call the Homeland Security advisor. We call him on the unclassified line if it is an open issue, but if it is classified, we have secure communications. And Homeland Security has made certain that the UNYRIC as well as New York City has classified capabilities.

I have substantially augmented cryptographic capabilities for New York City so that they can communicate with the Federal Government. And on top of that, I am going to put in a secure video for Commissioner Kelly up in New York City so that he can dial in if he has a problem or a worry about something, we can just sit and secure a video conference and discuss the threat.

Mrs. LOWEY. Well, I personally, before I go and vote, want to thank you for that, because Chairman King and I—I am not sure,

Chairman Simmons, whether you were with us at the time, it was shortly after 9/11, and we went down there and met with Commissioner Kelly, and it was clearly, good luck from the Federal Government, he was on his own. And as you know, he has established a counterterrorism network around the world. And I have been with David Cohen and others visiting their system and their various offices, and it really is impressive. They really follow up on every single lead.

I just wonder, how many leads do you get from the Federal—just on average, from the Federal Government coming down to them, or are they really picking them up themselves through their own networks?

Mr. ALLEN. Well, I think we get quite a number of threats that relate to this country that flow in from overseas, and obviously from the extraordinary capabilities of the FBI. Many of these are not valid; we have to look at their credibility. And this is something that goes on every day. New York City also picks up suspicious activity, and they are very good at informing us.

New York City is a model for doing counterterrorism, and we learn from working with New York City it is a two-way street. I have learned a great deal from working with Dave Cohen, a man with whom I worked with at the CIA, as well as Mr. Sanchez. So I think it is a mutual sharing of information. And Commissioner Kelly has made it clear that he wants to work very closely with the Department and with the operations that I direct.

Mrs. LOWEY. I gather I have to vote, but let me just say thank you very much. You have been on the job for how long now?

Mr. ALLEN. I have just arrived 9 months ago.

Mrs. LOWEY. Well, I appreciate it. I remember on our other committee it took 2-1/2 years out of 9/11 for an inspector general to set up a computer system. So all these questions that we have, why hasn't it been done, that is past, and I hope that you can move as expeditiously as possible. And I know that New York City will be grateful for your efforts.

One thing really impressed me as I visited these centers. They follow up on every single lead, no matter how minor, because you never know how minor it really is. So I thank you very much for your important work, and I guess I had better vote.

Mr. ALLEN. Thank you, Congresswoman. Believe me, New York City is on my thoughts all the time. They ask me what worries me always, and I am always worried about New York City. And I am always sure to tell David Cohen I worry about it before I go to sleep.

Mrs. LOWEY. You keep worrying about it, because I have five of my seven grandchildren living in New York City, plus two of my three kids. So I worry about it morning, noon and night. And hopefully we will continue to put all the appropriate procedures in place. Continue to worry because that is the only way we can make sure we are covered. And I thank you very much.

Mr. ALLEN. Thank you, ma'am.

Mr. SOUDER. [Presiding.] I assume this is done—and I am not trying to get into specifics that would be classified, but I assume that on a daily basis there is attempts to see where our vulnerabilities are, where we are testing our border crossings,

where we are testing our ports, where we are testing our airports, and you are checking to see where our holes are. Is that a correct assumption?

Mr. ALLEN. That is correct. Whether it is terrorism from abroad, al-Qa'ida, whether it is sort of global—inspired homegrown terrorists that are looking for weaknesses. We see alien smuggling networks and narcotraffickers always trying to find new ways of getting across our borders, yes.

Mr. SOUDER. One of the concerns that I have is historically—I chair the narcotics oversight committee directly and have spent most of my career working with narcotics as well as the Speaker's Drug Task Force, and came on here because, having worked narcotics issues, it was a logical thing to move to Homeland Security and border because they are so interconnected, and their functions are interconnected—is that often we are better at figuring out after some things happened in explaining patterns rather than being able to prevent. And it is much more difficult to try to put the little pieces of the alphabet in the connection until you have actually had the action. And yet the risk is so much higher even in Homeland Security on one big tragic thing than kind of the daily pounding we take on narcotics and other types of illegal activity.

My question is, how much of the focus in the intelligence gathering—is it the National Targeting Center? Who is primarily trying to figure out when we do this, this is how they may change? In other words, let's say we put a fence over parts of the border. Where are they going to move next? Are we going to squeeze them into the Caribbean, are we going to move into the—if we control the Florida area, are they going to move in where we don't have as much air surveillance between, say, Galveston and the center of Florida? What if we do this will move them more to the Canadian border? What will move them to North Dakota as opposed to through the main border crossings? Is that type of discussion occurring? Is it interagency? How does it interrelate with the NORTHCOM and SOUTHCOM and the JATFs?

Mr. ALLEN. And it is a very good question because—and I will let my colleagues—again, Mr. Bortmes, Mr. Sloan and Ms. O'Connell—talk particularly about the daily looking at changing patterns.

My job—and I have here my Chief Threat Assessment Officer—is to look at how these patterns change, working with all sources of information from the traditional Intelligence Community as well as from the operational components of Homeland Security to try to focus very clearly on where things have shifted because—and I am sure Mr. Sloan can tell you about maritime patterns and how, as the Coast Guard increases pressure in one area, the roots move to another.

I think we have to do this very, very systemically. I have talked to Mr. John Walters, who heads their Office of Drug Enforcement Policy, and he believes that we have to look at this very holistically, and we have to stand back and get strategic intelligence. If we simply follow the latest lead, the latest tip, and just do tactical intelligence, we won't understand it.

And your question is very much on target. We have to do both; we have to do tactical operations, and we have to do strategical

analysis, otherwise we will never win this—and I don't know if win is the right word—otherwise we will never be successful in this struggle to secure our borders.

Mr. SOUDER. One of the challenges, when there was a lot of focus on the Arizona border, we took resources from California and Texas and moved them over. It is not clear that the groups who are moving any kind of illegal traffic, whether it be human, narcotics, terrorists or anything else, behave in zones like we behave. While they may have certain syndicates that control certain parts of those zones, they don't match up to our sectors. And what clearly happened is we had an increase in activity in areas where we had pulled out, and so the net reduction wasn't anything like consolidating in one zone.

If we put the Guard on the border, if we fence certain sections, I presume that as we are making those decisions, much like—I mean, anybody knows who goes to San Ysidro, you can see all the watchers. You can see the watchers on their side and our side going back and forth, and the lane movements, and both sides are watching that. And I would like to think that we are increasingly doing that anticipation of what, if we do this, the next move is going to be. And a lot of that is intelligence-driven: Are we doing preventative intelligence as well as reactive intelligence? And that is kind of the biggest challenge that you have in the services.

One other question on NORTHCOM. They have been talking about standing up more intelligence and coordination, whether it is down at El Paso or up in Colorado. Do you know what the status of that is? And do you have an opinion as far as how—whether the Defense Department needs to get into more aggressive intelligence on the border?

Mr. ALLEN. Well, let's just go back to proactive intelligence activities and ways to do prevention. I think Mr. Bortmes may talk about intelligence-driven activities or operations on how we have tried to anticipate, if there is a threat, to preempt people from entering and crossing our borders who could have very nefarious plans.

The one thing that we are working on right now broadly within the Intelligence Community as well as the Department of Homeland Security is the issue of radicalization. We are also working with State and local governments because we are finding that the States are studying radicalization. What causes a person to move from, say, a fundamentalist view of the world to one of extreme, say, solipsism and where violence might be created? How can you prevent that deterrence? How can you engage in a policy of deterrence or a policy of preemption? So we are working at that.

And my deputy for intelligence, who is not here, has formed a Radicalization Working Group, and we work across the community and across the Department.

On the NORTHCOM issue, that is very important. I'm getting a NORTHCOM officer assigned directly to my office so we can coordinate more. I met with Admiral Keating. I have met with retired Captain Mike Knoll, who is a J–2 out there. It is clear that they do wish to expand their energies and efforts to work secure borders. They have had some issues getting all the activities in which

they want to undertake, but we are working very closely with them, and they are expanding their energy on border security.

Ms. LOFGREN. Just real quickly. All of the terrorists who attacked the World Trade Tower, the first attack and the second, actually came in with visas through airports, not across the land borders. Does your plan that you are working on address that element?

Mr. ALLEN. The intelligence campaign plan is more focused on securing the land borders in particular, both north and south. We have come leaps and bounds since September 11th in being able to control particularly the movement through the air and our airports of entry. I believe the kind of programs that are in place now and which are being improved is much greater.

I know that Mr. Sloan could talk about security at ports as well as maritime and border intrusions. But what we have since September 11 is a much harder country to enter illegally. However, I am very concerned about the potential for ″clean skins″ getting breeder documents, getting genuine documents, say, in Western Europe and being able—as Director Mueller might say—to be only an e-ticket away from entering the United States. So we do worry about that.

Ms. LOFGREN. Thank you, Mr. Chairman. And I would yield back so that my colleague from California can begin her questions.

Mr. SIMMONS. The Chair recognizes the gentlelady from California, the distinguished Ranking Member of the Intelligence Committee. Thank you.

Ms. HARMAN. Thank you for holding this hearing.

Welcome, Charlie. I just voted not to adjourn Congress. I actually think there are some important things to do, and one of them is to enact a comprehensive immigration reform strategy. I realize you are not here testifying on that, but I thought I would, until I collect myself, make a point, which is that we do need stronger border enforcement at all of our borders and not just our southern border. We surely need an intelligence strategy to fit with border enforcement, because most folks coming here are just looking for a better way of life, they are not potential terrorists or criminals. But we also need the rest of it, which is some fair and reasonable suggestion for how to deal with 11—or 12 million people who are already here. And I hope we will do both, and I think it would be a huge mistake if some folks in this Congress prevent us from doing both. So that is my rant. Now I have collected myself.

And I know you have been asked that question about fusion centers and some of the other issues that I care about, too. I sort of want to approach this more philosophically, if I can, and that is to get your sense, and I know you can give us your sense because this is your background in what you do for a living, of how critical the intelligence piece is to border enforcement. If you get this right, and if the intelligence—if the fusion centers work, and if information sharing actually happens, what could we begin to see? And if you get it wrong and there isn't information sharing, and the fusion centers implode, and the intelligence products are bad, what could we see?

Mr. ALLEN. I think a strong intelligence integrated capability with law enforcement along with good policies and good cooperation

with our neighboring countries will make a world of difference. I think intelligence can and should be a major driver because, to me, to be able to understand the threat, to focus in on those threats that are most worrisome to us—and, as you said, it is not just the illegal workers. What really worries us are the narcotraffickers, the alien smugglers and, above all, special interest aliens, some of whom may be coming here from Asia, the Middle East, South Asia, or Africa as part of an extremist group.

If we get this right—and this is something that we are working with Ambassador Negroponte. As you know, Ambassador Negroponte served in Honduras, he served in Mexico City, he knows some of the border issues very well, and we discussed it. He looks to the intelligence-driven efforts that we are conducting as very much part and parcel of the overall national intelligence effort. Ambassador Negroponte, and I saw him last night, is very determined to work with us on this issue.

Ms. HARMAN. Well, I agree with that. We call him Director Negroponte, by the way, in the Intelligence Committee because we think he has got to lead this endeavor and not just be an ambassador. But that is a comment for the winds.

At any rate, I agree. And if we get it wrong, conversely, the highest fences in the world, 3 million Border Patrol folks I doubt will prevent us from being harmed by either the criminal element or terrorist element because there is no such thing—and I am asking a rhetorical question, but I assume you agree with me, Charlie. But there is no such thing as 100 percent security anyway; is that correct?

Mr. ALLEN. That is absolutely correct. I talk about stabilizing our borders. The term "seal our borders" is not a phrase I use. I want stability on the borders so we can then be able to focus on those real threats. And they are real threats, and some that I see every day that give us great concern.

Ms. HARMAN. Well, I thank you for that. And, Mr. Chairman, let me conclude by saying if we don't get the intelligence piece right, we will never get border enforcement right, period. And border enforcement obviously is more than the Mexican and the Canadian borders. It is port security; it is airport security; it is those folks who come in on cruise ships to Catalina off the coast of California where there are no border controls, and then take the ferry boat into San Pedro or Long Beach, or pick another island in another location. None of this will work if Charlie Allen doesn't succeed. So, no pressure, Charlie, but please succeed.

Thank you, Mr. Chairman.

Mr. SIMMONS. I thank the gentlelady for her questions and her comments. And I share with her that I could not agree with her more, that what we do intelligencewise on the border, how we focus our intelligence assets is going to determine whether or not we succeed; that we simply cannot put a policeman or a soldier in every place for 12,000 miles. It simply won't work.

And in excusing our first panel, I would like to comment again where he says ongoing operational efforts to push the border outward and build a layered defense extending within the United States. We talk about the border as a line in the sand, but from an intelligence standpoint we are talking about someone who may

appear on the radar in Afghanistan, transit Europe, show up on a ship or in Canada or in Mexico, and at some point in that process we try to get a line on them so when they hit the border, we can grab them, or when they cross the border, they set off a trigger mechanism and ring a bell so that subsequently we can get them within the United States.

So it is not a question of intelligence just at that point; it is a question of intelligence in depth overseas and intelligence follow-up within the continental United States, again, within the framework of our civil liberties and our rights.

Thank you, Mr. Allen, for your testimony. And I would ask the second panel to quickly gather. I know our Coast Guard friends have some time constraints, but we want to pick their brains. Thank you very much.

The second panel will be made up of what you might call the operational components of intelligence at the border. We have Mr. James Sloan, Assistant Commandant For Intelligence of the U.S. Coast Guard, charged primarily with port security and offshore security activities; Ms. Cynthia O'Connell, Acting Director, Office of Intelligence, Immigration and Customs Enforcement. And I think we all have an understanding of what our Immigration and Customs folks are doing intelligencewise at the border. And then lastly Mr. L. Thomas Bortmes, Director, Office of Intelligence, Customs and Border Protection.

I welcome the three witnesses. I know they all have prepared statements. We would appreciate it if they could summarize the high points of their statements for no more than 5 minutes, allowing the Members to ask questions.

And why don't we start with the Coast Guard. Mr. Sloan, the motto is Semper Paratus. Are you prepared?

STATEMENTS OF JAMES SLOAN, ASSISTANT COMMANDANT FOR INTELLIGENCE, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY.

Mr. SLOAN. Yes, I am, Mr. Chairman. And thank you. And thanks also to Ranking Member Lofgren.

I am Jim Sloan. I am the Coast Guard's Assistant Commandant For Intelligence and Criminal Investigations. And I do have a prepared statement that I would ask be inserted into the record.

Mr. SIMMONS. Without objection.

Mr. SLOAN. Thank you, sir.

I would like to thank each of the members of the committee for the opportunity to discuss the Coast Guard's intelligence and criminal investigations program and its role in support to Coast Guard missions regarding border security.

Bounded by the oceans, America always has been a maritime Nation. The oceans are a resource that we have to protect, a path for global commerce, and, unfortunately in today's world, a route for potential terrorists and other threats to our national security.

Mr. Chairman, you commented on the 12,500-mile border that is the maritime border, but in addition to that, the Coast Guard is responsible for 95,000 miles of coastline when you consider the laws that the Coast Guard has to enforce within 3.4 million square miles of Exclusive Economic Zones extending 200 miles from the

United States and its territories and possessions. This places us in a position to push our borders out and react to the threats far at sea.

It is through the Coast Guard's Intelligence and Criminal Investigation Program, that includes not only those personnel serving in Coast Guard headquarters, but those serving as liaison officers at various agencies, the intelligence analysts, the COASTWATCH personnel at the Intelligence Coordination Center, as part of and partnered with the Office of Naval Intelligence at the National Maritime Intelligence Center, the intelligence specialists at the Area Maritime Intelligence Fusion Centers, the field intelligence support teams at U.S. ports, and our criminal investigators are all involved in accomplishing the objectives to provide immediate actionable warning intelligence on terrorists and other threats to the Coast Guard's operational commanders, the Commandant, the Department of Homeland Security, and our other consumers.

Many Coast Guard missions are cued by intelligence such as counterdrug initiatives, alien smuggling, migration, fisheries enforcement, and other law enforcement functions. It is the personnel at the Department's Office of Intelligence and Analysis that Charlie Allen represents, the Area Maritime Intelligence Fusion Centers, and the Intelligence Coordination Center that blends the information and places it into the appropriate channels.

As part of the Department of Homeland Security's intelligence architecture, I am committed to integrating the Coast Guard intelligence capabilities with other components in the Department to support a unified DHS intelligence enterprise. Significant challenges remain, and many of them have been discussed in the last hour, and more work needs to be done, but the Coast Guard and the organizations represented here today are dedicated to ensuring the safety and security of the American people.

Thanks for this opportunity, and I am prepared to answer any questions.

Mr. SIMMONS. I thank you very much.

[The statement of Mr. Sloan follows:]

PREPARED STATEMENT OF JAMES SLOAN

Good morning Mr. Chairman and distinguished members. It is my pleasure to be here today, alongside Ms. Cynthia O'Connell, Intelligence Director of ICE and Mr. Tom Bortmes, the Intelligence Director of CBP, appearing before you today to discuss the Coast Guard Intelligence Program's role in border security.

The security of the U.S. borders is a top priority for the Coast Guard and the Department of Homeland Security (DHS). This hearing is a testament to the continued importance placed on border security and recognition of the Coast Guard's vital role in port and border security. Border security conveys the thought of land masses converging together. The reality is our maritime borders are the longest front in this battle. The Coast Guard's authority focuses not on land-to-land borders but land-to-water borders that include the Pacific and Atlantic Oceans as well as the Gulf of Mexico and the Great Lakes. These shores involve key border security issues that must be included in any border security discussions and decisions.

As the Nation's primary maritime law enforcement agency, an armed force, and lead Department of Homeland Security (DHS) agency for maritime security, the Coast Guard has significant authorities and capabilities with regard to maritime security. Still, success in achieving maritime border security requires the full and complete cooperation of our interagency, state, local, tribal and private sector partners.

The maritime domain is an avenue for those wishing to smuggle people and illicit drugs into our communities - and an avenue that could be exploited as a means to smuggle weapons of mass destruction and/or terrorists into our country. In 2005 alone, the Coast Guard

pted 9,500 undocumented migrants attempting to enter the United States illegally by sea, a 100 percent increase over 2001; and

Prevented more than 338,000 pounds of cocaine (an all-time maritime record) and more than 10,000 pounds of marijuana from reaching the United States.

While the 9/11 Commission noted the continuing threat against our aviation system, it also stated that ″opportunities to do harm are as a great, or greater, in maritime or surface transportation.″ There has been a great deal of focus on container security, which is appropriate; however, a container is only as secure as the ship and crew that carries it. In fact, the most often observed U.S. maritime threat remains smuggling. As on land, we know that there are numerous professional migrant smuggling rings that operate in the maritime realm. The proximity of U.S. population centers to the maritime domain and the diversity of maritime users present significant and wide ranging vulnerabilities. Effective intelligence support can address these vulnerabilities to detect and defeat threats along our maritime borders.

Many of the Coast Guard's mission successes are cued by intelligence. In addition to supporting our focus on preventing terrorist attacks, timely intelligence is critical in our efforts to stop international maritime drug trafficking, maritime alien smuggling, illegal high-seas driftnet fishing encroachment of U.S. natural resources in the Exclusive Economic Zone, and damage to the marine environment. Intelligence is a needed force multiplier given our limited assets and expanding mission requirements, it is the value added to enhancing maritime domain awareness.

Leveraging our longstanding partnerships and unique maritime authorities, access and capabilities the Coast Guard has significantly enhanced nationwide maritime security. The role of intelligence is to provide timely, accurate and actionable information so that decisions can be made and actions taken that support the operational commanders. Significant challenges remain and much more work needs to be done, but we are focused on the right priorities.

The Coast Guard Intelligence and Criminal Investigations Program has established and actively participates in several partnerships to enhance border security and other Homeland Security initiatives, such as:

The Coast Guard works in close partnership with DHS Office of Intelligence and Analysis (I&A) and other elements of the Department to provide intelligence support to homeland security. We are providing strong support for the standup of the intelligence functions within OI&A by detailing intelligence analysts and assisting in building relationships with other Intelligence Community partners.

The Coast Guard Intelligence Program and the Office of Naval Intelligence continue to build an effective joint intelligence partnership to enhance maritime domain awareness. The Coast Guard's Intelligence Coordination Center is co-located with the Office of Naval Intelligence, which comprises the National Maritime Intelligence Center (NMIC);

The NMIC has been designated as the core element for the Global Maritime Intelligence Integration (GMII) Plan. The GMII Plan is one of the eight support plans that make up the National Strategy for Maritime Security (NSMS). The Coast Guard's Intelligence Coordination Center (ICC) and the Office of Naval Intelligence (ONI) have been the foci of the GMII effort thus far. Achieving Final Operating Capability (FOC) is dependent upon strong representation from the other core elements, including: DHS - CBP and ICE, DOJ - FBI and DEA, Treasury - OFAC and FINCEN, NSA, and NGA. The overarching GMII requirement is to identify, locate, and track potential threats to U.S. maritime interests and subsequently transfer accurate, relevant, and collaborated information to those operational entities.

Within the Coast Guard's Intelligence Coordination Center (ICC), the Coast Guard and CBP have exchanged personnel to enhance data sharing between the ICC's COASTWATCH program (which gathers and analyzes information based on the ship's 96-Hour Notice of Arrival (NOA) report on vessels and people approaching U.S. ports) and CBP's National Targeting Center (cargo tracking) process. COASTWATCH has improved processing of NOAs by more than 600 percent since FY05. This COASTWATCH mission has detected and provided advance warning about numerous arriving individuals identified in federal law enforcement and immigration databases as criminal or security concerns, including active warrants and ″deny entry″ orders for previous border crossing violations. In addition, several individuals wanted for questioning by federal agencies about possible extremist associations have been identified in advance of arrival and referred to the relevant agency for investigation.

The Coast Guard provides access, where authorized and appropriate, to its intelligence and criminal investigations databases, as well as advice to others developing intelligence sharing architectures. The Service has also provided intelligence analysts, exchange personnel, and liaison officers to other agencies active in the maritime arena;

The Coast Guard's Intelligence and Criminal Investigations Program provides a permanent presence on the FBI's National Joint Terrorism Task Force (JTTF) and select regional JTTFs;

″Operation Drydock″, which began in December 2002, is a joint Coast Guard and FBI criminal and counterterrorism investigation into national security threats and document fraud associated with U.S. merchant mariner credentials. Currently, the databases compiled are managed by the Coast Guard Investigative Services (CGIS) and are used by El Paso Intelligence Center (EPIC), Coast Guard ICC, and Coast Guard Sector Commands nationwide. The ″Operation Drydock″ databases are also used by Coast Guard Regional Examination Centers (REC) to vet applicants seeking merchant mariner documents and licenses; and

″Operation Panama Express″ is a multi-agency Organized Crime Drug Enforcement Task Force (OCDETF) investigation that began in the mid 1990s to help stem the flow of illegal narcotics flowing from Central and South America via maritime means. The Coast Guard Investigative Service is a partner in Panama Express. The CGIS agents assigned to Panama Express speak fluent Spanish and have a wealth of practical hands-on experience in Coast Guard maritime law enforcement operations and CGIS narcotics investigations.

The Coast Guard has also increased its efforts to share law enforcement and intelligence information collected by the Coast Guard with other DHS components and other federal government agencies. In addition, the Coast Guard's Intelligence Program activities have been enhanced to assist in countering potential maritime threats there

Establishment of Field Intelligence Support Teams (FIST) in various key U.S. ports. FISTs gather local law enforcement information, establishes contacts, interviews masters and crewmembers to better understand maritime threats;

Enhanced intelligence capability at the theater-level with the standup of the Maritime Intelligence Fusion Centers (MIFCs) Atlantic and Pacific. The MIFCs increase collection and analytical capabilities, enhance all-source intelligence and information fusion, improve the timeliness and quality of intelligence support to Coast Guard

operational forces. The MIFCs also ensure the rapid reporting of information gathered by Coast Guard forces into the Department of Homeland Security and Intelligence Community at the national level; Conducting Port Threat Assessments as a complement to the MTSA-mandated Port Security Assessment, to provide analyses of threats for specific ports, inclusive of both terrorism and crime - foreign and domestic - using law enforcement and intelligence information; Fielding of Sector Intelligence Officers put intelligence support at the tactical level; and, the Coast Guard's membership in the Intelligence Community; our wide-range of missions, and our expertise in the maritime domain allows us to interface in numerous and diverse forums at various levels within the DoD components, law enforcement agencies, intelligence community, state and local stakeholders, and private industry.

Analysis of the maritime threat to U.S. ports is challenging. Characterization of incidents and trend analysis is complicated by the convergence of large volumes of cargo, alien smuggling networks, the narcotics trade, terrorism, regional conflict, maritime criminal enterprises, and some activities that fall into multiple categories but fall short of being a direct security threat to U.S. ports. It is the Coast Guard's overarching strategy, through layered security architecture, to ″push out our borders.″ Our unambiguous goal is to meet threats far offshore in order to prevent hostile persons, vessels, or cargoes from entering our ports or coastal regions. Our ability to push the borders out is an essential element in protecting our homeland.The Coast Guard faces challenges in the maritime domain similar to those of our colleagues in securing the land border - with a limited set of resources, located amid vast geographic areas and huge amounts of legitimate activity - stop those seeking to do us harm. The foundation of the Coast Guard's maritime strategy relies on three key priorities:

Achieve Maritime Domain Awareness;
Establish and Lead a Maritime Security Regime; and
Deploy effective and integrated Operational Capability.

These are not stand-alone goals, but rather part of an active system of layered maritime security. For example, the Maritime Transportation Security Act (MTSA) led to the establishment of domestic and international AIS carriage requirements for certain commercial vessels. But without investment in systems to collect, analyze and disseminate the AIS signals we lose the opportunity to assess threats early. Similarly, the detection, identification and interdiction of small vessels (that certainly do not advertise their position) used by smugglers throughout the Caribbean and Eastern Pacific requires persistent surveillance capabilities. In the end, Coast Guard assets must be capable of mounting a dependable response to identified threats lest we have information but not the capability to act.

Coast Guard assets and systems are required to operate across a diverse operating area including within our ports, in the littoral region, and far offshore. Thanks to the strong support of the administration and Congress, a number of initiatives are underway to transform Coast Guard capabilities. I would like to highlight a few of these initiatives as each will have a broad and substantial influence on our intelligence capabilities to mitigate current and future maritime risks.

Integrated Deepwater System. The centerpiece of the Coast Guard's future capability is the Integrated Deepwater System, recently revised to reflect post-9/11 mission requirements such as enhanced intelligence gathering and handling capabilities. The Integrated Deepwater System was designed to secure the nation's maritime borders.

The vessels delivered by the Deepwater program will serve as the Coast Guard's ″eyes and ears″ and allow the nation to see, hear and communicate activity occurring within the maritime domain. The Coast Guard's sustained presence along our maritime borders is unique. More capable Deepwater assets, linked to each other and multiple agencies through Deepwater's net-centric command-and-control system will significantly improve information sharing, collaboration, and interoperability in the maritime domain.

Vessel tracking. Securing our vast maritime borders requires improved awareness of the people, vessels and cargo approaching and moving throughout U.S. ports, coasts and inland waterways. The most pressing challenges we now face involve tracking the vast population of vessels operating in and around the approaches to the United States. In support of this requirement, the Coast Guard has:

Established the Automatic Identification System (AIS) to provide continuous, real-time information on the identity, location, speed and course of vessels in ports that are equipped with AIS receivers. AIS is currently operational in several major U.S. ports, and the Coast Guard's Nationwide Automatic Identification (NAIS) project will expand AIS capabilities to ports nationwide; and

Under U.S. leadership the International Maritime Organization recently unanimously adopted a global long Range Identification and Tracking scheme that will provide information about all commercial ships of 300 gross tons and above operating within a 1,000 nautical miles of our coast whether the ship is bound for a U.S. port or is on innocent passage. Additionally, we will have tracking information out to 2,000 nautical miles when ships have declared its intent to arrive in a U.S. port.

Maritime C4ISR Enhancement. Existing Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems and operational concepts must be reoriented and integrated with current and emerging sensor capabilities and applicable procedures. Similar to the nation's air space security regime, the maritime security regime must integrate existing C4ISR systems with new technologies and national command-and-control systems and processes. For example:

The Common Operating Picture (COP) and corresponding Command Intelligence Picture (CIP) must continue to grow and expand to federal, state, and local agencies with maritime interests and responsibilities. The COP provides a shared display of friendly, enemy/suspect and neutral tracks on a map with applicable geographically referenced overlays and data enhancements. The COP is also a central element of the Deepwater solution tying Deepwater assets and operational commanders together with dynamic, real-time maritime domain information. This link is essential to ensure effective command and control of all available Coast Guard assets responding to a myriad of border security threats.

An expansive and interoperable communications network is critical for maritime security operations and safety of life at sea. In the coastal environment, the Coast Guard's Rescue 21 system will provide the United States with an advanced maritime distress and response communications system that bridges interoperability gaps, saves lives and improves maritime security.There is no single solution to maritime border security. It requires a layered system of capabilities, established competencies, clear authorities, and strong partnerships. The cost of allowing blind spots in our awareness, security regimes or operational capabilities is too high.This is the mandate for the Coast Guard Intelligence and Criminal Investigations Directorate to support those priorities, which ultimately supports the overall strategic and national level objectives of the Nation.Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Mr. SIMMONS. And we will now go to the second witness Ms.O'Connell. Welcome.

CYNTHIA O'CONNELL, ACTING DIRECTOR, OFFICE OF INTELLIGENCE, IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. O'CONNELL. Good morning. Thank you, Chairman Simmons. I will have just a few brief statements. I respectfully request that my full statement be submitted for the record.

Mr. SIMMONS. Without objection.

Ms. O'CONNELL. Chairman Simmons, Ranking Member Lofgren, members of the subcommittee, I am Cynthia O'Connell, Acting Director of the Office of Intelligence for Immigration and Customs Enforcement. I sincerely appreciate this opportunity to share with you how the men of women of ICE Intelligence employ our capabilities to help secure our Nation's borders.

I am also honored to testify alongside my colleagues from Customs and Border Protection and the U.S. Coast Guard, as well as Mr. Charles Allen from the Department of Homeland Security. As the DHS Chief Intelligence Officer, as you know, Mr. Allen has been instrumental in coordinating with the Intelligence Community and providing guidance on Homeland Security-specific issues.

The ICE Office of Intelligence supports ICE and DHS intelligence requirements and priorities. We have made significant progress and continue in expanding our responsibilities to support the needs of ICE, DHS, and the Intelligence Community.

With the unique Immigration and Customs authorities and intelligence tools, ICE Intelligence has also enhanced its detection, collection, and analysis capabilities.

In addition to ICE Intelligence headquarters in Washington, D.C., we have six field intelligence units located in New York, Long Beach, Chicago, Houston, Tucson, and Miami; two technical collection facilities, the Tactical Intelligence Center, and a Special Operations Center; and intelligence assets at the El Paso Intelligence Center.

ICE Intelligence headquarters supports ICE management and DHS intelligence and analysis efforts and coordinates ICE Intelligence programs and operations nationwide. The field intelligence units provide intelligence expertise to field investigative offices and detention facilities and to DHS intelligence as a whole. Our technical collection facilities act in concert for the Intelligence Community, the military, and other Federal agencies to safeguard the border that extends beyond our borders outward. These are powerful capabilities, and we have moved to organize them in a coherent and effective support system both to advance the ICE investigative mission and to support and integrate ICE into the DHS intelligence functions.

Our specific intent is to integrate our intelligence capabilities with other components in the Department to support a unified DHS intelligence enterprise. ICE Intelligence takes advantage of currently operating effective projects and programs, and combines them with proposed new programs and capabilities, and unites the whole under a common strategic purpose, the protection of our country against threats that could arise from our borders.

Our Special Operations Center detects and locates smugglers moving contraband and aliens across the borders by collecting intelligence through real-time technical means. Its methodologies not only interdict the incursion, but also helps identify smuggling organizations for investigation and dismantling.

We coordinate Customs and Border Protection air and marine operations in the Office of Border Patrol and Office of Border Patrol assets to stop illegal activity. This year they have supported the interdiction of about 35 tons of marijuana with the seizure of associated vehicles and weapons and the arrest of countless smuggled aliens.

ICE is integrating its Special Operations with geospatial intelligence capabilities sponsored by DHS and the analytical functions of our Southwest Field Intelligence Unit. We are working with DHS Intelligence, Surveillance and Reconnaissance to leverage available Department of Defense and DHS science and technology resources for upgrades to this dedicated border protection unit.

What I have just described to you is true border-focused intelligence support. However, our protective effort is not devoted to just the land borders; we are also heavily involved in maritime and air transportation environments.

Operation Last Call exploits the intelligence value of hundreds of thousands of individuals who enter the detention system annually. This highly effective operation collects, evaluates, analyzes, and disseminates information derived from detainees in ICE custody.

Project Aegis supports the ICE visa security program which places ICE personnel in foreign countries to work with State Department consular officials in vetting these applicants.

The Border Enforcement Security Task Force is a DHS-inspired initiative that responds to the increase in border violence. It is actively supported by analytical resources from our field intelligence units.

ICE Intelligence is also working with DHS I&A on its intelligence campaign plan, a borderwide security effort aimed at more efficient consolidation of relevant field intelligence information.

Operation Capistrano is a cooperative initiative with Department of State Consular Affairs where we train password examiners to recognize indicators that may point to potential narcotics and currency smugglers. This initiative has led to over 1,300 seizures and 1,300 arrests with more than 1,700 pounds of heroin and 2,600 pounds of cocaine seized.

Operation Roswell uses similar techniques to identify alien smugglers, immigration fraud violators, and child sex tourism suspects. In the past 2 years, Operation Roswell resulted in 26 aliens removed, produced evidence of over 60 marriage fraud schemes, and in one significant case yielded analysis that led to eight arrests, ten removals, and the dismantling of an organization that smuggled 37 foreign nationals into the United States.

In spite of all these successful initiatives, we are not content to rest on present production and current capabilities. Business plans and performance metrics based on objective customer evaluations must support all our work. From these markers, ICE Intelligence proposes the development and acquisition of advanced technologies, new techniques and new processes, and additional integration into multiagency and multinational operations. This is our future path to a safer and more secure border and homeland.

I thank you for the opportunity to describe some of our initiatives that support border security. I would be happy to answer any questions at this time.

Mr. SIMMONS. Thank you very much.

[The statement of Ms. O'Connell follows:]

PREPARED STATEMENT OF CYNTHIA O'CONNELL

Chairman Simmons, Ranking Member Lofgren, Members of the Subcommittee,

I am Cynthia O'Connell, Acting Director of the Office of Intelligence for U.S. Immigration and Customs Enforcement (ICE). I sincerely appreciate this opportunity to share with you how the men and women of ICE Intelligence employ our capabilities to help secure our nation's borders.

The ICE Office of Intelligence supports ICE and Department of Homeland Security (DHS) intelligence requirements and priorities. We have made significant progress in continuing and expanding our responsibilities to support the needs of ICE, DHS, and the Intelligence Community (IC). With unique Immigration and Customs authorities and intelligence tools, ICE Intelligence has also enhanced its detection, collection and analysis capabilities.

In addition to ICE Intelligence Headquarters in Washington DC, we have six Field Intelligence Units located in New York, Long Beach, Chicago, Houston, Tucson, and Miami; two technical collection facilities - the Tactical Intelligence Center (TIC) and a Special Operations Center; and intelligence assets at the El Paso Intelligence Center (EPIC).

ICE Intelligence Headquarters supports ICE management and DHS Intelligence and Analysis (I&A) efforts, and coordinates ICE intelligence programs and operations nationwide. The Field Intelligence Units provide intelligence expertise to investigative offices and detention facilities in the field and to the DHS Intelligence

as a whole. Our technical collection facilities act in concert with the Intelligence Community, the military, and other Federal agencies to safeguard the southern border and to extend coverage of our borders outward even to the shores of South America.

In intelligence terms, these are very powerful capabilities, and we have moved aggressively to organize them into a coherent and effective support system, both to advance the ICE investigative and operational missions, and to support and integrate ICE in the DHS intelligence functions. We have accomplished this through the ICE Intelligence Strategic Plan, which was constructed with the specific intent to integrate our intelligence capabilities with other components in the Department, to support a unified DHS Intelligence Enterprise.

The ICE Intelligence plan takes advantage of currently operating, demonstrably effective projects, programs, and activities; combines them with proposed new programs and capabilities; and unites the whole under a common strategic purpose - the protection of our country against threats that could arise from our borders. It is more than just a plan. It reflects real, effective action on the front lines.

Special Operations Center

The Special Operations Center detects and locates smugglers moving contraband and aliens across our borders by collecting intelligence through real-time technical means, primarily signals and imagery intelligence. It supports ICE investigations with methodologies that not only interdict the incursion, but also helps identify smuggling organizations for investigation and dismantling. This kind of intelligence has real long-term benefits. The unit's emphasis to date has been on the U.S. and Mexico border.

We coordinate with Customs and Border Protection (CBP) Air and Marine Operations and Office of Border Patrol assets to stop illegal activity. The information we collect is disseminated to ICE and Border Patrol agents in affected areas along the border from California to Texas.

ICE is currently integrating its intelligence program with the Special Operations Center geospatial intelligence capabilities, sponsored by DHS, and the analytical functions of our Southwest Field Intelligence Unit. We are working with DHS Intelligence, Surveillance, and Reconnaissance (ISR) to leverage available Department of Defense and DHS Science and Technology resources for upgrades to this dedicated border protection unit.

What I have just described to you is true, border-focused intelligence support; however, our protective effort is not devoted to just the land borders. We are also heavily involved in maritime and air transportation environments. We view border security as a continuum - it starts in various foreign countries, proceeds internationally to our borders, seaports, and airports, and extends into the interior of the United States, where support structures exist for criminal organizations as well as illegal immigrants. ICE provides intelligence at all points along this continuum.

ICE Intelligence Projects and Programs

The Port Intelligence Center (PIC) was created in response to Secretary Michael Chertoff's directive to develop a task force that addresses New York and New Jersey seaport vulnerabilities. The ICE Northeast Field Intelligence Unit (NEFIU), in coordination with the ICE Special Agent in Charge/New York (SAC/NY) and SAC/Newark, CBP, USCG, the New York City Police Department (NYCPD), and other state and local law enforcement groups, have established the NY/NJ Metropolitan Area Port Intelligence Center. The PIC will develop a seaport intelligence collection strategy aimed primarily at cultivating human intelligence in the maritime environment. It utilizes the intelligence resources of its members to prioritize vulnerabilities and pursue entities and individuals for potential source cultivation.

The National Security Integration Center (NSIC) is an Office of Investigations and Office of Intelligence joint center that assesses information, targets suspects, and supports national security investigations conducted by ICE.

Operation Ardent Guardian targets the illicit use of legitimate immigration channels, seeking the indicators of asylum fraud, marriage fraud, false documents, and other fraudulent mean of entry.

Extraterritorial Criminal Travel Strike Force (ECT) is a new cooperative initiative by the ICE Office of Investigations and the Criminal Division of the Justice Department. Supported by ICE Intelligence, the targeting capabilities of ECT are designed to leverage extraterritorial investigative and prosecutorial expertise to attack foreign-based criminal networks.

Operation Last Call exploits the intelligence value of hundreds of thousands of individuals who enter our detention and removal system annually. This highly effective operation collects, evaluates, analyzes, and disseminates information derived from detainees in ICE custody. Customers for Operation Last Call intelligence are

ICE operational units, DHS I&A, the Intelligence Community, the Federal Bureau of Investigation (FBI), and other Federal agencies. This program focuses on relevant collection in the areas of force protection, anti-terrorism, on-going criminal enterprises, human trafficking and smuggling, contraband smuggling (weapons of mass destruction, drugs, etc.), threats to critical infrastructure, and the movement of money that support illicit activities.

Project Aegis (Domestic Visa Security) supports the ICE Visa Security program, which places ICE personnel in sensitive foreign countries to work with State Department consular officials in vetting visa applicants. The ICE Intelligence domestic program performs detailed research on the resident U.S. sponsors and contacts listed in visa applications and reports on the background and potentially suspect activities of those individuals. This program provided substantial intelligence on the Lodi, California, Pakistani community that has recently figured prominently in terrorist investigations and action.

Border Enforcement Security Task Force (BEST), the DHS-inspired initiative that responds to the increase in border violence, is actively supported by the analytic resources of the Houston and Tucson Field Intelligence Units. In addition to the BEST program, ICE Intelligence is working with DHS I&A on its Intelligence Campaign Plan (ICP), a border-wide security effort aimed at more efficient consolidation of relevant field-generated information.

Operation Crystal Ball, a joint operation involving ICE, the Office of Naval Intelligence, the U.S. Coast Guard (USCG), and CBP, tracks suspect vessels and crewmembers and maintains historical databases to respond to queries from investigators and officers working in the maritime environment. ICE Crystal Ball analysts use electronic collection techniques and perform both classified and unclassified research to derive movement and position information. They also populate Naval Intelligence databases with large volumes of current vessel tracking data. Crystal Ball support has repeatedly resulted in drug seizures from merchant vessels and crewmembers, and continually contributes to the strategic goal of awareness in the maritime and seaport environment.

Operation Capistrano, a cooperative initiative with the State Department's Office of Consular Affairs, trains passport examiners to recognize indicators that may point to potential narcotics and currency smugglers. This initiative has led to 1,366 seizures and 1,300 arrests.

Operation Roswell, an outgrowth of Operation Capistrano, uses similar techniques to identify alien smugglers, immigration fraud violators and child sex tourism suspects. In the past two years, Operation Roswell has led to the removal of 26 aliens, provided evidence of over 60 incidences of marriage fraud schemes, and in one significant case, yielded analysis that led to 8 arrests, 10 removals, and the dismantling of an organization that had successfully smuggled 37 foreign nationals into the United States.

Operation Watchtower, working in coordination with USCG and CBP, analyzes the international movements of vessels and cargoes to provide timely intelligence and risk assessment for investigative and threat detection support.

These examples are all actual ongoing activities, presently producing valuable intelligence that protects our borders. Many of these activities also directly support the Department's Secure Border Initiative. We also maintain a full-time senior liaison officer posted permanently to DHS I&A, which serves as an open conduit between ICE Intelligence and I&A.

In spite of such successful initiatives, we are not content to rest on present production and current capabilities. Business plans and performance metrics based on objective customer evaluations must support all our work. From these markers, the ICE Intelligence strategic plan proposes the development and acquisition of advanced technologies, new techniques, new processes, and additional integration into multi-agency and multi-national operations. This is our future path to a safer and more secure border and Homeland.

Thank you for the opportunity to describe some of our initiatives that support border security. I would be happy to answer any questions at this time.

Mr. SIMMONS. And our third witness is from U.S. Customs and Border Protection, Mr. Bortmes. Welcome. We have your testimony, so if you summarize in 5 minutes, that would be great.

L. THOMAS BORTMES, DIRECTOR, OFFICE OF INTELLIGENCE, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BORTMES. Will do, sir.

Thank you, Chairman Simmons, Ranking Member Lofgren, distinguished members of the subcommittee. I thank you for the opportunity to join my Department of Homeland Security intelligence colleagues, Assistant Secretary Allen, Director O'Connell, and Assistant Commandant Sloan, to discuss with you the role intelligence plays within the United States Customs and Border Protection to help secure our Nation's borders. I have submitted, as you stated, sir, a formal statement, and would request that it be accepted for the record.

I want to begin this very brief oral statement by saying that I am privileged to serve as the Executive Director of Customs and Border Protection's Office of Intelligence, which is charged with three primary responsibilities. The first is to directly support the Commissioner and Customs and Border Protection's headquarters and field leadership with the acquisition, analysis, and timely dissemination of intelligence information critical to CBP's primary mission of detecting, identifying, and preventing terrorists and terrorist weapons from entering the United States.

The second is to efficiently manage a developing integrated Customs and Border Protection intelligence capability that ensures frontline CBP officers and decisionmakers have the value-added intelligence required to sustain border situational awareness, drive operations, and support policy. This larger CBP intelligence enterprise consists of the intelligence capabilities within the Office of Intelligence, the Office of Border Patrol, CBP Air and Marine, the Office of International Affairs, and the Office of Antiterrorism, and works very closely with the National Targeting Center and operational field analysis capabilities of the Office of Field Operations.

And, finally, as a member of the Department's Homeland Security Intelligence Council, it is the responsibility of the Office of Intelligence to represent CBP's intelligence requirements and equities to the DHS Chief Intelligence Officer and assist him in directing an integrated DHS intelligence enterprise.

Customs and Border Protection intelligence exists to support an agency that, in addition to facilitating international trade critical to the United States economy, is responsible for border security. As you stated earlier, Mr. Chairman, and I won't repeat the numbers, it is responsible for protecting more than 5,000 miles of border with Canada, 1,900 miles of border with Mexico, and operating 325 official ports of entry.

An average day in Customs and Border Protection, from the statements you have already made this morning, is a demanding day. We process well over 1.1 million passengers and pedestrians; 69,000 containers; 333,000 incoming privately owned vehicles; $81 million, almost $82 million, in fees, duties, and tariffs; execute 62 arrests at ports of entry; over 3,200 apprehensions between the ports for illegal entry; seized over 5,500 pounds of narcotics; and not to forget over 1,100 prohibitive meat and plant materials, animal products at and between the ports of entry; refuse entry to 868 noncitizens at the ports of entry; and intercept 146 smuggled aliens, and over 200 fraudulent documents, while rescuing 7 illegal immigrants in distress or dangerous conditions between the ports of entry. And I remind you, again, that is every day.

As the figures demonstrate, CBP addresses a variety of threats to U.S. borders that include illegal immigration, illegal drugs, border violence, illegal incursions, pests and diseases, and a host of trade violations running from smuggling to international property rights.

While all of these threats to our borders are demanding in their own right, everyone at Customs and Border Protection understands that their priority mission is to prevent terrorists and terrorist weaponry from entering the United States.

While the Office of Intelligence and the broader CBP intelligence enterprise directly support operations aimed at addressing all border threat categories, they also remain focused on supporting CBP's priority mission of preventing terrorists and their weaponry from entering the United States. Our first priority is to operationalize intelligence reporting on terrorist threats.

In my formal written statement I discuss how CBP intelligence supports border security by supporting CBP's layered defense strategy, a strategy that, in partnership with an array of countries, international organizations, private businesses, trade entities, as well as State and local governments, has developed a host of programs and initiatives aimed at pushing our zone of defense as far outward as responsible to identify people and cargo long before they have the opportunity to board or enter the United States.

I look forward, sir, to answering yours and the committee's questions and working with my colleagues here today, and appreciate the opportunity to speak on these matters.

[The statement of Mr. Bortmes follows:]

PREPARED STATEMENT OF MR. L. THOMAS BORTMES

Introduction

Chairman Simmons, Ranking Member Lofgren, distinguished Members of the Subcommittee. I thank you for this opportunity to join my Department of Homeland Security colleagues - Assistant Secretary for Intelligence and Analysis, Mr. Charles Allen, Ms. Cynthia O'Connell the Director of ICE's Office of Intelligence and Mr. Jim Sloan, the Coast Guard's Assistant Commandant for Intelligence and Criminal Investigations - to discuss with you the role intelligence plays within U.S. Customs and Border Protection (CBP) to help secure our Nation's borders.

I am privileged to serve as the Executive Director of the CBP Office of Intelligence (OINT), a critical element of the Office of the Commissioner, charged with three primary responsibilities. The first is to directly support the Commissioner and CBP headquarters and field leadership with the acquisition, analysis and timely dissemination of intelligence information critical to CBP's primary mission of detecting, identifying and preventing terrorists and terrorist weapons from entering the United States. The second is to efficiently manage an integrated CBP intelligence capability that ensures front-line CBP officers and decision makers have the value-added intelligence required to sustain border situational awareness, drive operations and support policy. And finally, as a member of the Department's Homeland Security Intelligence Council (HSIC), it is the responsibility of the OINT to represent CBP's intelligence requirements and equities to the DHS Chief Intelligence Officer/ Assistant Secretary for Intelligence and Analysis, and assist him in directing an integrated DHS intelligence enterprise that provides one DHS face to the National Intelligence Community. I will address each of these responsibilities from the perspective of intelligence support to border security.

U.S. Customs and Border Protection Overview

In addition to facilitating the international trade critical to the United States economy, CBP is responsible for protecting more than 5,000 miles of border with Canada, 1,900 miles of border with Mexico and operating 325 official Ports of Entry. On an average day in 2005, CBP personnel: processed 1,181,605 passengers and pedestrians, 69,370 containers, 333,226 incoming privately owned vehicles and $81,834,298 in fees, duties and tariffs; executed 62 arrests at ports of entry and over

3,257 apprehensions between the ports for illegal entry; seized over 5,541 pounds of narcotics and 1,145 prohibited meat, plant materials or animal products at and between the ports of entry; refused entry to 868 non-citizens at the ports of entry; and intercepted 146 smuggled aliens and 206 fraudulent documents while rescuing 7 illegal immigrants in distress or dangerous conditions between the ports of entry. As these figures demonstrate, CBP, the nation's unified border agency, addresses a variety of threats to U.S. borders that includes illegal immigration, illegal drugs, border violence, illegal incursions, pests/diseases and a host of trade violations ranging from smuggling to intellectual property rights.

Countering Terrorists

While these threats to our borders are addressed each day, all CBP personnel understand that their priority mission is to prevent terrorists and their weaponry from entering the United States. While OINT directly supports operations aimed at addressing all border threat categories, it also remains focused on supporting CBP's priority mission of preventing terrorists and their weaponry from entering the United States. The first priority of CBP's Office of Intelligence is to operationalize intelligence reporting on terrorist threats. Each day, OINT watch standers and analysts review over 1000 intelligence community products, engage with CBP liaison officers and analysts embedded in DHS and the national intelligence community, and leverage long-standing partnerships with federal, state, local and international law enforcement and intelligence organizations to ensure early awareness of all potential terrorist travel or movement of materials to the United States. Working closely with their operational counterparts, OINT analysts meld this intelligence with information, trends and patterns identified in CBP operational reporting to properly assess and place in context these threats, discern vulnerabilities, evaluate potential consequences and ultimately calculate the risk these threats may pose to the borders of the United States. The results of this daily all-source analysis and risk assessment process is disseminated via over a dozen intelligence product lines and services including intelligence reports and alerts to CBP's operational and field elements on the border that provide situational awareness, address officer safety and/or assist in developing targeting criteria against specific terrorist threats to the United States.

Operations and Intelligence Briefings/Intelligence Driven Operations

Regular, all-source, intelligence briefings are provided to the Commissioner and CBP operational Assistant Commissioners from the Offices of Field Operations, Border Patrol, Anti-Terrorism, Air and Marine and International Affairs. During these briefings, CBP's senior leadership review the most current threat developments, maintain continuity on existing terrorist threat streams and utilize the latest intelligence available to formulate appropriate operational actions required to counter those threats. CBP's senior leadership has a number of operational courses of action available to operationalize threat intelligence, to include directing intelligence driven operations. Once CBP's senior leadership concurs that there is viable intelligence indicating a threat to our borders, an operational response plan is quickly formulated to address the specific threat modus, timeframe and geographic locations. These threat-based operations are put together by CBP's affected headquarters and field elements, formally vetted through the DHS Chief Intelligence Officer, then promulgated to the appropriate CBP operational field components for implementation. Additionally, OINT will regularly report the results of these operations via Homeland Security Intelligence Reports, and the CBP Office of Field Operations or Office of Border Patrol will formally assess the operational results upon their conclusion.

Supporting Forward Operations

To meet its priority mission, CBP has implemented a layered, defense in-depth strategy that thoroughly addresses people and cargo for linkages to terrorism prior to entering the United States. In partnership with an array of countries, international organizations, private businesses, and trade entities, CBP is involved with a host of programs and initiatives aimed at pushing our ″zone of defense″ outward. A key example of this is the Container Security Initiative (CSI), which places CBP personnel teams in key overseas ports to assist in identifying high-risk cargo. OINT has selected and trained intelligence research specialists to work as members of these CSI teams. Embedded with their host country, CSI intelligence personnel are supported daily by OINT which routinely provides them overviews of the latest intelligence threat reporting and vets their individual and company names of interest against U.S. intelligence terrorist data bases for derogatory information, etc.Another example of CBP pushing its ″zone of defense″ outward is the Customs and Trade Partnership Against Terrorism (C-TPAT) which has CBP partnering with over 9,000 private businesses to ensure the security of the international supply chain to prevent terrorists from exploiting legitimate trade. Membership in C-TPAT requires the

CBP to regularly certify partner company due diligence, and OINT plays a significant role in supporting CBP with intelligence research, entity searches, and the verification of information.

Supporting Operations at the Border

In addition to OINT's regular products and support to intelligence driven operations, OINT provides daily support to, the operational offices charged with maintaining CBP's border presence and security. These operational offices have placed subject matter experts within secure OINT facilities in order to increase information sharing and agency cooperation. Furthermore, OINT maintains a permanent detachment at CBP's National Targeting Center (NTC) with secure connectivity to national intelligence community reporting and data bases. This detachment supports the NTC's mission to assess all cargo and passengers enroute to the U.S. for potential links to terrorism and to directly support CBP Officers and Agents when they encounter individuals or cargo linked to terrorism.Q02

Managing the Integrated CBP Intelligence Enterprise

It is the responsibility of the Office of Intelligence to functionally manage the larger CBP intelligence enterprise. A number of CBP components have formally designated intelligence organizations, while others, such as the Office of Field Operations, have robust operational information analysis capabilities that work closely with these intelligence organizations. The Office of the Border Patrol has a significant intelligence organization that includes a national headquarters division, a Border Field Intelligence Center in El Paso, Texas and intelligence units at each of the 20 Border Patrol Sectors, all responsible for directly supporting front line Border Patrol Agents. CBP Air and Marine has a formal intelligence capability with designated intelligence personnel at their national headquarters, Air and Marine Operations Center in Riverside, California and with their Directors of Air Operations and Branches around the United States. These intelligence organizations are staffed with a combination of intelligence research specialists as well as Border Patrol Agents and CBP Air and Marine officers filling intelligence positions.

As you can imagine, each of these organizations generate standing and ad hoc information needs, intelligence requirements, requests for information, collection requirements, as well as a host of personnel, training, connectivity, equipment and policy needs. OINT aggregates, validates and prioritizes these requirements and brokers them through the DHS Office of Intelligence and Analysis to the national intelligence community for satisfaction.

Leveraging the DHS Intelligence Enterprise

CBP leverages the DHS Intelligence Enterprise largely by OINT's membership in the larger DHS intelligence enterprise. Working with the Chief Intelligence Officer, Assistant Secretary Charles Allen, the Department of Homeland Security is putting into place a rapidly expanding capability to support its agencies' intelligence components. As CBP's Key Intelligence Official, I am a member of Assistant Secretary Allen's Homeland Security Intelligence Council (HSIC) - the primary DHS intelligence decision-making body. Personnel from my office represent CBP's intelligence requirements on over a dozen HSIC-established panels, boards and working groups that address issues ranging from analytical production coordination to collection, training, and information systems. It is through this maturing DHS intelligence enterprise management architecture that OINT is addressing critical intelligence concerns such as supporting Operation Jumpstart's deployment of National Guard Bureau intelligence personnel to the Southwest Border and supporting implementation of the Southwest Border Counter-Narcotics Strategy. Additionally, by leveraging the developing DHS report writers and intelligence training programs, CBP is gaining personnel and training necessary to ensure that it can translate its significant operational information flow into a steady supply of timely, intelligence reports. These reports are earning acclaim for their relevancy from national, state and local intelligence and law enforcement customers, and make CBP a leading producer of intelligence reporting among DHS components. OINT will continue to play a leading role in developing this DHS intelligence enterprise and leverage it to facilitate its own developing intelligence integration plans and meet its intelligence needs.

Closing

I would like to thank you again for the opportunity to testify today with my Department of Homeland Security intelligence colleagues. I will be happy to answer any questions you may have.

Mr. SIMMONS. I thank all three witnesses for their testimony. We have learned there is another procedural motion and vote on the floor. We will do our best to keep this dialogue moving forward. My

colleague has gone to vote. I will keep the mike open, and we will do our questions.

Mr. Sloan, in your testimony on page 4 you make reference to information collected by the Coast Guard.

Ms. O'Connell, in your testimony you also make reference to the collection capabilities of your organization.

And, Mr. Bortmes, you just referred to what I called surveillance and depth.

The Coast Guard is now a full members of the U.S. Intelligence Community. The other entities I don't believe are. But the Coast Guard does not have a history and tradition of collection in an intelligence sense. But since 9/11 and in the new environment, the issue of collection of these assets to me is critically important. I don't want to know that you are acquiring information; in other words, that somebody hands you something and you take it. I do want to know that you are engaged in collection, because that seems to me to be a very worthwhile addition to our capabilities in a post-9/11 environment.

Could each of you talk a little bit about how you operate in the field and what opportunities you have to collect information that others don't have? In other words, what is your value added from that standpoint to the overall intelligence efforts of our country?

Mr. SLOAN. Sir, I will begin. First of all, as you probably know, in addition to being a member of the Intelligence Community, the Coast Guard is also one of the largest law enforcement agencies in the United States Government, particularly in DHS, and our law enforcement activity principally revolving around the maritime domain also includes information at ports, and we have over 360 ports for which we are responsible in addition to those miles of coastline.

In each of the ports and I will focus first, if I may, on the law enforcement intelligence collection activity. In most of the strategically and economically important ports of the United States, we have what are known as field intelligence support teams. These are law enforcement information collectors who work with not only the Federal counterparts, but the State and local counterparts in each of these ports. New York, for instance, they work with the New York City police and the police authorities.

Mr. SIMMONS. If I could interrupt for just 1 minute. But when you collect for law enforcement, is that shared with your intelligence folks?

Mr. SLOAN. Yes, sir. That is the point I was going to get at. All of this information that is collected, to include, I might add, the interview of the masters of ships who come from overseas who can give us essentially the lay of the land in the port that they just departed from, this information is then put into field intelligence reports, which not only go to-in a law enforcement capacity not only go to Coast Guard Intelligence Fusion Centers, but also to the Homeland Security Department.

When they arrive at our fusion centers—and as you might recall, I indicated we have one on each coast as well as a production center out in Suitland with the Office of Naval Intelligence—the information, where appropriate and authorized, bumps up against validated requirements that the Intelligence Community has to an-

swer. And that is where the nexus occurs, and then, of course, published into the larger community if it would answer an intelligence—validated intelligence requirement.

Mr. SIMMONS. I appreciate that. I know my time is going to run out.

Ms. O'Connell, you collect, you provide new information to the community; is that correct?

Ms. O'CONNELL. We do. We have got the six field intelligence units and the tactical intelligence centers out in the field where we collect information and then analyze it and put it back out into the operational components. For instance, in Operation Watchtower we work jointly with Coast Guard, Customs and Border Protection in order to get information and identify individuals that may be a threat coming in. Also on Operations Capistrano and Roswell, we are looking at those individuals who are coming in to the airports, getting, collecting information, and analyzing that, and then identifying individuals that pose a vulnerability.

The field intelligence units work with State and local Federal, State, and local and tribal authorities collecting intelligence, put it in Homeland Security intelligence reports, which we then bring into—some of them are brought into headquarters. Some of them are developed into intelligence information reports that go to the Intelligence Community. Other information is pumped out through the law enforcement components.

Mr. SIMMONS. Mr. Bortmes.

Mr. BORTMES. Again, all the information that we are able to put in the Intelligence Community channels is derived from our law enforcement authorities and done in the normal process of our duties in carrying out those authorities. For instance, at our ports of entry each day, as individuals are encountered, and, in fact, we realize that they might have, for instance, a record, a tied record or something along those lines, they are taken to a secondary examination. We are able to sit down with our colleagues from ICE, from the FBI or the JTTFs, go into a more in-depth interview to determine their admissibility. That information and what might be obtained from those interviews will then be forwarded out to our National Targeting Center and to the Office of Intelligence. We ensure that gets captured in Homeland Security information reports, intelligence reports, and sent down to the community through the Department. So that occurs. And it gets posted, regularly sent to the National Counterterrorism Center, et cetera.

The value added there, again, is that granularity, the ability to look at an individual up close. If they are denied admissibility into the United States and returned back, we have them for that time frame. So that is a unique piece of value added.

Mr. SIMMONS. Thank you very much.

The Chair recognizes the Ranking Member.

Ms. LOFGREN. I will be quick so that my colleague will also have a chance to ask her questions.

Last year there was an effort made to add an additional 550 Border Patrol agents and additional 200 immigration investigators, and again, in December, an effort to authorize 3,000 additional Border Patrol agents, for a total of 12,000 by 2010, along with a new training facility to expand capacity.

As the Executive Director of Intelligence Office at CBP, would you find these resources helpful to you when you are doing your job?

Mr. BORTMES. Border Patrol agents all represent to me a collector, a conduit of information.

Ms. LOFGREN. Thank you very much.

We have, we know, on the northern border, our 5,000-mile-plus northern border, at any given time we have between 200 and 300 Border Patrol agents. Do you believe this is an adequate force at the northern border?

Mr. BORTMES. I believe that the number of Border Patrol agents on the border is closer to 1,000. But—

Ms. LOFGREN. But they are post positions. So we have only got at any given time 200 or 300 physically there. So do you think that is adequate?

Mr. BORTMES. I don't believe anyone thinks it is adequate right now.

Ms. LOFGREN. Thank you very much.

The 9/11 Act mandated an additional 800 immigration enforcement agents over the next 5 years, but we have only actually funded 350. The 9/11 Act also mandated an additional 800 detention beds, but we have only funded, Congress has only funded, an additional 1,800. Do you think that this is adequate to deal with the flow that you have seen?

Mr. BORTMES. The question is again directed at me?

Ms. LOFGREN. Yes.

Mr. BORTMES. These are questions again, ma'am, that I believe are best answered by our operational folks, and I would like to take it for the record and have them respond to you and the previous question about adequate numbers on the northern border.

Ms. LOFGREN. That would be fine.

Ms. LOFGREN. And I think I will stop my questioning at this point and yield back so that my colleague Mrs. Lowey may ask her questions, and we can all get our votes in.

Mr. SIMMONS. The Chair recognizes the distinguished gentlelady from New York.

Mrs. LOWEY. Thank you. And I will ask it quickly because the bells are still going off.

I would like to direct it to Mr. Bortmes. You have heard us talk frequently about the fact that only about 2 percent of our cargo is being inspected while Hong Kong inspects 100 percent. I am sure you are going to say you are not satisfied with 2 percent, but can you tell me what is actually being done to remedy that? And why can't we move more quickly?

Mr. BORTMES. Ma'am, I believe you are really addressing the issue of physically inspecting all of the cargo. As you know, a great deal of the cargo from our perspective, CBP's perspective, is inspected. The records are looked at long before it is loaded aboard—the manifests.

Ms. LOWEY. Do you think it is adequate?

Mr. BORTMES. The efforts that I have seen so far and, again, it is our operational elements as opposed to our intel pieces. From what I have seen, the automated targeting system that is in place

is working extremely well at identifying those suspect cargos that I have to worry about as the Executive Director for Intelligence.

Mrs. LOWEY. If you had your way, would you move in more physical inspection, as you call it, or are you including a more advanced technology in that description as well?

Mr. BORTMES. Again, this is a question that if—I think if we bring our operational folks back to talk with you about in more detail, they can address it far better. But from all the discussions I have been part of, it is a combination of the reviewing them, the manifest information, better material, information arriving quicker, the nonintrusive inspection capabilities that are being developed. And there are plans for far more robust abilities to do that, and then actually devanning or having to inspect cargo, physically inspect the cargo. If you are doing all those things up front adequately and robustly, then the necessity for that latter part would not be there.

Mrs. LOWEY. But as I understand it, you just said you do have plans for more robustly inspecting the cargo.

So, Mr. Chairman, I would like to certainly request from the gentleman more detailed information, if you can follow up with us on that, because it is very disturbing to the average American when we continually read that Hong Kong is doing it, and we are not doing it, and we are all living at the edge these days. So I would appreciate that information.

Mrs. LOWEY. And I thank the panel again. I am sorry we have to run, but I thank you for your important work.

Thank you, Mr. Chairman.

Mr. SOUDER. [Presiding.] Thank you.

I have—let me first—you heard me ask the first panel that as I visited the many border crossings north and south, and fast pass lanes or whatever it is called in different places, when they put their scan card in, if there is a question, a little pop-up occurs, and the person then has run a check. And what my question is is in the different intelligence agencies, are you confident that, first, within DHS, all the information is getting there with an individual name? And then, secondly, is the entire system getting into that?

Now, the danger of having every single piece of intelligence available to everybody, if there is one leak, you compromise the entire system. But the question is why can't at least a pop-up occur if anywhere in any of our intelligence systems there is a question about this name, even if it is just wanting to know where they are moving? Are you confident that that information is getting into our systems at this point? Could each of you briefly comment on that? Because you each deal with slightly different types of things. Maybe start with CBP, and whether the Coast Guard is getting it if they have a boat, and then ICE if you are doing an investigation.

Mr. BORTMES. Sir, I am very confident that the information that is within the Intelligence Community on particular names, identifying data, the plus one data, et cetera, on those that we know are linked particularly to terror and then to criminal activity as well, that it is there. It is popping up. We have done, I think, efforts and strides have been made to make sure that it actually pops up in front of the CBP officer or the Border Patrol agent when they do

run that information check. So I am confident that every effort—that great strides have been made.

Clearly there leaves this hole of what you do as you are developing information, names that are being investigated, operations that are under way by the Intelligence Community. There are other names there that are not quite yet definitive or authoritative. We always worry about that. We take great strides within CBP that as we are associating or linking individuals with terrorist backgrounds to others to make sure that that information gets in the appropriate law enforcement and terrorist databases so that it is there, with the caveat that, hey, we are now looking at this individual linked to another in this particular way.

So great strides, I believe, have been made, and I am comfortable that the information the community has is getting there. You clearly always want it faster; you always want it better, clearer. And I know there are a number of initiatives throughout the community to make that happen.

Mr. SOUDER. Because you have seconds. Your agent at the line at San Ysidro is going to be backed up hours at almost any time of the day, so there is huge pressure in seconds. That is why it has to—even a 6-hour delay, if it is not instantaneous, we could miss somebody going through the border.

Before I follow up, let me clarify here, because you had some other—you had a question I want to follow up briefly. Is it CBP or ICE at our embassies that would have a DHS person doing a check, a background check? Is it ICE?

Ms. O'CONNELL. ICE has. We have attaches and assets overseas.

Mr. SOUDER. I just want to make sure. I couldn't remember which one it was. In Pakistan, when I was there recently, that is, at the front desk—this isn't just about whether we have agents at the border, this is an interrelated system inside the United States and externally. And the ICE agent had identified somebody on one of the lists, but the list of this person's name had like 12 variations, because it isn't just like Mark Edward Souder. Often they will have six names, will have an A and E turned around, will have two or three of the names here. Are you confident that at our borders, at the CBP or at the Coast Guard, or as we are doing the investigations, that all the different variations of the name are getting into the system as well?

Ms. O'CONNELL. If we have an ongoing investigation, and with the focus on antiterrorism national security issues, I am confident that the names are in the system. It may be the main name and then AKAs, also known as, attached to that. Many instances when individuals coming into the port of entry Mr. Bortmes can speak on this also—an inspector will look at that name, and it will possibly highlight it, and in instances would identify that person who would go into secondary, and then you would work out different names and other uses.

Mr. SOUDER. Let us say it is not an ongoing investigation, but a person on a watch list. We have a potential latent cell. Part of the way they move from just kind of casual watch to an aggressive watch to whether it is an ongoing, or whatever information you put together, so, for example, if we think that they are located in someplace in Indiana and haven't moved, but then we see this person

who we really were—just casually had on the list because of his relationship to, say, several individuals, all of a sudden we see them move at a border place in Texas, then we see them move up by Buffalo, then we see him at an embassy, it suggests that there may be a pattern. But without kind of core information, you can't even get to the point.

And so I understand if there is an active investigation, I have seen them pull into secondary on that. I am just wondering how far we are moving on this, and are we getting enough information in the system to be proactive other than an ongoing investigation?

Ms. O'CONNELL. If they are identified as a lookout, yes, I am confident that they are in the system.

Now, when you mentioned about movement between States, keep in mind that the identification of an individual in the system would be when they are coming in through the border. So there is obviously no checks going from State to State. But I am confident that that individual, if they rise to the level of putting them in as a lookout, that they would be in there, yes.

Mr. SOUDER. That is assuming that they are a citizen of the United States. We would have no way of seeing whether a person who has either overstayed their visa or is on a visa is moving inside the United States?

Ms. O'CONNELL. It is not just individuals that are U.S. citizens that would be put in the record that inspectors would identify coming through the border. It is also other individuals, lawfully admitted permanent residents, visitors, students.

Mr. SOUDER. In the Coast Guard is there adequate technology now on—in most of our vessels to be able to read it if they pick somebody up or detain somebody?

Mr. SLOAN. Well, sir, if I could just back up 1 second. The Coast Guard obviously doesn't have a border check, if you will, but we do have a responsibility to vet the names of all crew members of certain vessels over a certain tonnage that must be supplied to us 96 hours prior to the arrival in the United States; otherwise, the ship can't enter. And we vet those names not only against the law enforcement database, but intelligence database that you can imagine we have available to us, to include the Terrorist Screening Center.

The names, if they provide a hit, clearly the ship will be boarded before it arrives in the United States and the individuals be dealt with appropriately to the degree that it is a law enforcement matter or somebody who shouldn't be coming into the country. But also, we provide some degree of check and balance. We want to make certain that the names that are being supplied to us and the passport information and the last port of call information and the origin of the particular crew, we will actually inspect vessels to verify before the vessel arrives to make certain that the information that was provided is, in fact, accurate.

Mr. SOUDER. Two of the biggest potential areas for terrorists to hide are in Detroit and also crossing in upstate New York. I am from Fort Wayne, Indiana. I have been to Michigan many times, been at the border crossing many times there as well as other reasons, certainly the St. Clair River, Lake St. Clair. The islands there are such at you can swim in 5 minutes between them, and the Coast Guard does, in fact, have primary responsibility at that point

if a boat is coming into our waterway. The same thing in the St. Lawrence Seaway, that—and what I am wondering is, if the—do you, if—do you have the capability if you find that, or do you then if you have a suspect take them into another agency, have to run them to shore? Are we moving towards having some sort of onboard vessels? I know for narcotics we do in the Caribbean, but I am trying to think as we look at some of the Great Lakes areas and the St. Lawrence River, too, as well as the area coming into Seattle where the Coast Guard has a huge waterway with lots of San Juan Islands and everything.

Mr. SLOAN. Yes, sir. The San Juan Islands are a perfect example as are the Great Lakes. But I would point out that although the appearance of Coast Guard efforts in the Great Lakes and the San Juan Islands would not look like what is going on in the Florida straits and the eastern Pacific and the Caribbean, the same amount of attention is being paid to it.

And I recall from some of the discussion that occurred in the prior panel, the relationship with Canada is particularly important. We do have representatives of the Coast Guard who operate out of Ottawa, we have law enforcement agreements with the Canadian authorities, and we actually have a Canadian representative in our National Maritime Intelligence Center. So the link and the exchange of information with the Canadians is as important to cue our activities relative to those issues as anything else.

Mr. SOUDER. I have one additional question, if I may, Mr. Chairman, that one of the things as we have looked at the border challenge is that—is the networks that work in between the borders. Particularly we have looked at OTMs as a higher risk, theoretically at least, in terrorism, other than Mexicans, but it could be any number of smuggling organizations. And the question is are we proactive?

We have tried to increase legislation on coyotes, for example. In San Diego, Congressman Issa said that the penalty was 6 months, and it took 9 months to get to trial, so nobody was investigating that. Yet, in fact, for major smuggling organizations it is much going to be like Panama Express. In other words, when somebody—we don't believe at this point that the Veterans Administration files were stolen for that purpose; it appears to be some college kids, and we are watching that very closely.

But much of identity theft in the United States is related to trying to get the Social Security numbers and IDs; that when somebody does a package to come across the border, whether it be an other than Mexican or a Mexican coming across, and they purchase this, often somebody is providing a map, providing a van to pick them up, providing a false green card, that with the Social Security number, and obviously work sites. As they come into Indiana, in my district, which is the number one manufacturing—and the bottom line is we have a number of people there or we wouldn't be making it in manufacturing.

I am not taking immediate sides on that question. I am asking, do we have a systematic way? Because we clearly have an "interterior" smuggling organization that has places they rent the vans, buy the vans, markets. We had three green card manufacturers taken down in 30 days in my district. Is this being investigated

in holistic? Because this is a gaping hole in our system over the last couple of years.

Ms. O'CONNELL. I can speak a little bit about that on the operational side of ICE. The investigations program has just identified identity and benefit fraud units that will actively work within the interior of the United States. I don't want to state a number. I have got one in my head, but I don't know it 100 percent. So anyway, identity and benefit fraud units.

Then, on the intelligence front, I have got a unit at headquarters that specifically specializes in human smuggling, in trafficking, immigration fraud types of things that have identified a number of areas. As a matter of fact, we had a case related to the vans that are moving people from the southern border up into the northwest or the northeast coast.

Also, the field intelligence units that are out there on the ground work daily with the SAC offices, the special agent in charge offices, and get information in and work on and analyze different organizations and try to pull those details together, add the classified information, and try to identify target packages for those smuggling organizations.

Mr. SLOAN. Sir, may I comment on that? Clearly asymmetrical immigration is a concern to the Coast Guard. This is where SIAs or people who might have a terrorist link or associations would come in by absconding or deserting or being a stowaway on a vessel.

But your point relative to identification, I think, is an important one for the Coast Guard. We issue merchant mariner licenses for hundreds of thousands of individuals, and I think it is important for me to testify to the fact that over the last 2 years, actually over 2 years, the Coast Guard Investigative Service along with the Federal Bureau of Investigation and the cooperation that we get from our partners in Homeland Security, Defense Department, and the Intelligence Community, has been vetting close to a quarter of a million merchant mariner documents to make certain that they are in the hands of the correct people.

In fact, I couldn't even tell you in an open session that we have associated nine individuals—it doesn't seem like a lot out of a quarter million, but it is significant—who actually have associations with terrorism over the course of that period of time. It is an effort that continues, ongoing, and actually our regional centers that issue mariner documents are now trained to go through that program before mariner documents are actually allowed to be issued.

Mr. SIMMONS. [Presiding.] I want to thank this panel for their testimony. It has been extremely interesting and thought-provoking. I realize that some of our panelists have stayed beyond their anticipated time of testimony, and particularly you, Mr. Sloan. So we thank you very much. It has been very informative.

And at this point I will excuse the second panel and invite our third panel to come forward.

The third panel is made up of two individuals, Mr. Michael W. Cutler from the Center for Immigration Studies, and Mr. Michael O'Hanlon of the Brookings Institute. I welcome both of you gentlemen to testify. I think you have already determined that we have your written statements in our notebooks, we have reviewed those

written statements prior to today's hearing, so feel free to cherry-pick the most cogent points to present to us so that we can get into the questions and answers, which is often very informative for the subcommittee. And, again, I thank you for being here.

And I would ask the staff to secure the door so that we can hear the testimony.

Thank you, gentlemen. C comes before O. Why don't we proceed on that basis. Mr. Cutler.

STATEMENT OF MICHAEL W. CUTLER, FELLOW, CENTER FOR IMMIGRATION STUDIES

Mr. CUTLER. Thank you, sir. Chairman Simmons, Ranking Member Lofgren, Members of Congress, ladies and gentlemen, I welcome this invitation to appear before you today at a hearing that I believe is of critical importance to the safety of our citizens and indeed to the very survival of our Nation.

The gathering of effective intelligence is essential for effective law enforcement and for issues relating to national security. Nothing can be of greater significance than the issue of developing effective intelligence; that is to say, the culling of accurate information and understanding its place in the overall picture.

Intelligence should be thought of as being comparable to the way that a digital photograph is made. A digital photograph is comprised of a huge number of elements or pixels which are placed in the proper location to paint the clear picture. As the number of pixels increases, the clarity of the photo increases proportionately. So, too, the clarity of the picture painted by effective intelligence is proportionate to the quantity and quality of the intelligence nuggets or bits of information that can be gathered and placed into their proper position in the mosaic that makes up the overall pictures. And the ability to understand the significance of each kernel of information also contributes to the clarity of the picture that the intelligence will create.

But effective intelligence also requires that it be disseminated quickly to the ultimate users of the intelligence. It has a short shelf life, and, therefore, where critical intelligence is concerned, time is of essence. Pixels do not lose their value over time, but intelligence does.

Additionally, it is important to understand that human nature often creates additional hurdles. Approximately 400 years ago, Sir Francis Bacon said, knowledge is power. That statement is as true today as it was when he first said it. Various Federal agencies realize that intelligence that they possess provides them with a certain amount of power, and therefore their members have been reluctant to share their knowledge with other agencies. However, to the point that intelligence is to protect our Nation, intelligence is critical today that will become worthless in a very short period of time if it is not freely and expeditiously shared with those who possess the need to know.

Rather than to continue to read my prepared statement, what I do want to do is point to something that I did talk about in my prepared statement that I would like to paraphrase.

You know, I have heard today members of the subcommittee talk about the idea of allowing people in to work because we are con-

cerned about terrorists and we are concerned about the border. But the point of fact, the border alone won't solve our problems. I have often spoken about the need to think of immigration law enforcement as a tripod, with the inspectors who enforce the immigration laws at ports of entry, the Border Patrol between ports of entry, but you need to have enough special agents to enforce the immigration laws from within the interior of the United States so that we have a seamless coordinated effort.

I share Ms. Lofgren's concern about the numbers of people that have been proposed to be hired. In fact, in May of last year I testified at the Immigration Subcommittee about the fact that while Congress had authorized the hiring of 800 new special agents, the administration only hired 143, or wanted to hire 143. The number was eventually increased.

But this has been going on for the longest time. There was no response to the first attack on the World Trade Center from an immigration perspective, and today we are in a situation where we are not even giving foreign language training to the special agents who are supposed to be investigating illegal aliens operating within our country. And, quite frankly, if you can't communicate with people, then you are unable to investigate those people. And the day-to-day routine enforcement of the immigration laws is critical to our security because it is during the routine enforcement of the laws that you will encounter potential terrorists and develop information.

Twenty years ago—and this is also my prepared testimony—I was doing a rather mundane and routine job. I was assigned to the squad that was responsible for investigating locations that were knowingly hiring illegal aliens, and we arrested a bunch of people working illegal in the United States in a diner at Staten Island. One of the individuals whom we arrested turned out to be a citizen of Egypt; and we went back to his apartment in order to get his passport, which was the standard procedure. What we found were bags filled to the brim with food coupons and dog food coupons and detergent coupons. And we could not understand why he had this, and he had no adequate explanation.

Mr. CUTLER. We had no place to go with that information and no place to make inquiries. We ultimately deported that guy. And months later I was shocked to listen to a television news report about how the PLO had sent some of their folks into our country to commit coupon fraud to fund terrorism in the Middle East.

It is important that if we are going to secure our country and protect our people, that we have enough agents and that we understand who we are really dealing with. And quite frankly, I am very much concerned when I hear stories about guest worker programs that would provide official documentation to illegal aliens whose true identities we don't know. There is no way that we can develop a system that will deal with millions of people who have no way of proving who they are, where we would wind up giving people official identity documents without knowing whether or not these are bad guys, because I would like to remind you that the job of a terrorist, just like a spy, is to hide in plain sight, and if we give identity documents to people without knowing their true identities, we make it that much easier for them to hide in plain sight.

And finally, I want to make one point, if I may. I have heard some of the folks today talk about interior enforcement, and they are right, but they have limited it to people who have been identified on the border who fail to show up, the so-called OTMs who failed to appear, and employer sanctions.

A big issue is immigration benefit fraud. Janice Kephart was the counsel to the 9/11 Commission, and I provided testimony to her, and she did a little bit of a study and found that there were over 90 terrorists that were identified in our country operating during the decade leading up to 9/11. Of those 90-odd aliens, some 59, or about two-thirds, had used immigration benefit fraud either to enter into the United States or to embed themselves in the United States once they got here.

If we don't address immigration from all aspects, then I think we are going to have a very serious problem. And intelligence is only a part of the metrics; we also need to look at the visa waiver program as well.

I know my time is up. I thank you for your indulgence, and I look forward to your questions.

Mr. SIMMONS. Thank you for that insightful statement. We appreciate the breadth of experience you bring to the issue.

[The statement of Mr. Cutler follows:]

PREPARED STATEMENT OF MICHAEL W. CUTLER

Chairman Simmons, ranking member Lofgren, members of Congress, ladies and gentlemen, I welcome this invitation to appear before you today at a hearing that I believe is of critical importance to the safety of our citizens and indeed to the very survival of our nation.

The gathering of effective intelligence is essential for effective law enforcement and for issues relating to national security. Nothing can be of greater significance than the issue of developing effective intelligence, that is to say, the culling of accurate information and understanding its place in the overall picture. Intelligence should be thought of as being comparable to the way that a digital photograph is made. A digital photograph is comprised of a huge number of elements or pixels, which are placed in the proper location to paint a clear picture. As the number of pixels increases, the clarity of the photo increases proportionately. So too, the clarity of the picture painted by effective intelligence is proportionate to the quantity and quality of the intelligence or nuggets of information that can be gathered and placed in the proper position in the mosaic that makes up the overall picture. The ability to understand the significance of each kernel of information, also contributes to the clarity of the picture that the intelligence will create.

Effective intelligence also requires that it be disseminated quickly to the ultimate users of the intelligence. It has a short "shelf life" and therefore where critical intelligence is concerned, time is of the essence. Pixels do not lose their value over time, intelligence does. Additionally, it is important to understand human nature. Approximately 400 years ago Sir Francis Bacon said, "Knowledge is power." That statement is as true today as it was when he first said it. Various federal agencies realize that intelligence that they possess provides them with a certain amount of power and therefore their members have been reluctant to share their knowledge with other agencies. However the point to intelligence is to protect our nation and intelligence that is critical today will become worthless in a very short period of time. That is why it must be freely and expeditiously shared with those who truly possess the "Need to know."

It is also worth noting that intelligence comes from many sources. It comes from electronic surveillance and other high-tech means and also comes from low-tech sources; informants who are willing to talk and field personnel who make observations in the field when they find documents and other materials that yield valuable information. That is why it is essential that field agents understand that they have a vital role to play in the development of intelligence. They are our government's eyes and ears on the ground and their discoveries and insights are invaluable. Because of this, not only must they be provided with accurate intelligence to help them do their jobs, they must also be provided with an opportunity to share their observa-

tions with intelligence analysts who may be able to take seemingly unconnected observations and even ″hunches″ and weave them into a tapestry of effective intelligence.

I would like to share with you an experience I had approximately 20 years ago which is as relevant today as it was when it occurred. Back then I was assigned to a unit of the former INS in New York that was charged with finding illegal aliens who were working illegally in the United States. My colleagues and I were in the process of arresting a number of illegal aliens who were working in a diner in Staten Island, New York when one of the illegal alien employees, a citizen of Egypt, fled the restaurant when he realized we were present. He made an exhaustive although ultimately futile effort to evade us and we succeeded in taking him into custody. We took him back to his apartment to attempt to retrieve his passport, a standard procedure, since his passport would be helpful in positively identifying him and determining his date place and manner of entry into the United States. His passport would also be useful in arranging for his deportation should the immigration judge order him deported. With his consent, we entered his apartment and were surprised to find that there were numerous department store shopping bags lining one of the walls in his sparsely furnished apartment. These bags were filled to the very top with hundreds upon hundreds of coupons for all sorts of merchandise ranging from dog food to detergent to cereal. He had no meaningful explanation for this but we had no way of making any inquiries to understand the possible significance of those coupons. We retrieved his passport and he was ultimately deported. Several months later I was shocked to learn from a televised news program that the PLO had sent a number of their people to the United States to engage in coupon fraud in order to fund terrorism in the Middle East. Purportedly this tactic netted the PLO millions of dollars in ill-gotten funds. This young man who was seemingly engaged in nothing more sinister than washing dishes in a diner was apparently an operative of a terrorist organization. We had him in custody and we deported him, losing a potential treasure trove of intelligence from a terrorist operative or at least terrorist sympathizer. To this day I wonder what intelligence we might have gained had we understood the significance of the shopping bags filled with coupons on the day we arrested him. I also wonder where he is now and what efforts he might be engaged in that pose a threat to our nation or our allies today.

If the news media understood the significance of coupon fraud, why did not the former INS make certain that their field agents were aware of such activities? Keeping our law enforcement personnel in the dark not only keeps them from being as effective as possible at carrying out their day to day duties, it also keeps them from recognizing situations that may make their jobs more hazardous and also prevents them from pressing an investigation further, where the results might yield highly critical information.

This is also the reason that I am greatly concerned when I hear members of the administration talk about the need to conduct field investigations where critical infrastructure facilities are concerned such as airports and nuclear power plants but where limited resources make routine immigration law enforcement a non-priority. Certainly it is vital that we make certain that we make vital infrastructure facilities as secure as possible and not only where hiring illegal aliens is concerned, but from other perspectives as well. However, as we have seen in a number of terrorism investigations over the past several years, many of the suspected terrorists who have been identified and arrested have not worked as such sensitive locations as airports and nuclear power plants, but had relatively ″pedestrian″ jobs driving taxi cabs and ice cream trucks as well as teaching in schools and working in used car lots. The goal of terrorists is to ″hide in plain sight″ or in the parlance of the 911 Commission, to ″embed″ themselves in our nation.

The routine enforcement of immigration laws can provide our government with the opportunity to cultivate informants and provide essential insight if our agents are properly briefed and properly debriefed. They need to be encouraged to come forward whenever they make observations that arouse their suspicions or curiosity and need to have an easy way to report on their findings in the field.

Finally, we also need to provide our field personnel at ICE with appropriate training, including foreign language training. When I attended the Border Patrol Academy in 1972 I was required to successfully complete a Spanish language training program as were all enforcement personnel who were hired by the INS. Today, incredibly, that foreign language training is not only not required, it is not even offered for newly hired special agents of ICE. As I have stated at previous Congressional hearings at which I have testified, you simply cannot investigate people you are unable to communicate with. It is absolutely essential that our ICE personnel be given Spanish language training and they also need to be trained in various strategic languages such as Arabic, Farsi and Urdu to name a few. They also need to

be given on-going training to properly identify fraudulent and/or altered identity documents, since these documents are the linchpins that hold the immigration system together. From what I have been told, this training is far from adequate at present, and this is not in our nation's best interest. I would remind you that the terrorists who attacked our nation on September 11, 2001 used multiple identities and false documents as well as documents that were improperly issued to them, in order to embed themselves in our country as they prepared for the horrific attacks that they launched against our nation and our people on that terrible day.

I look forward to your questions.

Mr. SIMMONS. Mr. O'Hanlon.

STATEMENT OF MICHAEL O'HANLON, SENIOR FELLOW IN FOREIGN POLICY STUDIES, BROOKINGS INSTITUTION

Mr. O'HANLON. Thank you, Mr. Chairman and Congresswoman. It is an honor to be here. I will try to be very quick. I just want to make one broad comment. Having listened to the great expertise this morning and learned a lot myself, I think it highlights, if you put it all together, one broad observation, which is that intelligence is very important clearly at land border crossings, but we are never going to have good enough intelligence to find individuals and be able to target Border Patrol assets accurately. Our only hope using intelligence really is at the places where people come through official points of entry. That is where we spotlight attention.

So this leads me to a couple of broad conclusions. While I think we do need to keep working on intelligence capability for land crossings, we are never going to know enough about coyotes and about preferred points of entry and so forth to have that be a reliable way to stop people. It takes very good luck to find someone, it is going to always take very good luck, which leads me to think we need to continue to increase capacity first to seal those borders to the extent possible, even though we all know it is not theoretically truly possible.

Secondly, to be able to do a very good job at official points of entry in certain areas where we are not doing very well right now, I think we need to be making inquiries of a lot more passengers inside of cars at official points of entry and not simply hoping that the driver's identity gives us a sufficient tip as to whether that car is suspicious.

And I also think that, in keeping with some of the comments that have just been made, we do need to think hard about better forms of identification for American citizens, standards for driver's licenses, possibly even national ID cards.

The 9/11 Commission, I think, was quite convincing on these points. Americans have a very strong civil liberties concept on our Nation's history and in our thinking, and therefore, there is always pushback against this sort of idea. But I think tougher standards on driver's licenses and other forms of identification are critical, because we have to always be looking inside the country, too, because we are going to have people keep crossing across the land borders. That is never going to be sealed enough, and we can't assume that intelligence is going to ever get good enough to solve that problem.

So, official points of entry, whether it is people coming through or cargo coming through, we need more capacity, more capacity for land borders to reduce the likelihood of people getting through because intelligence is not going to help us pinpoint to know exactly when and where to look for whom. We are going to have to try to

increase general capability across that land border. And in general, on sort of a broad unfocused note, but more, more, more. We need more capacity in general because intelligence is never going to be smart enough to tell us when and where to look for whom. And I will stop with that simple point.

[The statement of Mr. O'Hanlon follows:]

STATEMENT OF MR. MICHAEL O'HANLON

Border protection is a critical pillar of homeland security. It keeps dangerous people and materials out of the country before terrorists can even get into a position to attack. In other words, it is preventive in nature-and thus represents an optimal approach to homeland security policy, as my coauthors and I argue in our new Brookings book, Protecting the Homeland 2006/2007.

Border protection should not be principally viewed as a literal defense of the nation's perimeter. It is not tantamount to the creation of a moat around American borders. Rather, it is a set of efforts that exploits the fact that people and goods are relatively easily monitored when they arrive at checkpoints. In other words, movement across borders allows spotlighting to occur. To be sure, some border protection functions represent something closer to the direct physical protection of borders-most notably, the efforts of the border patrol along the long perimeters of the United States, as well as some activities of the Coast Guard and the Department of Defense. But the spotlighting role is even more critical. Its failure is what allowed the 19 September 11 hijackers to enter the country. Similarly, the nation's inability to know accurately what goods are coming across its borders have much more to do with holes in the official inspection process-that is, with the spotlighting function-than with the weaknesses of our national walls.

Done right, border security activities can offer additional benefits beyond the homeland security sphere, meeting another one of our four recommended guidelines. Digitized and computerized borders can allow more dependable and rapid movement of people and goods in and out of the United States. They can also provide better knowledge of where ships and goods are when in transit. That in turn translates into, among other things, a greater ability to prevent or respond quickly to other dangers such as piracy and ship accidents that can afflict trade and travel. This should be the goal of tighter border protection; we must avoid the risk of borders turning into chokepoints. Homeland security efforts should reinforce, not compete with, economic competitiveness.

America's geography generally helps in the effort to monitor borders and to use them as a means of funneling goods and routing people through places where spotlighting is possible. But the country has two long land borders that remain very difficult to guard. And they are far from the only main challenge facing this domain of homeland security. This testimony considers a number of relevant problems, as well as the general matter of aviation security, which is in part a matter of border protection. Its conclusions, in short, are that there is no magic bullet for keeping illicit goods and people out of the country, and no easy analytical way to deduce what level of increased inspection or monitoring capacity would be sufficient for national security. Ongoing efforts since 9/11 have been headed in the right direction, however, and the gradual increase in capacity for monitoring borders as well as goods should continue. In addition, some additional policy steps such as much more uniform standards for drivers' licenses are called for.

Monitoring of People

There has been progress in regulating and monitoring the movement of people into the United States. It is much harder for individuals to gain access to this country while disguising their true identities, particularly for those on terror watch lists. Notably, someone trying to fly into an airport from abroad is unlikely to get through under their own name if on a terrorist watch list, and indeed is unlikely to be allowed entry even under a false name if his or her fingerprints are already on file. This is a major step forward since 9/11.

Other useful measures have also been adopted. For example, the Student and Exchange Visitor Information System (SEVIS) now appears to be functioning quite well in helping track those foreigners in the United States on student visas. Those who overstay visas can be more quickly identified and located.

Biometric indicators are used increasingly to control foreign travel. The U.S.-VISIT program requires foreign visitors from all countries except Canada to submit to fingerprinting (of right and left index fingers) and digital photography upon arrival in the United States. A complementary program, the State Department's Bio-

metric Visa Program, requires that fingerprints be taken of visa applicants before travel to the United States and compared to those in a DHS database (known as IDENT) consisting of some five million individuals, some of whom are ineligible for American visas. Upon arrival in the United States, visitors' fingerprints taken by DHS under the U.S.-VISIT program are also checked against those on the visas to confirm that the individual in question is indeed the one to whom the visa was granted.

To reduce the chances that individuals planning terror attacks will find a legal way into the country and then overstay their visas, it would be useful to record exits in real time from the United States. Those remaining longer than they should could then be more easily identified and pursued (as the 9/11 Commission recommended).

A remaining problem in air travel security arises from what is known as the Visa Waiver Program. Until digitized passports with biometric indicators are widely used by qualifying countries, the visa waiver program (VWP) will continue to constitute a substantial loophole in U.S. border security, given the prevalence of stolen and forged passports around the world. While individuals entering under VWP are still checked upon entry, there is less ability to interview them thoroughly when required if such activities must be carried out at the actual border.

This circumstance argues for some other level of screening of individuals from VWP countries before they can board flights for the United States. For example, DHS security personnel could be deployed at foreign airline check-in counters in certain VWP countries (as Israel does with El Al flights).

Terrorist watch lists also need to be improved. The United States is presently consolidating some dozen watchlists into a single terrorist screening database (TSDB) using more extensive data in the terrorist identities database (TID) that is also now being constructed. (The effort to construct the TID began with the previous gold standard of terrorist watch lists, the State Department's TIPOFF list. The list was subsequently scrubbed and expanded by consolidating it with other databases.) Some new specialized watchlists with limited information (easier to share with people not possessing security clearances) are being created as well, such as the Secure Flight database to assist in monitoring aircraft passengers and improve the accuracy with which their names are matched against those of suspected terrorists. Thankfully none of the watchlist consolidations have turned into complete fiascos, as the FBI's attempts to computerize its case files unfortunately has. But the consolidation and integration process remains slow. For example, Secure Flight had not yet been tested as of September 2005.

Even digitized passports with biometric indicators cannot track new recruits with no known ties to terrorist organizations. It is therefore important to recall that there are inherent limitations to these sorts of terrorist tracking efforts. This is one clear example of the reason why a multi-tiered strategy for homeland security is imperative.

The problem with screening people also works in the opposite direction--keeping good people out while they wait for security reviews to be completed. This is true for example for foreign students, who when screened through the so-called Visas Mantis program have had to wait months for their visas in many cases. Improvements have been underway in these programs, including allowing students to get a single visa for an entire period of study (rather than requiring annual renewal). But there are still long delays. This problem also applies to individuals trying to enter the country to conduct business, seek medical care, or pursue other important matters.

The student problem has not truly become severe. While the 2003/2004 academic year did register a 2.4 percent decline in foreign students relative to the year before, the number of foreign students remained greater than in 2000 or any year before. Moreover, numbers of applications from the Middle East to U.S. graduate schools actually increased in both the 2003-2004 and 2004-2005 academic years (while numbers from China, India, and Korea continued to fall). Indeed, the overall number of foreign students in the United States was 4.5 percent greater in 2004/2005 than just before the September 11, 2001 attacks, though there was a decline of 14 percent in Middle Eastern students. And the U.S. figures were not notably worse than those witnessed in the United Kingdom. That said, the problem could again intensify--and could affect some of the most talented individuals in the broader foreign student pool, convincing disproportionate numbers of them to go elsewhere. Further measures to address this problem, such as increases in government capacity for processing such paperwork, are therefore warranted.

In situations involving certain non-western countries, American technical and financial help may be needed to ensure good border security and travel controls. The simple fact of the matter is that the United States has a greater interest in tracking the movement of many terrorists than do developing countries. Even when that is

not the case, many countries will not have the resources to do all they should given the urgency of the threat. Seen in this light, President Bush's June 2003 East Africa Counterterrorism Initiative (EACTI) is a good step in the right direction. It provides $100 million to improve border control, police, airline security, and related homeland security operations in a region that has been hit hard by terrorist violence. The latter includes the 1998 U.S. embassy bombings in Kenya and Tanzania and the 2002 attacks on a hotel and airline in Kenya (the latter thankfully not successful), not to mention ongoing civil strife in places such as Somalia. This is enough money to make a real difference in a region of relatively low incomes. But these funds were apparently taken in large part out of existing programs, meaning that their net beneficial effect is difficult to ascertain. And similar programs are probably needed in other regions such as Central Asia.

Ensuring adequate capacity to screen individuals and issue visas, as well as proper means for verifying their identities, helps the United States beyond the homeland security arena. It can expedite the movement of people into the country who can contribute to the economy, and who can ideally become goodwill ambassadors as well as important contact points for the United States once they return home. Whenever a homeland security program can have additional benefits beyond that immediate objective, it is especially worthy of serious consideration and serious support.

The Special Problem of Land Borders

The preceding discussion pertains generally to the movement of individuals to and from the United States. But monitoring the movements of people at land borders poses special problems. It also offers unique opportunities, underscoring our theme about the need for greater international cooperation in the ″homeland″ security effort. To the extent Canada and Mexico make it hard for terrorists to use their countries as staging bases or waystations, the United States benefits from an added line of defense of its own country. That does not make its own border enforcement job unimportant, but it does allow a somewhat greater (and more realistic) margin for error at that inherently difficult line of defense. If Canada and Mexico improve their own monitoring of persons traveling into and out of the country, only modest additional improvements may be needed in border security along the U.S.-Canada frontier, and other lines of protection in the broader homeland security arena may become more effective.

The United States has 216 airports, 143 seaports, and 115 land facilities that are official ports of entry, at a total of 317 places. Those land facilities generally involve car and truck traffic that is especially difficult to regulate. In addition, of course, land borders are very hard to control in between official points of entry. At many official checkpoints, passengers in cars are not checked as long as they are in vehicles with legitimate license plates. This policy should be changed. Care must be taken to do it in a way that does not seriously slow movement at checkpoints, with resulting consequences for commerce as well as convenience of travel. That suggests that the change in policy will have to be gradual to allow time for more inspectors to be hired and new procedures to be developed (such as adding lanes at checkpoints). Given typical car passenger loads, it may be necessary to increase staffing by as much as 100 percent.

Open land borders are also a serious problem. For example, U.S. land management agencies are responsible for the 30 percent of the borders owned by the federal government. Yet they have only 200 full-time law enforcement officers, a number increased by just 20 percent in the first two years after September 11. Such numbers cannot begin to credibly monitor or prevent off-road border crossings.

Such limited vigilance of U.S. land borders is a mistake. It can deprive the country of the opportunity to ″spotlight″ people effectively at official points of entry, thereby blunting one of the very best homeland security tools that the United States and the international community in general possess. There are relatively few dependable ways to search for terrorists among the huge throngs of individuals on the planet; this needle-in-haystack effort requires some means of rendering people visible, and official border crossings can do that. So it is especially important to ensure that individuals pass through such locations when traveling.

Take for instance the sparsely guarded Canadian border, which can be an important means of entry. The Patriot Act led to a tripling of the number of U.S. agents along that border, but the total remains just under 1,000 for an enormously long and porous border, and there is little reason to think the number adequate. The United States also needs an integrated plan involving increased, random patrols and better equipment for surveillance and mobility for the U.S.-Canada border, as well as better cooperation with Ottawa in this effort. There is movement in the right direction. DHS is developing a way to have response capability anywhere within an hour of notice of a problem, and to improve monitoring as well. This might not help

with the "lone wolf" terrorist sneaking through the woods, but could pick up illicit vehicle movements or groups of individuals. Five DHS bases near the Canadian border are being created to help in the effort. Overall, this border is better protected than before, and will soon be monitored even more effectively. But the absolute numbers of U.S. capabilities are still extremely modest, suggesting an enduring problem.

Although few Canadians would pose major terrorism-related concerns, Canada's efforts to monitor its own borders against terrorist infiltration are wanting in a number of areas. For example, its coast guard does little to monitor Canada's long shorelines and cruise ships coming ashore do not have passenger manifests examined. This underscores the importance of Canada improving its own regulations on individuals visiting the country, but also means the United States must assume that foreign terrorists may try to reach this country via our northern neighbor.

A greater worry is the Mexican border, where despite the presence of almost 10,000 border agents, an estimated 4,000 illegal aliens cross per day. They are mostly Latinos, but also include individuals from countries such as Afghanistan, Egypt, Iran and Iraq with a greater corresponding risk of possible terrorist infiltration. Intelligence reports express concern that al Qaeda may indeed try to exploit the porosity of this border and infiltrate operatives through it.

A rough benchmark for the above proposals to increase monitors at borders is that adding 1,000 employees costs the government $100 million. So the costs associated with the above proposals might be roughly $1 billion a year, if the doubling of inspectors recommended to monitor passengers in vehicles crossing the border were matched by comparable increases in other aspects of the border protection effort. Accurately estimating the appropriate number of additional inspectors is beyond the scope of this analysis, but the above number gives a reasonable ballpark. The number of inspectors has grown by 5,000 over the last decade, with some beneficial effect on estimated infiltration rates. Indeed, it possibly reduced them by one-third, though it is admittedly difficult to be sure of the exact numbers as well as the true causes of any decline. It makes sense therefore to continue on the same trajectory while also introducing new operational procedures and new technologies--such as UAV patrols, the sea wall near San Diego, and America's Shield Initiative involving multispectral sensors and cameras as well as magnetic and seismic detectors. The Bush administration's idea of using National Guard forces as a temporary means of supplementing DHS personnel at the borders seems in this light to be a good idea.

The right policy is to start increasing border patrol personnel year by year in significant numbers and then attempt to modify procedures to improve border monitoring. As experience is gained, it can then be determined more accurately how many will be enough. Unfortunately, the Bush administration's request for additional border agents in 2006 totaled just 210 individuals, a far cry from the scale of increase that would be appropriate, given the present porous nature of the country's perimeter. But Congress wisely added $600 million to the president's request in this area, enough for 1,000 additional agents.

The database used by DHS's Border Patrol, IDENT, is not fully integrated on a national scale with other databases. IDENT uses a photo and two fingerprints, whereas the FBI's IAFIS (or Integrated Automated Fingerprint Identification System) uses all ten fingerprints. Reportedly, all U.S. Border Patrol stations now have interoperable systems capable of accessing IAFIS records and cross-checking the Border Patrol's IDENT entries against those records. But Border Patrol agents cannot access the consolidated name-based terrorist watchlist maintained by the Terrorist Screening Center at their stations.

Another problem is that the consular identification cards issued to their own citizens by some foreign governments, including Mexico, can be fraudulently obtained fairly easily. They are often used for identification in the United States. Lax standards for such cards cannot be tolerated. The United States may need to consider contributing seed money to encourage Mexico in particular to develop more rigorous and real-time databases of possible terrorists as well as better ID technology of its own. At present, the United States has a plan to require visitors crossing the Canadian or Mexican borders to present a passport or one of four other hard-to-counterfeit documents. But that plan is not due to be implemented before December 31, 2007.

Summing up, the land border security problem poses three special challenges. One, making sure that smaller border crossing posts receive up-to-date technology to become full participants in new efforts such as U.S.-VISIT, is mostly a matter of taking the problem seriously and providing adequate funds. A second, improving screening of individuals in cars--and working toward a standard by which all who pass through a land border are checked-is more demanding conceptually, though

surely doable. It will take new procedures not yet developed. They could slow crossings dramatically, however, so considerable work is needed to add inspectors and increase the numbers of lanes at key crossings. Third is a problem for which solutions have not yet been successfully conceptualized, even in theory--closing down U.S. land borders to illegal infiltration, which is of course linked to broader U.S. immigration policy. More technical and human resources to monitor borders are generally well-advised to mitigate the problem, but are unlikely to solve it--again underscoring the need for a multi-tier approach to homeland security that begins by pushing America's own borders ″outward″ and improving cooperation with other countries' parallel homeland security efforts.

There is clearly also a major benefit to improving border monitoring outside the homeland security domain. It is an important means of reducing illegal immigration, with all of its associated economic and political repercussions. Thus, focusing on land border controls within a homeland security strategy is consistent with the principle, as presented in the introduction, that the United States should be especially keen to pursue programs with multiple benefits. Indeed, the United States and Canada might push this logic one step further and consider another crossing point in the Detroit/Windsor area (where more than $100 billion of trade occurs annually between the two countries). If built outside of the immediate urban areas, it would not only provide backup in case a major bridge were destroyed, but reduce traffic congestion under normal conditions.

Mr. SIMMONS. I thank you both for your comments.

My recollection—and I couldn't find it right away in the book—is somewhere in the 9/11 Commission report it made some interesting statements about who is to blame and what went wrong. And the Commission stated that our aim has not been to assign individual blame, which is a position that I also agree with. If anyone is to blame, we are all to blame. We are all to blame because after the Cold War ended, we felt that there were no threats, no real threats, that were presented against us, and certainly in those days not the threat of terrorism, which was a nonsovereign nation, nongovernmental-sponsored activity.

But somewhere else it says that some of our failures were a failure of imagination; a failure of imagination. I have used the image of the Great Wall of China to try to illustrate what I consider to be the fundamental problem. We have such extensive borders. We are engaged economically, socially, politically with the rest of the world on an hourly basis, much less a daily basis. We have a set of standards and values with regard to rights and liberties that make us the most open and free country in the history of the world, and yet that very freedom allows those who hate us to attack us. I mean, this is a huge problem.

And I guess you can take pieces of it, like language training, pieces of it like who is on a certain port of entry and how are they trained and how many are there, but I think we have to apply imagination as well. And I guess that, to me, is where intelligence does come in. We don't have perfect security, we never will, but how—you work for the Congressional Budget Office, I believe—

Mr. O'HANLON. I do.

Mr. SIMMONS. How do we apply those resources intelligently? If we have 200 on the border, is 1,000 going to solve the problem; or should we have 800 at the border and the money for 200 go to mandatory language training? How can we apply our imagination to this problem for which we don't have unlimited resources, Mr. Cutler?

Mr. CUTLER. Well, one of the things that we seem to have developed a fixation is high technology, and sometimes that can be very good. But there was a story not long ago about—I think it was

220—or $230 million that was spent on cameras on the border. Cameras don't make arrests. Half the cameras, as it turned out, didn't work.

You know, I am a New Yorker. The ashes of 9/11 actually landed on my house. And I have been working as a volunteer with 9/11 Families for a Secure America who lost their family members. I can't tell you how many yellow ribbons are tied to my neighbors' trees. It is a constant reminder to me about our failings.

And I have arrested terrorists in my career. And sometimes you get to play a hunch, and when I was a new agent, I had a guy come in at the airport, and he had an altered visa. And he kept calling Israel Palestine. He had an Israeli passport. We dug a little deeper. Long story short, he had a diagram in his possession, and the diagram was of their oil refinery. He was here to get the money to blow it up. We eventually prevented it from happening, and that was in my first year as a special agent. I had 30 years in with the INS. But what it taught me is playing hunches and freeing people up to sometimes follow that wild idea, but not with technology as much as with human resources.

Mr. SIMMONS. If I could interrupt for just that point. When Commissioner Kelly and Mayor Bloomberg say we need the Federal Government to give us dollars for human beings, there is a lot of value in that.

Mr. CUTLER. There is absolutely a lot of value. And I like that comparison because I want you to think about something. It is estimated that right now there is about 15—, 20 million illegal aliens in the United States, depending on whose statistics you want to read. New York has 8 million residents. We are the safest big city in the United States because we have 37,000 cops. We have less than 10 percent the number of Special Agents to enforce the immigration laws with double the number of people as there are residents in the city of New York, and they are scattered across a third of the North American continent. That is not a workable situation.

When I hear about these so-called successes that ICE broke up a ring that brought in 50 or 60 or 80 people, and we are dealing with millions of illegal aliens, I am sorry, it leaves me not feeling very confident. We need to make the effort to do a far better job and dedicate the resources. We can't do it on the cheap, but look at what 9/11 cost us, besides the precious human lives which no money can replace.

Mr. SIMMONS. Mr. O'Hanlon.

Mr. O'HANLON. Congressman, just a very brief point. I am glad you pushed me on the issue of priorities. We do need to establish priorities, and there are proposals in Homeland Security that I think are excessive, but not usually on the prevention end of things. Most of what I think you are considering in this committee today and in general are border protection problems, intelligence. These are on the front end, the preventive end, and that is where we should be emphasizing in general.

So I know I gave a bit of a broad-brush comment that most of the things we touched on today require more resources, and in one sense that can never be a good enough answer. But I would prioritize preventive areas of activity over consequence management. We need some capacity for consequence management, but

some of the ideas I have heard in the homeland security debate in the last 5 years to equip most first responders in the country with state-of-the-art chem gear or interoperable radios, or have them drill several times per month in terms of response to incidents that have already occurred that we didn't stop, some of these are excessive, and that is where you can spend too much. More of the money should be spent on preventative efforts, on intelligence and on border protection.

Mr. SIMMONS. I really am glad to hear you say that.

And for you, Mr. Cutler, my daughter's apartment was so close to Ground Zero that she never reoccupied it after 9/11. She now lives in Brooklyn and works in Manhattan. So, like you, this is a daily—

Mr. CUTLER. I hope she is going okay today.

Mr. SIMMONS. She is physically—

Mr. CUTLER. I don't think any New Yorker has been the same after that.

Mr. SIMMONS. No. Well, two of her four roommates went down with the building.

Mr. CUTLER. I am so sorry.

Mr. SIMMONS. The gentlelady from California.

Ms. LOFGREN. Thank you, Mr. Chairman.

All of us, even those of us in California, were touched in some way by 9/11. The valedictorian of my high school class, Naomi Solomon, was on the Windows on the World that morning, and we lost her. So this is something that touched the whole country, and something that we are committed to preventing again.

I don't have a lot of questions because both witnesses have been very clear. I would note just for the record, a little parochialism here, that although San Jose may not seem like a big city to New York, it is the 10th largest city in the United States and has the lowest crime rate of any major city in the United States, just for the record.

Mr. O'Hanlon, thank you for the book that you coauthored. The Chairman has suggested that I get your autograph on it, which maybe we will do after the hearing. But I did want to talk a little bit about your comments on page 103 about IDENT, the database used by the Border Patrol, and that it is not fully integrated on a national scale with other databases. And this is something that bothered me from the very beginning, and I asked about this both in the Homeland Security Committee, the Science Committee and the Judiciary Committee on why we were not going to have interoperability, and even asked NIST how long and how much would it take to integrate this. And for reasons I cannot understand, we never took care of that.

And as you point out, the FBI now has an integrated automated fingerprint identification system using all 10 prints, and the Border Patrol now have interoperable systems capable of accessing IDENT and the IAFIS records, but they are not interoperable, and they don't have access to the consolidated name base terrorism watch list.

What do you think needs to be done here? I mean, it is heartbreaking actually that we didn't plan at the beginning, and now we

have this proliferation? What should we do? How much is it going to cost?

Mr. O'HANLON. Thank you for the question.

I am glad you are pursuing it, because, speaking honestly, from the point of view of an analyst, it is hard to keep track of this for two reasons: One, some of this is classified. Secondly, when you are doing a book, there is a lag time between when you write and when it is published. This has to be followed up in real time continually, and they are making progress, as I understand things, at integrating these two different systems.

So I think the broad story of integrating the terrorism watch list in the last 5 years, thanks in large part to the scrutiny of committees like this, is that we have a progress.

Ms. LOFGREN. The sad thing is they could have been the same system at virtually no additional cost to the country.

Mr. O'HANLON. But the reassuring news, despite that, is that we are essentially sharing names in one way or another at this point, even though there are these inefficiencies, and it took us too long, and thank God we weren't attacked in the meantime.

Ms. LOFGREN. But the names yield false positives all the time. It is the biometrics that really give you—I mean, you can do one false identification, but only one; I mean, once you have got their biometrics.

Mr. O'HANLON. Well, you summarized it as least as well as I could.

I will just make one additional point, if I could, which is on the visa waiver program and visa issues, we typically give our European friends a hard time, as we should, for being too slow in some of their upgrades, but they have, I think, one thing right that we need to reconsider, which is they realize fingerprints are the way to go, or something better, with IRIS for example. We are still relying too much in visas on photographs; not a good way to do biometric-reliable identification.

Ms. LOFGREN. Well, I would just note that the other concern that I have—and then I actually am supposed to chair a meeting over in the Capitol 20 minutes ago—but the US-VISIT is not interoperable in terms of the algorithms and the biometrics with the other systems. So we are building up data that ultimately I think we are going to have to go back in and redo. And did you have an opportunity to examine that, along with the IDENT, the other issue here that you mention in this chapter?

Mr. O'HANLON. My broad sense is that, to the extent we can understand this problem, we have had a lot of inefficiencies and delays, but ultimately we are working towards systems that, however inefficient, however much different from one another where they don't need to be, at least now you do have the ultimate information, which is the names of the individuals, being shared in much better real-time ways. It has taken too long, it has been too slow, and thank God we haven't been attacked—

Ms. LOFGREN. Well, I appreciate it. My time is just about up.

I would like to ask unanimous consent to put in the record an editorial from the San Jose Mercury News in yesterday's paper about immigration hearings, if I could, Mr. Chairman—

Mr. SIMMONS. Without objection.

Ms. LOFGREN.—as well as thank the witnesses and give my opinion that in the end it is going to cost us billions to go back and redo these biometrics. And we could have done it for a couple of million if we had done it at the beginning.

And I yield back and thank the gentlemen.

Mr. O'HANLON. I think you are right on cost, by the way.

Mr. SIMMONS. And I would ask unanimous consent that the chapter you referred to in the book be copied and entered into the record, if that doesn't violate your copyright rules.

Mr. CUTLER. Could I make one fast point?

Mr. SIMMONS. Please.

Mr. Cutler. In 1997, I testified at my first congressional hearing, and the advice I gave them was the need to use biometrics. And after everything that I heard and saw afterwards, the fact that here we are almost 5 years after 9/11 and we are still banging our head against the wall. You know, World War II ended in less than 4 years. And what frustrates me is we are not hitting the ground running, we haven't been, and we need to be, and that is something that concerns me tremendously.

Mr. SIMMONS. I appreciate the comment. And I think that those of us who have been involved with the terror issue for any period of time—and for me it goes back pretty much to my service to the Central Intelligence Agency back in the mid 1970s, certainly in 1979 when colleagues were seized in the embassy in Iran, and when my roommate was killed in the Beirut Embassy in 1983—we have always felt—or I have always felt that we need a consolidated database on terrorists just as we needed it for counterespionage, and if we had moved aggressively in the early 1980s to create those databases, we wouldn't have the problem that we have today. But unfortunately, there are several libertarian issues that arose at the time, and people felt that the focus on the Cold War was more important than a focus on this kind of unconventional war.

Sadly, we have learned the hard way that you cannot ignore multiple threats, that the world is dangerous in multiple ways; that our democracy is threatened and our values are threatened, our people and resources are threatened in multiple ways. We can't pay for it all, so we have to be smart. And in the past mistakes have been made.

Mr. CUTLER. I just wanted to respond quickly. I know we are running long on time.

The administration has been doing these operations to target airports and nuclear power plants, and I think we need to. I mean, that should be a given if it is a secure facility. But the idea of hiding in plain sight—you know, there was a terrorist suspect who was arrested in Lodi, California, who was driving an ice cream truck. That ice cream truck kept me awake for a couple of weeks.

I spent half my career doing drug and terrorism investigations, and much of what I did also involved surveillance. When a bad guy gets into a car and drives for a half hour to a parking lot and meets somebody else, you know he has had a meeting. How many people approach an ice cream truck on a hot afternoon? How hard would it be to slip a memory card from a little PDA device into a $5 bill, pay for ice cream and get another one in return? And those things can hold over a gigabyte of data. There have been terrorist suspects

driving taxi cabs. The guy that was involved with terrorism in Canada that drove a school bus, which gave him easy access to easily persuadable children, young men.

So the problem is that if we focus on secure facilities, two things have happened, in my judgment: Number one, we are leaving out the broader potential that the bad guys are hiding in plain sight. Somebody once said that a spy is somebody that wouldn't attract the attention of a waitress in a greasy spoon diner. The point of fact is it might well be that the waitress or the waiter is the spy or the terrorist.

But the other thing is we have also given the other side a playbook. Don't get a job in a nuclear power plant if you want to stay under the radar, get a job selling hot dogs right outside the gates of the nuclear power plant, and nobody will pay attention to you.

The reality is that we need to have an immigration system that has integrity. For far too long this has been a fragmented effort. And one of the things I have testified at a few prior hearings was about the structure of ICE versus CBP. And literally it has been versus, where there have been barriers erected, noncooperation and so forth. We need a seamless operation. And this needs to be seen as a continuum, not simply if you get past the Border Patrol, you are home free. It is kind of like trying to play baseball and telling your outfielders not to bother showing up in the outfield, hit the ball over the second baseman's head, and you have got an in-the-park home run. And that is the way immigration has been enforced and administered for far too long.

And I would also ask, I don't know if procedurally this can be done, but the GAO did a report that was issued on March 10th of this year that addressed the issue of immigration benefit fraud. And if we do everything possible on the border and made the border completely impermeable, if we don't get to the issue about how we give out residency and citizenship and do those other things that constitute the benefits program, it would be the same thing as a homeowner securing his house and putting strong doors and locks on his windows and doors, and then handing out the keys to anybody who walks by. So all the efforts on the border will mean nothing if the immigration system itself lacks integrity, in my judgment.

Mr. SIMMONS. I agree with you completely. Just again referring back historically to the Soviet Union, Colonel Abel, who was one of the KGB's most successful spies, came through Canada, established himself as a photographer in Brooklyn, I believe, for 7 years, and only after 7 years was activated, and by that time he had established his bona fides. He was a member of the community, et cetera, et cetera.

You know, sleepers commit espionage, sleepers commit terrorist acts, and we need to be imaginative in how we go about targeting these problems, because if we are not imaginative, we will simply build that Great Wall of China, take a look at it, say, well, you know, we have emptied the Treasury, so therefore we have done everything we can do because the Treasury is empty, we haven't spared a dollar, the taxpayers have been decimated, and we have got this big wall, but it doesn't work. Maginot Line bankrupted the French. Didn't work. So the challenge is to apply economics and

imagination, as you have described, to the problem. And I thank you both for your testimony. It has been very insightful.

And I would say that members of the committee who have additional questions for the witnesses, we will ask them to respond to these in writing. The hearing record will be held open for 10 days.

Mr. SIMMONS. There being no further business, and without objection, I thank the members of the third panel for their excellent testimony, and the committee stands adjourned.

[Whereupon, at 12:26 p.m., the subcommittee was adjourned.

QUESTIONS FOR THE RECORD

[The information follows]:

Questions for the Record
House Homeland Security
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
"DHS Intelligence and Border Security: Delivering Operational Intelligence"
June 28, 2006
Assistant Secretary Charles Allen, Assistant Commandant for Intelligence James F. Sloan,
CBP Intelligence Executive Director L. Thomas Bortmes, &
ICE Acting Director of Intelligence Cynthia O'Connell

Questions from Representative Rob Simmons for Assistant Secretary Charles Allen

1. The following are some of the different DHS led operational intelligence units/centers established to better secure the border: the National Targeting Center (NTC), the Border Patrol Field Intelligence Center (BORFIC) in El Paso, the Command and Control Intelligence Coordination Center (CCICC) in San Diego, Field Intelligence Units (FIUs), Maritime Intelligence Fusion Centers (MIFCs), Air and Marine Operations Center (AMOC), Field Intelligence Support Teams (FISTs), and Maritime Intelligence Support Teams (MISTs).

a. How is the intelligence being generated from these different DHS entities being integrated to formulate a strategic policy for the protection and security of our borders?

Response: The Chief Intelligence Officer has established a new Border Security Analysis Team within the Office of Intelligence and Analysis (I&A) to focus on strategic analysis of intelligence and intelligence-related information received from various information sources, including all DHS intelligence units and centers. To further support the formulation of DHS policy and plans, I&A is developing a comprehensive intelligence campaign plan for the southwest border. It also has embedded a liaison officer in the Secure Border Initiative Program Executive Office to coordinate intelligence policy and planning.

b. How are the intelligence requirements being generated from these different DHS entities being represented in the Intelligence Community (IC)?

Response: The Office of Intelligence and Analysis (I&A) works with DHS components to identify their information needs. It then reviews and validates the information requirements as intelligence requirements. I&A collection managers disseminate the all-source and intelligence specific requirements to DHS' Intelligence Community partners for review and collection tasking. The Intelligence Community tasks collection agencies to satisfy these requirements and to provide DHS with an appropriate response. I&A collection managers also represent DHS' intelligence requirement equities as full participants in Intelligence Community collection management committees.

c. What do you see as the biggest hurdle to overcome in creating an integrated collaborative information sharing environment for border security?

Response: The biggest hurdle will be the implementation of our enterprise information management architecture, which will be the mechanism for flowing information to operational law enforcement elements and the border and receiving in turn the prioritized needs of DHS entities at the border.

2. How many different types of information sharing systems has your office identified that are being used by the different DHS intelligence assets at the border?

Response: To ensure that we use interoperable, integrated and scalable information systems throughout DHS, we have undertaken a study to identify and document all existing databases. This study is still ongoing. To combine our existing separate architectures, as a cost effective way to provide Department-wide connectivity, those databases certified as having valuable, relevant information are being integrated into the DHS Intelligence Enterprise Architecture and made available to all of DHS as well as to the State and Local Fusion Center user base. Where gaps are identified, existing systems may be scaled or new ones created to meet our mission needs. It is important to note that the focus of information sharing is both on the border and throughout the entire DHS Intelligence Enterprise.

a. With multiple types of information sharing systems, what types of gaps have been created in the ability of DHS analysts to produce timely actionable operational intelligence?

Response: We recognize that systems of legacy components are not yet fully integrated. These connectivity gaps mean that DHS intelligence analysts must perform multiple searches of applicable systems, using the same search criteria. This lack of integration impedes the ability of DHS analysts to produce timely and actionable operational intelligence products. A comprehensive, process-based information management structure is needed to govern the way we use our most important information systems. The DHS Intelligence Enterprise Architecture will help resolve this limitation.

DHS analysts have developed solutions to receive key data to which they do not have immediate connectivity or access. DHS analysts also have been building solid intelligence networks with colleagues throughout the intelligence, law enforcement, and other communities, which enhance their legitimate access to raw information and intelligence.

b. What is your office doing to consolidate the intelligence collected at the border to allow analysts to produce efficient, timely, and accurate operational intelligence for the different field components?

Response: My Office is helping to consolidate border intelligence by disseminating Homeland Intelligence Reports (HIRs) to DHS analysts and the Intelligence Community. DHS components gather significant amounts of intelligence and intelligence-related information at the border. The Office has partnered with its intelligence components to report this intelligence in a standardized format, the Homeland Intelligence Reports (HIR). It is consolidating the intelligence collected at the border by posting these HIRs in an easily accessible portal on secure systems. In addition, through my Office's training course for reports officers, I&A is currently training CBP and ICE personnel to identify what intelligence-related information needs should be reported in the

Department's HIRs.

3. In your opinion, what is the number one threat to our border?

Response: The threat to the border must be viewed holistically. I view terrorism as the most dangerous threat facing our country but, in my view, terrorism is inseparable from other cross-border criminal activity and the violence that inevitably accompanies such activity. Our adversaries have the potential to exploit criminal activities in border areas to facilitate or support terrorism. These activities entail multiple threats that include, but are not limited to, human, drug, weapons, and contraband smuggling and trafficking; transnational gangs; document fraud; and illegal immigration.

4. Do you have the necessary analytical staff and resources to perform your mission?

Response: To meet the many priorities, the Office has undertaken major analytic efforts in the areas of border security and radicalization; providing analytic support to an expanded set of homeland security concerns; and continuing to provide high quality assessments on terrorism issues. Addressing these priorities has stretched my limited analytic corps very thin. My requirements for additional resources and broader skills in my analytic corps are immediate and I am working with the Department as well as with the Director of National Intelligence to fill those needs – both in the near term and over the FYHSP.

5. Currently, at the Joint Interagency Task Force South (JIATF-South), local, state and federal agencies utilize a Secret-level, real-time information system, that has been operational for almost twenty years, called ADNET (Anti-drug network). Has DHS looked at this system for sharing operational intelligence across the Department's Intelligence Components?

Response: DHS has reviewed ADNET and found that it is a viable, complementary network that can be used by DHS components with intelligence functions. It is our intention to create a gateway to this network and leverage its national connections and user base to further the completion of our mission objectives. Because the network was established and funded for a counter narcotics mission, the user base, associated databases, and tool sets have very focused purposes. DHS analysts, who are appropriately cleared to handle classified information, will be able to access the data on ADNET through the gateway and use it to fuse classified and unclassified information.

6. The Human Smuggling and Trafficking Center (HSTC) was created to address human smuggling, human trafficking, and clandestine terrorist travel. It serves as an intelligence fusion center and information clearinghouse that is designed to support interagency efforts to address these serious issues, and to foster greater cooperation and communication between relevant agencies.

a. What is the status of the Department's support to the HSTC?

Response: The Director of the HSTC is an ICE Office of Investigations (OI) Supervisory Special Agent. ICE OI also has two full time Special Agents, one part time Special Agent, and one part time Analyst assigned to the HSTC. The Office of Intelligence and Analysis (I & A) has two part time Reports Officers assigned to the HSTC.

b. What type of DHS analytical support is being provided to the Center?

Response: All DHS personnel assigned to the HSTC have access to the investigative and intelligence tools necessary to provide analytical support to the HSTC.

c. What type of DHS interdisciplinary expertise is being provided in support of the Center?

Response: ICE personnel assigned to the HSTC come from the Human Smuggling and Trafficking Unit, the National Security Investigations Division, the Financial and Trade Investigations Division , and the Office of International Affairs. The I & A Reports Officers have expertise in creating and disseminating intelligence products. Each employee has immigration and customs enforcement skills and expertise, and has specialized in human smuggling and trafficking cases.

d. How is the intelligence being produced by the HSTC helping the component agencies with their day to day operations?

Response: The HSTC does not directly conduct intelligence collection or other operations, but it does produce reports based on information gathered by relevant agencies. A recent classified assessment of South Africa produced by the HSTC and the National Counterterrorism Center resulted in the development and implementation of a DHS operation to target vulnerabilities identified in the assessment. Analyses produced by the HSTC is incorporated into target folders for select ICE OI initiatives. Analyses produced by the HSTC is utilized by DHS for country assessments relative to the Visa Waiver Program.

Questions from Representative Rob Simmons for
Assistant Commandant for Intelligence James F. Sloan

1. In your opinion, what is the number one intelligence issue the Coast Guard faces? Is it information sharing within the department and other federal agencies? Lack of personnel?

Response: The Coast Guard and its Intelligence Community and Law Enforcement partners who focus on the maritime realm face many significant challenges:
To highlight just a few:

- The "intelligence battlespace" is essentially the entire maritime realm, which is truly vast and complex;
- The transnational terrorists and other threat actors who are our priority targets are many, diverse, and ever adaptive to evolving circumstances;
- Every intelligence organization is only as good as the talent, experience and dedication of its people, and the competition today to recruit and retain critical human resources is intense;
- There are overwhelming quantities of information to collect, fuse, correlate, and analyze in carrying out our basic intelligence functions; and
- While information sharing between and among federal and non-federal agencies continues to improve, there remains much work to be done.

2. The Coast Guard has the responsibility of protecting more than 361 ports and 95,000 miles of coastline - In your opinion, what is the greatest threat to our maritime borders?

Response: It is difficult to identify any one threat as the greatest threat to our maritime borders, primarily because there are many different threat actors and potential threat scenarios that are of concern. One constant threat that we focus very closely on every day is the maritime infiltration of Special Interest Aliens (SIAs) into the U.S. ports, via vessel crews or existing smuggling networks of aliens, drugs, small pleasure craft, and/or cargo.

There is currently no specific, credible information on terrorist targeting of U.S. ports, maritime infrastructure, or assets; however several suspicious incidents continue to indicate possible pre-operational surveillance in multiple locations.

To date, increased security levels, including a more robust maritime presence and newly developed security regimes, intelligence and law enforcement programs, have provided significantly more information on individuals and cargo entering into U.S. ports. This increased information is proving very useful in improving the effectiveness of the screening function carried out by the Coast Guard and its maritime security partners.

3. Do you have the necessary analytical staff and resources to perform your mission?

Response: Yes. The President's overall FY07 budget request will provide sufficient funds for the current operation of the Coast Guard Intelligence program. As we look to the future, our Headquarters staff continues to investigate potential future capabilities and additional enhancements that might improve intelligence support to Coast Guard missions and other national security priorities. Any future requests for budget increases above present levels would be vetted as appropriate through the Department of Homeland Security and others in the Intelligence Community—and any such requests would almost certainly track closely with our four current program priorities:

- Enhancing HUMINT;
- Promoting greater depth and breadth of analysis;
- Exploiting technology; and
- Developing the right organization and architecture.

In addition, significant intelligence analytical functions within the Coast Guard are funded via the General Defense Intelligence Program (GDIP) supplemental funding stream. It is important that these functions be funded via recurring funding to maintain the program's current and future analytical capabilities.

4. Can you discuss a recent example of Coast Guard intelligence directly supporting an arrest or interdiction of illegal material?

Response: Examples of Coast Guard intelligence directly supporting assets and/or interdictions of illegal material involve "For Official Use Only" and/or classified information. Intelligence Program staff are available to brief these examples in an appropriate venue upon request.

5. Currently, at the Joint Interagency Task Force South (JIATF-South), local, state and federal agencies utilize a Secret-level, real-time information system, that has been operational for almost twenty years, called ADNET (Anti-drug network). In your opinion, would this system work for sharing operational intelligence across the Department's Intelligence Components?

Response: The Coast Guard has been extensively and intimately involved with the ADNET program since its inception in the early 1990s. At one time, the ADNET technical architecture was the foundation of the Coast Guard Intelligence Program's classified architecture. Over time, as the ADNET architecture has evolved and Defense Information System Agency (DISA) networks have modernized, the ADNET community has become one of many business lines supported by DISA's Secret Internet Protocol Router Network (SIPRNet). Since the ADNET program's business is conducted over the SIPRNet, Coast Guard forces use SIPRNet as the backbone for its classified operations (Command and Control as well as Intelligence) and many more Coast Guard unit/commands/programs have access to the ADNET community than ever before. While the ADNET "system" does in fact support real-time information sharing - not only for SECRET information but UNCLAS/FOUO/SBU data as well, as a DoD/DISA program, the use of the ADNET model and its underlying networks would have to be approved for use outside of the current approved counterdrug contact. It is our understanding that DISA severely limits non-DoD agency access to SIPRNet. While there is extensive SIPRnet access throughout the Coast Guard (as part of the Service's military needs), there is only a limited amount of SIPRNet access within other DHS components and most of those are from access mostly related to prior ADNET work, such as was in existence in legacy Customs or INS. However, DISA has the ability to enable network-to-network access so that existing classified agency networks can interface with SIPRNet, thus affording real-time information sharing across SIPRNet/ADNET

and existing agency networks. It is our understanding that such an effort was envisioned between SIPRNet and the Homeland Security Data Network (HSDN - a SECRET high DHS network effort).

6. What are some examples of Intelligence, Surveillance, and Reconnaissance (ISR) assets owned by the Coast Guard and how do they contribute to operational/tactical intelligence being produced to better secure our borders?

Response: The answer to your question involves "For Official Use Only" and classified information. The Coast Guard staff is available to provide a briefing on this question in an appropriate venue upon request.

7. Are there issues of sharing operational intelligence between the DHS component agencies and other federal entities? What are some of those issues and in your opinion what are some potential solutions?

Response: Information sharing is improving throughout the federal, state, tribal, territorial, local, and private sector environment in which the Department of Homeland Security (DHS) and its components, including the Coast Guard, operate.

To assist in this development, DHS has established an Information Sharing and Collaboration (ISC) Program and the Coast Guard is an active member. As a member of the ISC Program, we are part of the overall initiative that seeks to improve information sharing and collaboration:

- With our state, tribal, and territorial, local, and private sector partners responsible for securing the people and infrastructure of this country.
- Between DHS elements.

The Coast Guard has taken a leadership role within DHS to ensure that intelligence products are shared rapidly and accurately throughout the federal government. Threat information and reports of suspicious activities from the maritime industry and other maritime stakeholders are shared with appropriate Intelligence Community members, appropriate offices within DHS, and the National Response Center (NRC).

The Coast Guard will continue to work in collaboration with the other components within the Department of Homeland Security. This is accomplished through the various secure and non-secure intelligence and law enforcement computer systems, watch and fusion centers, and exchange of liaison officers.

8. Can you please describe the breakdown of the roles and responsibilities between the Intelligence Coordination Center, the Maritime Intelligence Fusion Centers, District

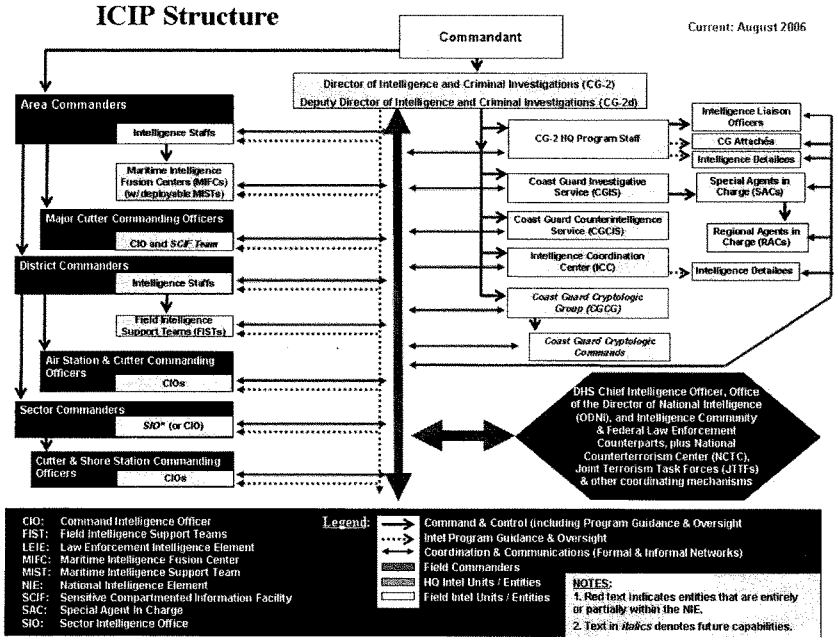
Headquarters, Field Intelligence Support Teams, and Sector commands as it relates to strategic, operational, and tactical intelligence?

Response: The diagram below outlines the basic structure of the integrated Coast Guard Intelligence and Criminal Investigations Program (ICIP).
Explanation of the diagram is as follows:

- The green blocks depict the headquarters-level intelligence entities, including the Intelligence Coordination Center (our lead Production Center that provides intelligence support to the Commandant and National-Level Decision Makers and coordinates on behalf of the Coast Guard throughout the Intelligence Community).
- The blue and yellow blocks show how intelligence is embedded in the field organization and hierarchy. At the theater / operational level, each area commander has an intelligence staff. Additionally, there are the two Maritime Intelligence Fusion Centers that provide tactical intelligence support to operational commanders and the districts, while also supporting the area commanders' intelligence needs.
- Below the area level, each district has an intelligence staff. The Field Intelligence Support Teams are intelligence collectors and provide first order analysis at the port and field level.
- The purple hexagon represents the external agencies with which the Coast Guard interacts regularly.

The Coast Guard brings unique maritime access and expertise to the Intelligence Community given our extensive experience and involvement in coastal operations, port security, maritime transportation, merchant mariner activities, maritime law enforcement and maritime intelligence. Others within the Intelligence and Law Enforcement Communities depend on the CG for valuable expertise, access and perspective on these issues. The CG has specific statutory authorities within the maritime domain that provide the basis for specific roles and functions that enable the CG to make unique contributions to the broader Intelligence Community.

Questions for the Record
House Homeland Security
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
"DHS Intelligence and Border Security: Delivering Operational Intelligence"
June 28, 2006
Assistant Secretary Charles Allen, Assistant Commandant for Intelligence James F. Sloan,
CBP Intelligence Executive Director L. Thomas Bortmes, &
ICE Acting Director of Intelligence Cynthia O'Connell



9. In the November 2005 DHS OIG-06-04 report, an issue of multiple systems being used by CBP and ICE to disseminate and receive intelligence has created an environment not conducive for effective analysis of the intelligence being shared. What are the primary systems the Coast Guard uses to disseminate and receive intelligence specific to the support of Coast Guard's operational and tactical missions?

Response: The Coast Guard utilizes both "push" and "pull" environments to receive and disseminate intelligence in support of operations. Collected information and finished intelligence are pushed to internal Coast Guard users and external partners at the federal, state, local and international levels, and the maritime industry, as appropriate, using formatted messages and tailored finished reports.

Messaging systems such as the Department of Defense's (DOD's) Automated Message Handling System (AMHS) and the Coast Guard's Messaging System (CGMS) provide the backbone for information dissemination. The Coast Guard also relies on WebTas, specially designed

government off-the-shelf technology, to assist in managing data in its Common Intelligence Picture (CIP).

From the Coast Guard CIP, operational and tactical intelligence can be pulled by users who have access to the Secret Internet Protocol Router Network (SIPRNET). Coast Guard intelligence homepages have been developed at each security classification level whereby Coast Guard intelligence products are posted and can subsequently be pulled by personnel with the proper clearance. Email, clear and secure voice communications, and video teleconferences provide further avenues for collaboration and dissemination in both routine and time-sensitive situations.

In the future, the Coast Guard's Deepwater acquisition program will deliver an integrated Intelligence Knowledge Center (IKC) that will consolidate available raw data and finished intelligence for effective analysis by Coast Guard analysts and subsequent sharing with the Coast Guard Intelligence Program's internal and external customers.

10. What are the primary operational intelligence requirements that drive the operational analytical production of the Coast Guard?

Response: The answer to your question is "For Official Use Only, Law Enforcement Sensitive." The Coast Guard staff is available to provide a briefing on the issue in an appropriate venue upon request.

11. How does the Maritime Intelligence Fusion Centers (MIFCs), Field Intelligence Support Teams (FISTs), and the Cryptologic Group effectively share operational intelligence for the sector to the other DHS component agencies located within the sector?

Response: The Maritime Intelligence Fusion Centers (MIFCs) are responsible for collecting and fusing intelligence information from multiple sources and providing actionable (i.e., timely, accurate and relevant) intelligence to Coast Guard operational and tactical commanders in support of all mission areas within their respective geographic areas of operations.

The MIFCs complement the Coast Guard's Intelligence Coordination Center's strategic focus and support District Intelligence offices, Field Intelligence Support Teams (FISTs) and Command Intelligence Officer (CIO) efforts, with the ultimate goal of supporting the National Strategy for Homeland Security.

The Coast Guard has had great success with Field Intelligence Support Team (FIST) personnel actively engaged with other federal, state and local agencies through participation with local level entities such as the Joint Terrorism Task Force, Antiterrorism Advisory Committees, Law Enforcement Coordinating Committees and Regional Domestic Security Task Forces.

FIST reporting has resulted in several significant ongoing local law enforcement and FBI investigations into suspicious activities. In other cases, FIST reporting and improved Other Government Agency (OGA) cooperation have cleared some threats as definite hoaxes that would otherwise have wasted investigative resources.

12. What kind of collaboration does the Coast Guard intelligence assets have with federal fusion centers like the Organized Crime Drug Enforcement Task Force (OCDETF) and the High Intensity Drug Trafficking Area (HIDTA)?

Response: The Coast Guard Intelligence Program works closely with federal fusion centers such as the Organized Crime Drug Enforcement Task Force (OCDETF) and the High Intensity Drug Trafficking Area (HIDTA).

Organized Crime Drug Enforcement Task Force (OCDETF): OCDETF provides a framework for federal, state, and local law enforcement agencies to work together to target well-established and complex organizations that direct, finance, or engage in illegal narcotics trafficking and related crimes. The Coast Guard Investigative Service (CGIS) is part of this framework.

- OCDETF Washington, DC
  The OCDETF Operations Chief Group - CGIS Deputy Director represents the Coast Guard. This group meets as necessary to coordinate OCDETF criminal investigations and task force operations, provide policy implementation input, and develop international drug and money laundering targets for inclusion in the OCDETF Consolidated Priority Organization Targets (CPOT) list.

- The OCDETF Washington Area Representatives Group - CGIS Assistant Director represents the Coast Guard. This group meets as necessary to discuss and formulate OCDETF policy and procedures, share investigative information, disseminate performance measures, and approve/disapprove OCDETF Consolidated Priority Organization Targets (CPOT) recommendations for criminal investigation and prosecution.

- OCDETFs San Juan, PR; Miami, FL; Baltimore, MD; New York, NY; Boston, MA; Seattle, WA; Honolulu, HI; San Francisco, CA; San Diego, CA; Atlanta, GA; Houston, TX; St. Louis, MO; Corpus Christi, TX.
  CGIS part-time representation. CGIS co-sponsors joint investigations and CGIS representatives participate in joint counterdrug-smuggling operations, facilitate smuggling information sharing, conduct operational intelligence collection, develop Regional Priority Organization Targets (RPOT) lists, and attend OCDETF Regional coordination meetings.

OCDETF investigation - *Operation Panama Express* (PANEX) is a multi-agency investigation

that began in the mid 1990s.

- Today there are personnel dedicated to PANEX from DEA, ICE, JIATF, FBI, IRS, U.S. Coast Guard, the U.S. Attorney's Office for the Middle District of Florida, the Florida Department of Law Enforcement, and the Sarasota, Hillsborough, and Pinellas County Sheriffs' Offices.

- Additional information on PANEX is For Official Use Only, Law Enforcement Sensitive. Coast Guard staff is available to provide a briefing on the issue in an appropriate venue upon request.

High Intensity Drug Trafficking Areas (HIDTA) Task Forces: The charter of HIDTA is to enhance and coordinate drug control efforts among local, state, and federal law enforcement agencies. The program provides agencies with coordination, equipment, technology, and additional resources to combat drug trafficking and its harmful consequences in critical regions of the United States.

- HIDTAs San Juan, PR; Jacksonville, FL; Miami, FL; San Diego, CA; and Brownsville, TX
  Coast Guard Investigative Service (CGIS) part-time representation. CGIS participates in joint counter-smuggling operations, information sharing, and operational intelligence collection.

13. How has the establishment of Maritime Liaison Agents at the Joint Terrorism Task Forces Offices helped the Coast Guard produce more effective operational intelligence?

Response: The Federal Bureau of Investigations (FBI) Joint Terrorism Task Force (JTTF) Maritime Liaison Agent (MLA) Program formally began in July 2004 and was developed to establish and maintain relationships with representatives of "maritime institutions" in their respective geographical areas. The Coast Guard Investigative Service (CGIS) was identified by the FBI as the agency best suited to train special agents designated in each JTTF as the MLA.

Training of MLAs by the CGIS is directed at ensuring that Coast Guard operational commanders, Field Intelligence Support Teams (FISTs), Maritime Intelligence Support Teams (MISTs), and senior Coast Guard decision makers receive rapid and actionable intelligence and information from MLAs relative to security to strategic ports of embarkation and debarkation, counter-terrorism and counterintelligence, port safety and security, and maritime law enforcement matters.

The MLA Program fosters a relationship between the Coast Guard and the FBI that appreciably increases the operational law enforcement effectiveness of both agencies. This relationship promotes cooperative law enforcement, drawing on the resources, capabilities, and expertise of each agency. The types of support provided by the FBI/JTTFs in response to specific Coast Guard requests have included bomb technicians, Weapons of Mass Destruction (WMD) experts,

Hazardous Material (HAZMAT) trained agents, and additional manpower, while Coast Guard support to specific FBI/JTTF requests has included the conduct of maritime law enforcement operations, training, and allocation of vessels and aircraft in support of FBI operations.

Between October 2004 and March 2006, approximately 650 investigative leads were followed up by Coast Guard special agent personnel in matters ranging from counter-terrorism, vessel absconders, and stowaways to criminal investigation of merchant mariners, security breaches of port facilities, and threat assessments of military load-out facilities, all as a direct result of intelligence and information sharing between the Coast Guard and JTTF MLAs.

14. Can you please explain what the Maritime Domain Awareness (MDA) initiative is and how it applies to the Coast Guard with a focus on operational/tactical intelligence?

Response: Effective Maritime Domain Awareness (MDA) enables the Coast Guard and other Maritime agencies to develop a layered defense for the identification of threats as early and as distant from our borders as possible, and to provide maximum time to determine the optimal actions that should take place. The Coast Guard Intelligence and Criminal Investigations Program continues to enhance the collection, integration, analysis and dissemination of maritime intelligence information in support of MDA. MDA requires collaboration within and outside the Coast Guard, including federal, state and local partners, to insure interoperability and unity of effort.

Achieving MDA does not involve simply one capability, but rather many diverse Maritime C4ISR capabilities working in a coordinated and integrated manner:

- It requires maintaining and accessing data on vessels, people, facilities and infrastructure.
- It requires collecting, analyzing and disseminating critical information to decision makers to facilitate effective understanding of the global maritime environment.

Operational/tactical intelligence provides critical, analytical depth to the MDA effort through various intelligence capabilities and analytical processes.

15. How has the enhancements to Maritime Domain Awareness (MDA) & related dissemination to the field affected the operational intelligence being produced by the Coast Guard?

Response: Achieving the end state of Maritime Domain Awareness (MDA) requires leveraging and building on existing capabilities within Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). Leveraging intelligence provides the CG with the ability to detect, identify and ascertain capabilities and intent of those threats that operate in (or from) the maritime domain.

The Coast Guard Intelligence and Criminal Investigations Program continues to engage the Intelligence Community and law enforcement partners to develop new sources, improve

analytical processes and provide actionable (i.e., timely, accurate and relevant) intelligence to strategic decision makers, as well as Coast Guard operational and tactical commanders.

By automating and combining what are presently multiple, manually-intensive data inquiries, Deepwater Systematic Screening of Vessels (SSV) future capability should enable more rapid, in-depth checks of vessels, cargo, and people than are presently possible. SSV will be available via classified government networks, providing direct access to Coast Guard operational and tactical commanders using a standard set of "tools" for all commands conducting screenings.

The Maritime Intelligence Fusion Centers (MIFCs) are responsible for collecting and fusing intelligence information from multiple sources and providing actionable intelligence to Coast Guard operational and tactical commanders in support of all mission areas within their respective geographic areas of operations. They complement the Coast Guard Intelligence Coordination Center's strategic focus and support District Intelligence offices, Field Intelligence Support Teams (FISTs) and Command Intelligence Officer (CIO) efforts, with the ultimate goal of supporting the National Strategy for Homeland Security.

16. Can you please describe how COASTWATCH screening supports nation-wide foreign vessel boarding and inspection process?

Response: COASTWATCH, within the Coast Guard's Intelligence Coordination Center (ICC) and part of the National Maritime Intelligence Center, is responsible for ensuring the 96-Hour Notice of Arrival information for vessels and people is vetted using appropriate intelligence and law enforcement databases. This program has detected and provided advance warning about numerous arriving individuals identified in federal law enforcement and immigration databases as criminal or security concerns, including active warrants and "deny entry" orders for past border crossing violations. In addition, several individuals wanted for questioning by federal agencies about possible extremist associations have been identified in advance of arrival and referred to the relevant agency for investigation, but none thus far have had known direct links to terrorism.

During the screening process, vessels or persons may be identified as "of interest" in regards to National Security or Law Enforcement. COASTWATCH warnings are rapidly distributed to other Department of Homeland Security (DHS) law enforcement agencies, the Department of Justice, Intelligence Community members, the Department of Defense and U.S. allies, where appropriate.

COASTWATCH's advance warning of suspect ships, people and cargo (via liaison with CBP's National Targeting Center), is used by Coast Guard sector commanders to reduce security risk by informing boarding priorities and allowing greater time to coordinate appropriate security responses with other federal, state, and local agencies. This systematic screening and early warning of potential threats directly enhances the Nation's capability to push out its maritime borders and enhance Maritime Domain Awareness.

17. Can you please describe what PANEX intelligence cueing is and how it has supported maritime illicit drug seizures?

Response: Panama Express (PANEX) cueing is derived primarily from multiple source Human Intelligence (HUMINT). That intelligence is then provided to JIATF-South J2 and J3 via structured daily reporting and real-time updates, and integrated into their Detection and Monitoring (D&M) efforts in the Eastern Pacific (EASTPAC). When Tactical Control (TACON) is shifted to the Coast Guard for law enforcement action, PANEX continues to supplement information with updates as they become available to attempt to provide Operational Commanders with the fullest possible degree of situational awareness.

The Coast Guard Intelligence and Criminal Investigations Program currently has four agents assigned as fully vested partners in Operation Panama Express (PANEX). These agents speak fluent Spanish and have a wealth of practical hands-on experience in Coast Guard maritime law enforcement operations and narcotics investigations. In addition, the Coast Guard participates in the multi-agency El Paso Intelligence Center (EPIC), which shares information that increases the effectiveness of Panama Express. By passing real-time, actionable intelligence information on smuggling operations to the Joint Inter-Agency Task Force South (JITAF-S) in Florida, transit zone interdiction operations become more effective.

The impact of PANEX is evident in the substantial seizures and other disruptions and in the fact that not only have drug trafficking organizations generally reduced the size of the cocaine loads they are smuggling by fishing vessel to an average of 3,000 kilograms, but also through PANEX, more than 500 mariners have been arrested, decreasing the supply of experienced mariners to operate the fishing vessels and go-fast boats used to smuggle cocaine.

Questions from Representative Rob Simmons for
CBP Intelligence Executive Director L. Thomas Bortmes

1. In your opinion, what is the number one intelligence issue CBP faces? Is it lack of access to national intelligence? Information sharing within the department and other federal agencies? Lack of personnel?

Response: Continuing to better integrate and structure the CBP-wide intelligence enterprise remains the most significant intelligence issue confronting U.S. Customs and Border Protection. Commissioner Basham has identified this issue as one of his three priorities and chartered a CBP intelligence enterprise working group to develop recommendations that will better: enable the receipt of timely and actionable intelligence to the CBP front-line officer or agent; provide for a CBP-wide common intelligence picture that enables total border awareness; and ensure that

information of intelligence value that is collected by CBP personnel during the course of normal business is identified, analyzed, and reported to our partners outside of CBP.

2. In your opinion, what is the number one threat to our border?

Response: The number one threat to the U.S. border is the entry of terrorists or terrorist weapons. The challenge for CBP intelligence is to respond appropriately to this priority while also addressing the variety of other threats that CBP officers and agents face on a daily basis including illegal immigration, drug and contraband smuggling and the violence associated with these criminal activities.

3. Do you have the necessary analytical staff and resources to perform your mission?

Response: CBP currently maximizes the use of its intelligence analysts and field personnel to support our primary mission of preventing terrorists and terrorist weapons from crossing U.S. borders, as well as other daily threats.

4. What is a recent example of CBP intelligence directly supporting an arrest or interdiction of illegal material?

Response: CBP Office of Intelligence analysts recently issued an intelligence report that identified an individual who was affiliated with a criminal organization that had been involved in commercial fraud and was possibly providing material support to terrorists. This assessment was made by fusing information obtained during a CBP seizure with information from reliable intelligence reporting. In July 2006, the individual applied for admission at the Detroit-Canada Tunnel Port of Entry. The identified individual's application for admission was refused based on the intelligence report and the results of this encounter were reported to interested outside agencies.

5. Within the CBP intelligence enterprise there are approximately 477 personnel. Outside of the 90 personnel assigned to the CBP Office of Intelligence, where are and what type of units/centers are the other personnel located?

Response: CBP has three "legacy" intelligence components within the Offices of Border Patrol, Intelligence, and Air and Marine. The majority of these intelligence assets is located in the Office of Border Patrol and the Office of Intelligence and comprises GS-0132 personnel and operational field personnel assigned to full-time intelligence positions. CBP is in the process of reviewing these positions to ensure proper alignment within a CBP-wide intelligence enterprise. There are just over a hundred GS-0132 intelligence specialists assigned in CBP. Within the Office of Border Patrol its intelligence personnel are Border Patrol Agents dedicated full-time to intelligence duties, along with a smaller number of GS-0132 personnel. These agents and

analysts are assigned to Border Patrol stations, sectors, the Border Patrol Field Intelligence Center in El Paso, and at CBP headquarters. CBP's Office of Intelligence (OINT) has sixty-five employees on-board as of the date of this response, approximately two-thirds are GS-0132 intelligence specialists with the remaining staff providing a variety of administrative and mission support functions. All OINT personnel are in the National Capital Region, most at CBP headquarters and others supporting the CBP National Targeting Center. OINT also manages a smaller number of GS-0132 personnel assigned overseas supporting the CBP Container Security Initiative. Finally, the CBP Office of Air & Marine has a small number of GS-0132 personnel, with most assigned to their Air and Marine Operations Center in Riverside, California and others assigned to individual branches.

6. What are some specific examples of how the CBP Office of Intelligence provides support to the day to day operations of Customs and Border Patrol agents?

Response: Two times a week the Office of Intelligence provides an all-source intelligence briefing to senior CBP leadership. This brief focuses on current threats to the border, providing leadership with the intelligence they need to make resource decisions that could impact any manager or officer in the field. The Office of Intelligence participates in bi-weekly conference calls with senior CBP field managers, providing regular threat updates. Office of Intelligence analysts prepare and disseminate intelligence alerts and assessments to CBP field offices, daily. These reports may detail new threat information, officer safety issues, or simply increase the recipient's situational awareness. The Office of Intelligence also has an all-source analytic detachment at the CBP National Targeting Center that supports the NTC mission of managing field encounters with potential terror suspects and determines the admissibility of high-risk persons.

7. What are some examples of how CBP intelligence provides support to the day to day operations of other DHS component agencies like ICE or Coast Guard?

Response: The CBP and ICE intelligence offices meet two times a week to discuss threat reporting and to share information on other issues of mutual interest. All CBP intelligence alerts and reports are routinely disseminated to ICE and ICE has used some of these reports to support or initiate criminal investigations. Homeland Security Intelligence Reports (HSIRs) produced by CBP intelligence are disseminated to DHS/I&A and DHS components.

8. Can you explain in greater detail how the Border Patrol Field Intelligence Center (BORFIC) supports the operational elements of CBP? How does the BORFIC share information and intelligence with other federal fusions centers like the El Paso Intelligence Center (EPIC) or ICE's Field Intelligence Units (FIUs)?

Response: The Border Patrol Field Intelligence Center (BORFIC), which was established in

January 2004 as the national border intelligence center for the U.S. Border Patrol, adds intelligence value in all aspects of the execution of the CBP Office of Border Patrol National Strategy. BORFIC facilitates the development and management of the national intelligence requirements for OBP; utilizes the intelligence cycle to help achieve OBP National Strategy goals and to maintain situational awareness of the national borders. In support of CBP's National Border Patrol Strategy, BORFIC conducts intelligence analysis to support CBP's operational field elements with actionable all-threat operational intelligence that serve to predict, deter, detect, identify and interdict terrorists, terrorist weapons, undocumented aliens, narcotics and smugglers of people and contraband at the nation's borders. BORFIC is also responsible for assessment, planning, and direction of intelligence assets to address all threats, risks, and vulnerabilities that exist on the U.S. borders through facilitating the collection of raw information needed to produce refined, actionable, and timely intelligence products and through processing and distilling raw information into a usable, easily understandable format. BORFIC analyzes and produces finished national level intelligence reports (e.g. Notes, Bulletins, Homeland Security Intelligence Reports (HSIR). All finished intelligence products are disseminated to all DHS intelligence entities, as well as federal, state, local and foreign entities authorized and having a need to know.

BORFIC management, analysts, and data researchers routinely contact and collaboratively work with the twenty CBP Office of Border Patrol Sector Field Intelligence Units (SIU) on a daily basis. The BORFIC Collection Manager actively participates in the bi-monthly Tri-Center Collection Management meetings with the collection managers of the El Paso Intelligence Center (EPIC) and Joint Task Force North. These meetings ensure that respective agency intelligence requirements are fully coordinated and supported, where possible, by the other agencies.

An ICE Senior Intelligence Research Specialist has been assigned full-time to BORFIC since its inception and serves to liaison with the ICE Southwest Border Field Intelligence Unit (FIU). In addition to being fully integrated in all BORFIC intelligence activities, the specialist ensures that key information and intelligence is shared with the FIUs on a daily basis. The ICE Intelligence Research Specialist for the El Paso Detentions and Removal Office (DRO) attends the BORFIC daily Analysts' Meeting and has an office and workstation at BORFIC. The ICE representative facilitates coordination and information sharing between BORFIC and DRO assets nationally.

The U.S. Army's Foreign Military Studies Office (FMSO) in Fort Leavenworth, KS is the U.S. Army's Center of Excellence for Open Source Intelligence (OSINT). FMSO has had a representative assigned to BORFIC on either a full-time or part-time basis since 2004. The FMSO representative is currently physically present on a part-time basis, but is immediately available as needed and responsive on a daily basis in support of mutual intelligence requirements.

BORFIC maintains a close working relationship with the El Paso Intelligence Center (EPIC), Joint Task Force North (DOD), the U.S. Coast Guard, White House Office of Drug Control Policy (ONDCP), FBI and various Joint Terrorism Task Forces nationwide, National Drug Intelligence Center (NDIC – DOJ), various High Intensity Drug Trafficking Agencies (HIDTAs), Joint Canadian – U.S. Integrated Border Enforcement Teams (IBETs), Royal Canadian Mounted Police and Canadian Border Services Agency, the U.S. Embassy to Canada, the U.S. Embassy to Mexico, Mexican Attorney General's Office (PGR), Mexican National Immigration (INM), and Mexican Federal Preventive Police (PFP), and the Honduran National Police.

9. What role does the CBP Air Marine Operations Center (AMOC) have in the contribution of operational intelligence for CBP?

Response: The Air and Marine Operations Center (AMOC) produces air-centric, tactical and operational intelligence through the fusion of live radar input, law enforcement, and investigative data with real-time and historical information from flight databases. AMOC's ability to tap national intelligence and unique local databases compliments the fusion and drives the placement of CBP Air and Marine assets for tactical interdiction and improved detection and deterrence.

10. What are some examples of Intelligence, Surveillance, and Reconnaissance (ISR) assets owned by CBP and how do they contribute to operational/tactical intelligence being produced to better secure our borders?

Response: The CBP Air and Marine Program owns several Intelligence, Surveillance, and Reconnaissance assets that directly contribute intelligence for securing the borders. Examples include: the Air and Marine Operations Center, which employs radar input and investigative data to provide tactical and operational intelligence; P-3 systems, which are multi-sensor, multi-intelligence platforms capable of receiving national-level intelligence; and Unmanned Aircraft Systems (UAS) surveillance and reconnaissance platforms. The P-3 border and foreign missions provide tactical cueing in support of interdiction as well as detection through multiple sensors of threats beyond the border, allowing the Interagency to collect and posture against these long-range targets. The UAS can provide a long dwell surveillance and reconnaissance capability on areas prone to exploitation, thereby extending the borders and providing tactical cueing to law enforcement officers for interdiction.

The Office of Border Patrol uses Remote Video Surveillance (RVS) systems, with thermal and daytime imaging capability, to detect targets and vector agents for interdiction and resolution. There are two types of RVS in use, static and mobile. Static RVS are usually 70-foot towers that have a platform on the top. One or more pairs (day/night) of cameras are mounted to each tower and remote controlled via microwave or fiber-optic. Mobile RVS assets are usually thermal cameras that are mounted to boom systems and installed on vehicles. This type of RVS is

controlled from the vehicle. RVS can also be used to assist local agencies for law enforcement purposes and for search and rescue. RVS images can be recorded for later enforcement or prosecution use.

The Border Patrol utilizes Unattended Ground Sensors (UGS) with a variety of sensing apparatus (Infrared, seismic, magnetic, etc), which are deployed in a covert manner to detect the presence of potential targets-of-interest. The activation of a UGS is transmitted through a repeater network to the Intelligent Computer Assisted Detection (ICAD) software system and is reported to Border Patrol Agents via radio communications. In addition to their tactical use, sensor data is also analyzed by Office of Border Patrol Sector Intelligence Units to identify traffic/activity patterns.

11. Outside of the CBP Office of Intelligence what centers has CBP established for the collection, production, and dissemination of operational intelligence?

Response: The intelligence component at the CBP Air and Marine Operations Center and the CBP Border Patrol Field Intelligence Center both perform limited collection, production, and dissemination of operational intelligence.

12. In the November 2005 DHS OIG-06-04 report, the report states, "*There is little institutional incentive for CBP and ICE to share and coordinate intelligence*". Do you believe there is an institutional incentive for CBP and ICE to share and coordinate field intelligence? What is that incentive and how is CBP and ICE coordinating field intelligence?

Response: CBP Office of Intelligence continues to place a high priority on intelligence coordination and sharing. Specifically, CBP and ICE have made significant improvements in intelligence sharing since the DHS OIG survey referenced above was conducted. At headquarters, CBP Office of Intelligence is an active member of the CBP-ICE Coordination Council established in response to Department direction for ICE and CBP to work more closely together. CBP and ICE intelligence personnel have worked jointly on a number of DHS and interagency working groups and analytic projects – all of which have had an impact on agency field operations. CBP and ICE analysts meet twice weekly to discuss ongoing analytic projects and identify opportunities to collaborate.

13. The Treasury Enforcement Communication System (TECS) was never designed to facilitate intelligence analysis, yet it is used for this purpose. TECS is a "pull-orientated" system. CBP and ICE personnel first have to know which records may be useful to them before being able to access them on the system. A "pull-orientated" system is not conducive for intelligence analysts to produce, retrieve, review, or share intelligence.

- How is TECS used in the CBP intelligence enterprise for the production of operational intelligence? What other types of IT systems are used by CBP to produce, retrieve, review, or share operational intelligence?

Response: The Office of Intelligence currently uses TECS, as well as the Joint Worldwide Intelligence Communication System (JWICS), the Homeland Security Data Network (HSDN), the Intelligence Reporting System (IRS – a recently developed tool intended as a replacement for a legacy Office of Border Patrol intelligence reporting system), and unclassified and classified email to share operational intelligence throughout CBP.

14. Are there issues of sharing operational intelligence between the DHS component agencies and other federal entities? What are some of those issues and in your opinion what are some potential solutions?

Response: CBP continues to work closely with the Department of Homeland Security and its external partners to ensure that intelligence collected by CBP and intelligence needed by CBP to carry out its border mission is adequately communicated and shared. Specifically, the CBP Office of Intelligence continues to work with the DHS Chief Intelligence Officer and his information management staff to ensure effective intelligence sharing with DHS and external partners.

15. In the November 2005 DHS OIG-06-04 report, the report states, CBP "...intelligence is disseminated and received through a myriad of systems..." What are some of those systems CBP uses to disseminate and receive intelligence and how can those systems be improved?

Response: The Office of Intelligence currently uses TECS, the JWICS and HSDN classified systems, and unclassified and classified email to share operational intelligence throughout CBP. The Office of Intelligence is working with the CBP intelligence enterprise and the CBP Office of Information and Technology to identify CBP-wide intelligence IT requirements that include improvements to our intelligence reporting systems and more robust intelligence sharing both inside CBP (between field components as well as with headquarters components) and with our external partners.

Questions from Representative Rob Simmons for
ICE Acting Director of Intelligence Cynthia O'Connell

1. In your opinion, what is the number one intelligence issue ICE faces? Is it lack of access to national intelligence? Information sharing within the department and other federal agencies? Lack of personnel?

Response: Information sharing continues to be a problem and ICE is working to ensure that its

expertise helps in developing practical solutions.

2. In your opinion, what is the number one threat to our border?

Response: The greatest threat facing the security of our borders is the vulnerability to illegal smuggling of people and contraband.

3. Do you have the necessary analytical staff and resources to perform your mission?

Response: The goal for the ICE Office of Intelligence (Intel) is to develop intelligence plans and resources based on business plans, customer evaluations and performance metrics. Intel has established relationships to share and receive information from agencies that include the CIA, NSA, National Guard, U.S. Geological Survey, Citizenship and Immigration Services, Federal Air Marshals, Financial Crimes Enforcement Network, and the DHS Office of Intelligence and Analysis.

4. What is a recent example of ICE intelligence directly supporting an arrest or interdiction of illegal material?

Response: First, on May 8, 2006, CBP Inspectors at the Miami International Airport examined a passenger targeted by the ICE North East Field Intelligence Unit. The passenger was arrested for smuggling and more than four pounds of heroin were seized.

Second, during a daily review of classified reporting, an ICE Intelligence Analyst assigned to the National Security Integration Center (NSIC) determined that a foreign national involved in fundraising for a designated foreign terrorist organization had recently entered the United States. The resulting investigative lead sent to ICE Joint Terrorism Task Force agents resulted in the individual's arrest in early June 2006.

Third, ICE Intelligence supports the National Security Council's Inter-Agency Working Group on human smuggling, which is responsible for 26 ICE-led arrests of Special Interest Alien Smugglers.

Fourth, on virtually a daily basis, ICE Intelligence collection assets provide tactical interdiction information that directly leads to seizure or destruction of numerous multi-ton drug shipments.

5. What are some examples of how ICE intelligence provides support to the day to day operations of other DHS component agencies like CBP or Coast Guard?

Response: ICE Intelligence, through Operation Watchtower, provides real time actionable intelligence on maritime smuggling to CBP and the Coast Guard. ICE's Tactical Intelligence

Center routinely supports Coast Guard deep water drug interdictions by providing intelligence on the activities of trafficking organizations. ICE Intelligence's Albuquerque Special Operations Center (ASOC) also coordinates daily with CBP. Moreover, ICE and CBP share classified intelligence during daily Secure Video Teleconferences and routine meetings, on matters of mutual interest.

6. In the November 2005 DHS OIG-06-04 report, the report states, "*There is little institutional incentive for CBP and ICE to share and coordinate intelligence*". Do you believe there is an institutional incentive for CBP and ICE to share and coordinate field intelligence? What is that incentive and how is CBP and ICE coordinating field intelligence?

Response: As partner agencies within DHS, ICE and CBP have an institutional incentive to share and coordinate intelligence and are currently doing so through joint efforts, such as Operations Capistrano, Roswell, and Watchtower, and the Port Intelligence Center. ICE and CBP are members of a DHS Coordination Council and further joint and parallel areas of responsibility.

7. The Treasury Enforcement Communication System (TECS) was never designed to facilitate intelligence analysis, yet it is used for this purpose. TECS is a "pull-orientated" system. CBP and ICE personnel first have to know which records may be useful to them before being able to access them on the system. A "pull-orientated" system is not conducive for intelligence analysts to produce, retrieve, review, or share intelligence.

- How is TECS used in the ICE intelligence enterprise for the production of operational intelligence? What other types of IT systems are used by ICE to produce, retrieve, review, or share operational intelligence?

Response: TECS is a highly valuable resource for conducting research in support of law enforcement intelligence products. TECS was also the primary system used to produce, retrieve, review, and share intelligence. ICE and CBP currently employ a sophisticated web-based system known as the Intelligence Reporting System (IRS) to prepare intelligence products and information reports at the headquarters and field level. Electronic reports from both agencies are indexed and housed within the DHS Operations Intelligence Fusion System, which is available to more than 10,000 authorized users within the federal government. This fusion system consists of over 50 million indexed names, intelligence products, subject records, reports of investigation, and open-source information on topics that include smuggling, terrorism, and transnational trends. This platform creates the most robust intelligence-sharing environment currently available within DHS. It also ensures that the analysis and intelligence generated by one agency is immediately available to other interested agencies. In April 2006 ICE developed an enhancement to the TECS system that provides the Office of Investigations with a method to acknowledge ICE Intel leads and track Intel leads that develop into open criminal investigations

and enforcement actions. This enhancement provides an opportunity to not only quantify the direct utility of Intel leads but it also directly assists in analyzing the type and nature of the content of Intel leads that develop into active investigations.

8. Are there issues of sharing operational intelligence between the DHS component agencies and other federal entities? What are some of those issues and in your opinion what are some potential solutions?

Response: Many of the barriers to sharing information between agencies that existed prior to the terrorist attacks of September 11, 2001, have been removed. Many of the practices government agencies instituted since then have allowed for the free flow of information. While there is always room for improvement, the open exchange of information has greatly enhanced our ability to share information with our intelligence and law enforcement partners.

9. What is a typical day for one of the ICE Field Intelligence Units (FIUs) along the border? How many information reports will they receive; what type of operational support will they be focused on; what other agencies or centers will they work with?

Response: A Field Intelligence Unit analyst:

- Monitors incoming information via classified/unclassified message traffic;
- Checks information through databases;
- Provides both tactical and operational intelligence on a daily basis to DHS, ICE, CBP, and U.S. Coast Guard personnel.
- Writes reports of intelligence and investigations, uploads the information into TECS and the Fusion Site, and distributes the information directly to customers.
- Attends meetings to obtain information from other federal law enforcement offices, state and local entities, and state and local law enforcement offices.
- Networks with analysts, investigators, inspectors, and others within and outside ICE on ongoing projects.
- Conducts checks on information via ad hoc requests from the field units, and is sometimes detailed to long-term investigations to conduct analysis of investigative information.
- Produces flow charts, time-lines, organizational charts, and other investigative evidence and exhibits when needed for analysis and case support purposes.
- Receives 50 to 100 informational reports a day, which are analyzed and disseminated to field offices as Memorandums of Information Received (MOIRS), intelligence alerts, and studies.
- Obtains information on narcotics, arms and strategic technology, human smuggling, and financial crimes from the High Intensity Financial Crimes Area, High Intensity Drug Trafficking Area, Federal Bureau of Investigation, Drug Enforcement Administration, United States Coast Guard, Field Intelligence Support Teams, El Paso Intelligence Center, Financial Crimes Enforcement Network, and National Drug Information Center.

10. What type of tactical and operational intelligence support to investigative and interdictory field assets does the ICE Office of Intelligence provide?

Response: The Office of Intelligence provides tactical and operational support to the ICE Office of Investigations on a daily basis, often as part of multi-year criminal investigations of complex conspiracies that require expert analytical support in both foreign and domestic intelligence venues. Network, telephone toll and financial analysis is conducted daily to support field investigators. ICE Intelligence is also increasing its ability to successfully leverage foreign assets in support of ICE investigations. For example, the ICE Intelligence facilitated the positive identification of an international alien smuggler residing in Eastern Europe who was previously known by first name only to domestic investigators.

11. What is and what type of operational support does ICE intelligence provide to the National Security Integration Center?

Response: In support of the overall ICE mission to protect the homeland and identify potential threats to national security, the ICE Office of Intelligence partnered with the Office of Investigations to create and staff the ICE National Security Integration Center (NSIC). The goal of the NSIC is the co-location and coordination of intelligence and operations related to ICE national security investigations. In addition to ICE Office of Intelligence and Office of Investigations personnel, the NSIC is staffed by representatives from the Federal Protective Service (FPS), the Federal Air Marshal Service (FAMS) and the U.S. Citizenship and Immigration Services Fraud Detection and National Security (FDNS) Unit. The Office of Intelligence serves as the primary entity within the NSIC responsible for researching; processing, analyzing, coordinating and disseminating classified intelligence reporting. Intelligence personnel are the main points of contact within the NSIC for coordination and communication with the Intelligence Community. They review open-source reporting, daily message traffic from the Intelligence Community, and significant field reporting that pertains to matters of national security. All information pertaining to potential threats, such as possible terrorist attacks or terrorist travel to the United States, is shared and coordinated with NSIC Office of Investigations counterparts. This coordination includes a joint evaluation of the credibility of the reporting and any potential for ICE enforcement action to combat the threat. When necessary, ICE Intelligence personnel work with the Intelligence Community to obtain additional information or make specific requests to member agencies.

In addition to coordinating intelligence reporting, ICE Intelligence personnel utilize DHS databases to "operationalize" threat reporting. They assesses threat reporting on high-risk foreign nationals, develop investigative leads relating to identified national security vulnerabilities, and identify non-obvious relationships between known or suspected terrorists and individuals located in the United States.

Questions for the Record
House Homeland Security
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
"DHS Intelligence and Border Security: Delivering Operational Intelligence"
June 28, 2006
Assistant Secretary Charles Allen, Assistant Commissioner for Intelligence James F. Sloan,
CBP Intelligence Executive Director Thomas Bortmes, &
ICE Acting Director of Intelligence Cynthia O'Connell

12. With the Detention and Removal Office (DRO) housing nearly 19,000 detainees at any given time, how does ICE intelligence assist in the real-time identification and screening of ICE detainees and the collection/processing of intelligence gathered from the detainees and their property?

Response: The ICE Office of Intelligence coordinates and oversees Operation Last Call, a comprehensive initiative to interview detained aliens in ICE custody to elicit intelligence information relating to areas of interest to the intelligence community and ICE's core mission areas.

13. What type of operational intelligence support is provided to Arms & Strategic Technology investigations as it relates to the unauthorized movement/procurement of critical technology, dual-use goods, chemical, biological, radiological, nuclear/conventional weapons, and unauthorized exports to sanctioned countries?

Response: ICE Intelligence analysts create a comprehensive quarterly report in which companies exporting high-risk dual risk technologies to proliferation countries or high-risk transshipment countries are identified. This report is provided quarterly to the ICE Office of Investigations.

ICE Intelligence also produces a monthly report of upcoming defense industry shows, conferences, expositions, and other similar events. This report is valuable to the Office of Investigations because foreign technology collectors often attend these events.

ICE ASTI analysts regularly meet with the Defense Security Service (DSS) to collect, review, research, and disseminate investigative leads for the Office of Investigations. This DSS reporting often includes foreign requests for U.S. technology that is export-controlled.

14. How are ICE operational intelligence requirements represented in the Intelligence Community?

Response: Currently, ad hoc foreign intelligence requirements are tasked, in the form of a Request for Information (RFI), to individual intelligence agencies based on specific operational needs. ICE Intelligence compiles and prioritizes operational intelligence requirements based on information needs driven by the ICE law enforcement mission. Standing collection requirements and information that can be collected overseas by the Intelligence Community are drafted as ICE Priority Intelligence Requirements (PIRs) and submitted to DHS Intelligence and Analysis for subsequent tasking to the U.S. Intelligence Community. ICE currently has over 200 standing intelligence requirements tasked to the Intelligence Community.

Questions for the Record
House Homeland Security
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
"DHS Intelligence and Border Security: Delivering Operational Intelligence"
June 28, 2006
Assistant Secretary Charles Allen, Assistant Commandant for Intelligence James F. Sloan,
CBP Intelligence Executive Director L. Thomas Bortmes, &
ICE Acting Director of Intelligence Cynthia O'Connell

Questions from Representative Bennie Thompson for Assistant Secretary Charles Allen

1. Mr. Allen, sharing border intelligence is sort of pointless if it doesn't tell a story and doesn't advise people what they need to do, what they need to prepare for, and what they should be on alert about.

- What is I&A doing to ensure that CBP, ICE, and Coast Guard are preparing and disseminating specific and actionable border intelligence information on a consistent basis?

Response: The Office's primary action to ensure that CBP, ICE and Coast Guard are preparing and disseminating border intelligence on a consistent basis is our reports officers program. My reports officers have access to law enforcement databases at CBP and ICE and they identify information that responds to Intelligence Community requirements and which has a nexus to border intelligence issues. This information is, in turn, disseminated to the Department Intelligence Enterprise and the Intelligence Community via Homeland Intelligence Reports (HIRs). HIRs are the Department's primary vehicle for sharing raw, unevaluated information with the Intelligence Community. The Coast Guard has a longstanding capability in this area, using the Intelligence Information Report (IIR) as its reporting format for unevaluated intelligence.

- From your vantage point in I&A, what determines who gets information and who does not, and how important is it for border intelligence to be shared to and from State, local, and tribal law enforcement?

Response: From the Office's vantage point, customer requirements and their priority drive who receives information and in what time frame. Sharing of border intelligence with state, local and tribal authorities is very important for maintaining a complete threat picture along the border. The Office seeks to ensure that sharing of intelligence and information is coordinated between federal and non-federal partners and occurs as widely as possible.

2. Mr. Allen, it seems to me that doing a risk assessment is a critical first step before making spending decisions relating to border security. A risk assessment should be informed by good intelligence about the threats we face at our borders.

- What kinds of border intelligence – in your view – should the Department be able to provide Congress and other policymakers us so we can help you assess, prepare, and respond to threats?

Response: The DHS Intelligence Enterprise should provide decision makers with the highest quality all-source assessments, using the most current available intelligence on the range of

border-related threats. We should provide the relevant threat assessments based on national intelligence collections and reporting, which is integrated with local and regional assessments and information. The assessments and information must be provided at the lowest possible classification level.

- What kinds of intelligence do you think will give us the biggest bang for the buck at the border?

Response: All-source intelligence analysis will give the United States the "biggest bang" by providing the capability to understand and counter effectively border threats, both tactically and strategically. National intelligence collection, reporting and analysis must be fused with DHS component, law enforcement, and operational information, along with other information generated at the state and local levels. Foreign partner information, particularly from Mexico and Canada, is critical to our efforts. Analytic findings and conclusions stemming from this intelligence must be appropriately actionable. We must constantly examine the range of available intelligence and information, identify the critical threats, and expertly integrate them to provide analyses and context specifically tailored to customers at the federal, state and local levels.

3. Mr. Allen, some of the law enforcement executives along the northern border that our staff has talked to tell us that the Canadians have no turf battles or political axes to grind when it comes to information sharing and accordingly are much more willing to share. They blamed the many bureaucracies at the border – CBP, ICE, DEA, FBI, and others – as creating a confusing maze that hampered sharing. What, in your view, would help us get beyond the apparent turf disputes that persist at our borders?

Response: We are working to facilitate more effective information sharing at our borders, among federal agencies, with our international partners, and with our state, local, and tribal partners with border security missions.

Key initiatives include the establishment of the government-wide Information Sharing Environment (ISE), a high level U.S./Canadian working group under the auspices of the Security and Prosperity Partnership of North America (SPP); DHS' State and Local Fusion Center Implementation Plan, which is establishing the policy and technology to support strategically-located regional and state information clearinghouses with strong federal participation; a pilot program in Seattle, WA that allows non-federal partners direct access to federal databases; and developing performance metrics to measure the effectiveness of information sharing activities.

The interagency effort to establish an ISE, first required by Executive Order 13356, and, then codified in the Intelligence Reform and Terrorism Prevention Act of 2004, will address many of the existing impediments to effective information sharing, including at the borders. For example, one of the first ongoing, critical ISE tasks is the development of a common framework for the

sharing of information between federal agencies and state, local and tribal governments, and the private sector. In addition to the common framework for sharing with non-federal partners, federal procedures for the designating, marking, and handling of sensitive unclassified information will be standardized and streamlined to make it easier to share sensitive but unclassified information with non-federal partners. The ISE effort is also separately examining the means to facilitate information sharing with international partners.

The SPP, a trilateral initiative with Canada and Mexico, also aims to improve cross-border information sharing and interoperability. DHS is the U.S. interagency lead for implementing the goals established by the SPP's Security Action Plan, which includes bilateral planning for increased interoperability with the Canadians.

In June 2006, Secretary Chertoff approved the DHS State and Local Fusion Center Implementation Plan, which focuses on developing and maintaining critical partnerships with state, local, tribal and territorial governments. Federal agencies, like DHS and DOJ, are both suppliers of information to and consumers of information in the fusion centers. Fusion centers allow non-federal partners access to a broader picture in serving as clearinghouses for information sharing.

Another initiative is to create the policy and technology for a collaborative tool that allows federal, state, and local partners to interact in a trusted collaborative environment. Access to the trusted environment will be based on roles and responsibilities. The tool ultimately will allow direct access to certain federal data sets so that users can perform their own direct queries. The direct access query tool will be informed by the lessons learned in the ongoing pilot program in the Seattle area, which involves both the FBI and ICE.

Finally, I&A is leading efforts to develop and implement performance metrics for information sharing that link to the Department's strategic goals. In order to produce immediate, near-term, and long-term improvements in information sharing processes and systems, metrics that link to these goals must be collected and analyzed. This effort will measure the level and utility of information sharing programs both within DHS and between DHS and external homeland security partners.

4. Mr. Allen, you recently testified about intelligence fusion centers and your office's efforts to populate them with I&A representatives to promote better communications with State, local, and tribal law enforcement.

- What, if anything, are you doing to encourage CBP, ICE, and Coast Guard personnel to staff fusion centers in border states, and how might they help you promote a consistent and far-reaching sharing of border intelligence information?

Response: As approved by Secretary Chertoff on 7 June 2006, the Office is the Executive Agent overseeing the SLFC program. As a first step in this program, we are conducting field visits to operational SLFCs to evaluate how best to support relationships between DHS and the fusion centers. After our evaluation is complete, we will make recommendations, tailored to each individual SLFC, on instituting the most appropriate and effective mix of federal and nonfederal personnel. By integrating DHS personnel within fusion centers, intelligence sharing will become more comprehensive, providing national level reporting to state and local authorities while developing rapport and trust between analysts and operators in furthering a consistent and far-reaching information sharing culture.

- To what extent have you explored the possibility of sending I&A staff to state and regional intelligence fusion centers to promote border intelligence?

Response: We are conducting field visits to SLFCs to evaluate how to best support relationships between DHS and state and local fusion centers. After our evaluation is complete, we will make recommendations for assigning intelligence officers to individual SLFCs. While the fusion centers are under state or local control, we are the DHS executive agent for ensuring that each center has the most appropriate and effective mix of DHS, other federal agency, and non-federal personnel. Our "boots on the ground" personnel will facilitate the development of a fully integrated enterprise, spanning federal, state, local and tribal jurisdictions, and will focus on the requirements of both DHS and its non-federal partners. These actions will help to produce an integrated and effective information sharing enterprise, to include promoting border intelligence.

5. Mr. Allen, it seems to me that technology must be part of the solution to promote information sharing at the border. Just yesterday, the Department's Inspector General issued a report that was very critical of the Homeland Security Information Network (HSIN). Law enforcement apparently doesn't think its offering much of any value – it doesn't have much useful information, they don't trust it, and they're falling back on tried and true ways of sharing.

- What are your comments on the IG's report, and what are you doing to make things better?

Response: The IG report recognized several challenges that the HSOC encountered during the implementation of HSIN, including the tight timeline prescribed to rapidly deploy this information sharing tool, which did not allow for much consultation with prospective user communities. Prior to the IG report, the HSOC had already identified the need to implement additional processes and governance to overcome many of the issues raised in the report. During the implementation of the I&A's HSIN-Intel and HSIN-S communities, we utilized business practices such as consultations with the users on requirements definition, focused training, and additional user feedback mechanisms, to enhance the chances of a more successful deployment.

- How will the IG report on HSIN impact your border intelligence strategies going forward?

Response: We are already in the process of identifying and validating specific requirements, creating sound business processes, and matching them to more suitable informational tools that further our border intelligence mission. We are applying multi-level applications and collaboration technology that will enable seamless sharing between all DHS components, federal, state, local and tribal partners.

- What thought have you given to including a border intelligence-specific feature on HSIN that can be accessed by State and locals?

Response: I&A is currently evaluating our HSIN-INTEL pilot program; as part of our evaluation, we will examine how to best meet our customers' intelligence needs, including for border intelligence. I have already undertaken several initiatives to make more intelligence information available on HSIN. For example, my Office already is using the HSIN portal to facilitate collaboration on border security intelligence, as part of my Intelligence Campaign Plan (ICP) to the southwest border. Personnel in the Arizona Department of Public Safety are the first state and local users to have access to the ICP website.

6. Mr. Allen, my question goes to interoperability. While interoperable communications is not an intelligence issue per se, it appears that even if I&A, CBP, ICE, and the Coast Guard want to share all the information they possess with State, local, and tribal law enforcement, the inability to communicate via radio would stymie their efforts.

- How central is improving interoperable communications to your strategy of improving information sharing generally , and what role if any are you playing in any Department-wide effort to address the issue?

Response: I have established an Information Management (IM) Division, staffed with experts in IT integration to resolve the technology barriers to information sharing across the DHS Intelligence Enterprise. Working closely with the Department's Chief Information Officer, the IM Division is rapidly devising and implementing solutions for interoperable intelligence communications, pushing connectivity down to our front-line personnel, and enabling access to data regardless of its source or location.

- What programs or policies or funding plans would you support to make interoperable communications a reality between the Department's intelligence components and State, local, and tribal law enforcement – at the border and elsewhere?

Response: We have recently completed an architecture study of the DHS Intelligence Enterprise and are completing an implementation plan to fill in the gaps in communications and information flow throughout the enterprise. We will work through our Intelligence Systems Board, reporting

jointly to the Intelligence Council and the CIO Council, to prioritize this implementation plan and identify any shortfalls in resources. I anticipate that we will leverage, to the maximum extent possible, the DHS CIO's OneNet and Homeland Secure Data Network (HSDN) programs.

7. Mr. Allen, we've heard from law enforcement professionals who serve communities along the northern border that there are vast expanses of territory where no CBP or ICE agents are present. Law enforcement is concerned that like drug smugglers and human traffickers before them, terrorists will soon figure out the relative ease with which the northern border can be crossed without detection. To what extent is I&A taking these facts on the ground into account as part of your longer-term border intelligence strategy? How is this information helping you to support a risk-based approach to homeland security at the border?

Response: We have an aggressive production plan on border security that will greatly increase our ability to understand border threats. My analysts use a holistic approach in addressing the full spectrum of border-related threats. We recognize the need for far greater border security than presently exists, and my Intelligence Campaign Plan for Border Security will establish a plan for full integration with the operating components.

8. Mr. Allen, what guidance, policies, or procedures does I&A have in place or have planned to encourage CBP, ICE, and the Coast Guard to hold regular meeting with sheriffs, chiefs of police, and other local law enforcement in border communities to share information? To the extent this is done on more of an informal, ad hoc basis, how might you encourage something more consistent?

Response: We recognize that there are multiple elements of DHS that are present, or have equities in, the State and Local Fusion Centers (SLFCs). For example, CBP officers and ICE agents, and Protective Security Advisors (PSAs, from the Infrastructure Protection Directorate) are already deployed throughout the United States and have developed working relationships at many SLFCs. While these meetings are not currently prescribed by policy, I see value in holding regular meetings between DHS components and law enforcement agencies with concurrent jurisdiction at the SLFCs. I have asked my SLFC program office to assess how to institutionalize such a practice. In addition, the Homeland Security Intelligence Council (HSIC), the advisory group for DHS intelligence integration, is developing standardized policies for the DHS Intelligence Enterprise that will address, among other things, the intelligence components' interactions with state and local authorities on the border.

In addition to the I&A activities described above, DHS components also staff Joint Terrorism Task Forces (JTTFs), OCDETF and HIDTA task forces nationwide, and ICE-created Border Enforcement and Security Taskforces (BEST). These various, multi-agency task forces foster an environment of information sharing and joint operations across federal, state, local and tribal agencies.

9. Mr. Allen, what is "border intelligence" in your view – what should it include, who is developing it, who should be receiving it, and how should it be shared? Also, what role should State, local, and tribal law enforcement play in the "border intelligence" process?

Response: The border challenge is multi-faceted and the associated reporting, research, analysis and production on diverse border threats must drive towards the understanding and mitigation of the many cross-border challenges that cause violence.

State, local and tribal enforcement entities should be full partners with the Intelligence Community and should participate to the fullest extent in both providing and receiving border security information. The traditional Community provides multi-source collection and reporting, but non-intelligence partners, such as federal, state, and local law enforcement organizations, gather a wealth of operational and investigative information that is crucial to border intelligence efforts. Whether the information is raw, unevaluated reporting or analytic findings and conclusions, border intelligence and information must flow freely, within the bounds of national security directives and the law, to the operational elements charged with the execution of the border security mission. A thorough, efficient interaction between the DHS Intelligence Enterprise and a broad range of partners will produce an effective information sharing atmosphere. This interaction will feed the intelligence cycle with information obtained at the border and will allow resultant intelligence products to be more complete and accurate.

10. Mr. Allen, I've been hearing a phrase used to describe how work is shaking out in your office and among the components – the need for folks to know their "lanes in the road." What is meant by "lanes in the road"? What are the proper lanes for CBP, ICE, and Coast Guard, and what is your proper lane, Mr. Allen?

Response: The phrase "lanes in the road" refers to authorities and responsibilities designated to certain DHS intelligence-related agencies and offices. For example, a key "lane," or mission area, for this Office is to analyze the use of non-conventional weapons by terrorists for key customers. CBP, ICE and the Coast Guard have "lanes" that are dictated by their respective agency missions and authorities. I am cognizant of the "lanes" of agencies within the DHS Intelligence Enterprise components, and will seek to enhance the fulfillment of their missions. My primary "lane" is to lead and manage the integration of the DHS intelligence components into a common enterprise. This is one my five key goals, or intelligence pillars, and is in accordance with Department Management Directive 8110, on "Intelligence Integration and Management." I have taken several steps to realize the objective of a fully integrated DHS Intelligence Enterprise. For example, I produced a DHS Intelligence Enterprise Strategic Plan to provide the shared vision for the enterprise; conducted program reviews of each DHS Intelligence Component to evaluate how effectively the enterprise is progressing towards a shared vision; and instituted the Homeland Security Intelligence Council Intelligence Integration

Board in order to address key substantive integration challenges across the intelligence cycle. I have also included the enterprise components as partners in the development of the Intelligence Campaign Plan.

11. Mr. Allen, there has been enormous discussion about the competing immigration bills in the Congress, and I note that the Sensenbrenner bill that passed the House includes a proposal to build a double set of steel walls with floodlights, surveillance cameras and motion detectors along one-third of the U.S.-Mexican border. Other physical barriers envisioned under the Sensenbrenner bill include radar, satellite, and Unmanned Aerial Vehicles (UAV) to ensure fuller coverage of the border. To what extent has I&A been consulted regarding these investments, and how is the border intelligence available to you informing these priorities?

Response: We were not directly consulted on the proposal in the Sensenbrenner bill to deploy surveillance cameras, motion detectors, and other sensors along the U.S.-Mexico border. However, my office, as DHS' Executive Agent for Intelligence, Surveillance and Reconnaissance (ISR), will identify those ISR technologies that will ensure improved coverage of the border. It will work closely with the relevant DHS components to identify and deploy the most strategic and advantageous mix of sensors, platforms and architectures for border security purposes. In addition, my Intelligence Campaign Plan (ICP) will drive the integration of information from these technologies with national level intelligence to better prioritize selection and placement of border technologies. Lastly, this Office will work closely with CBP to ensure that the best intelligence and information guides CBP decision making about the best mix of technology, infrastructure, and personnel.

Questions from Representative Bennie Thompson for
Assistant Commandant for Intelligence James F. Sloan

1. At the hearing, Mr. Allen described his campaign plan for border security. He stated that his plans and initiatives that are "on their way" or at least are being planned. To what extent is intelligence that is being developed in your offices being used to inform the campaign plan? What is Mr. Allen's process for incorporating your office into this planning, and what time frames are you aware of regarding the campaign plan?

Response: The Coast Guard Intelligence and Criminal Investigations Program staff has been working closely with and will continue to support the Department's staff in their endeavor to develop the Department's Intelligence Campaign Plan. Coast Guard capabilities and contributions are routinely integrated by the Office of Intelligence and Analysis with those of other DHS intelligence components.

2. Where, in your view, it the greatest threat at our borders – the northern border with Canada or the southern border with Mexico?

Response: While the Coast Guard can provide information for the maritime borders, a comprehensive answer to this question is best provided by DHS and would involve "For Official Use Only (FOUO)" and classified material presented in an appropriate venue.

3. What is "border intelligence" in your view – what should it include, who should be receiving it, and how should it be shared? What obligations do each of you, in your view, have to share "border intelligence" with State, local, and tribal law enforcement officers along the border?

Response: The role of Coast Guard Intelligence is to provide timely, accurate and actionable maritime border related information and other pertinent intelligence information so that decisions can be made and actions taken in support of the Coast Guard operational commanders, other members of the Intelligence Community, and law enforcement agencies.

The Coast Guard Intelligence and Criminal Investigations Program has established and actively participates in several partnerships to enhance border security and other Homeland Security activities:

- The Coast Guard and Navy continue to build an effective joint intelligence partnership to enhance maritime awareness. The Coast Guard's Intelligence Coordination Center is co-located with the Office of Naval Intelligence, which together comprise the National Maritime Intelligence Center (NMIC).
- The Coast Guard has provided access to its intelligence databases, advice to others developing intelligence sharing architectures, and provided intelligence analysts, exchange personnel, and liaison officers with other agencies active in the maritime arena.

The Coast Guard's partners are at all levels of government (local, state, and federal) and in the private sector. The Coast Guard provides timely dissemination of intelligence information related to homeland security. Within that framework, the CG uses a variety of methods to share intelligence information with state and local officials:

- Under the Maritime Transportation Security Act, the CG disseminates intelligence information to state and local officials through Area Maritime Security Committees.
- CG Field Intelligence Support Teams (FISTs) and CG Investigative Service (CGIS) Special Agents work closely with state and local law enforcement to share intelligence information.
- In close coordination with DHS I&A, the CG rapidly disseminates terrorist threat warning information to the maritime industry.
- Some of the coordination between the Coast Guard and state/local governments is formally recognized through memoranda of understanding, but much is also accomplished via informal working relationships.

4. We currently have more than 10,000 Border Patrol agents stationed along the1,933-mile southern border and 1/10th that number along the 5,525-mile northern border. We haven't heard

about any terrorist arrests in Mexico, but we've learned a lot over the last few weeks about a terrorist plot in Canada to use fertilizer bombs to blow up government buildings. It seems to me that "border intelligence" should at least tell us where we should be spending our money to keep us safe.

- In light of the Canadian arrests, what are your thoughts about where we have our border resources deployed, and how is border intelligence informing those choices? Should we be reconsidering our border security efforts in light of the recent arrests in Canada?

Response: While the Coast Guard can provide information for the maritime borders, a comprehensive answer to this question is best provided by DHS and would involve "For Official Use Only (FOUO)" and classified material presented in an appropriate venue. The Coast Guard will continue to work with the Department of Homeland Security and those components who participate in the Department's Border Security Initiative.

5. There has been enormous discussion about the competing immigration bills in the Congress, and I note that the Sensenbrenner bill that passed the House includes a proposal to build a double set of steel walls with floodlights, surveillance cameras and motion detectors along one-third of the U.S.-Mexican border. Other physical barriers envisioned under the Sensenbrenner bill include radar, satellite, and Unmanned Aerial Vehicles (UAV) to ensure fuller coverage of the border. To what extent have CBP, ICE, and USCG been consulted regarding these investments, and how does the border intelligence available to you inform these priorities? Based on the border intelligence that you have, where along the border is the greatest need for these kinds of investments and why?

Response: This Office will work closely with both CBP and ICE to ensure that the best intelligence and information guides CBP decision making about the best mix of technology, infrastructure, and personnel. The Coast Guard will continue to support the requirements from the Department regarding maritime borders, and has been involved in the planning and other deliberations related to various border security initiatives.

6. We've heard from staff that in some of the Department's component intelligence offices, information sharing isn't happening from location to location or from sector to sector within your own agencies. In other words, CBP or ICE agents in one area aren't talking to their counterparts in another area. That's ridiculous. How serious is the problem of not sharing within each of your agencies, how are you working to promote information along the border, and what technology solutions would be helpful to promoting a consistent sharing of information across sectors?

Response: As a member of the Information Sharing, and Collaboration (ISC) Program we are part of the overall initiative within the Department that seeks to improve information sharing and

collaboration:

- Within each of the Directorates of the Department,
- Between DHS elements, and
- With our state, tribal, and territorial, local, and private sector partners responsible for securing the people and infrastructure of this country.

Both the Coast Guard and DHS have standard connectivity through telephone (both classified and unclassified systems), standard INTERNET connectivity, Non-Classified Internet Protocol Router Network (NIPRNET) connectivity, Secret Internet Protocol Router Network (SIPRNET) connectivity, Joint Worldwide Intelligence Communications System (JWICS), and secure Video Tele-Conference (VTC) connectivity.

The Coast Guard has taken a leadership role within DHS to ensure that intelligence products are shared rapidly and accurately throughout the federal government. Threat information and reports of suspicious activities gleamed by the Coast Guard from the maritime industry and other maritime stakeholders are shared with appropriate Intelligence Community members, appropriate offices within DHS, and the National Response Center (NRC). The Coast Guard has provided access to its intelligence databases, advice to others developing intelligence sharing architectures, and provided intelligence analysts, exchange personnel, and liaison officers with other agencies active in the maritime arena.

Additionally, the Coast Guard and Navy continue to build an effective joint intelligence partnership to enhance maritime awareness. The Coast Guard's Intelligence Coordination Center is co-located with the Office of Naval Intelligence, which together comprise the National Maritime Intelligence Center (NMIC).

7. I understand that the operational intelligence at the border involves the day-to-day information that your agents and officers in the field come to possess during the course of their everyday activities. How are each of your agencies taking that information and turning it into an intelligence product; how are you consistently sharing those products with your customers; and what of this day-to-day information are you sharing with State, local, and tribal law enforcement at the border?

Response: The majority of field information on a day-to-day basis within the Coast Guard is through the Field Intelligence Support Teams (FISTs) currently located at 30 ports. The primary mission of the FISTs are port-level intelligence collection and reporting in support of Coast Guard operations and Homeland Security missions, intelligence training of local CG personnel, and liaison with Federal, state, local, tribal and industry partners.

FISTs have reported on activity that could be terrorist pre-operational planning and have helped identify threats in the maritime environment, including illicit drug and human smuggling

operations, avenues for potential sea borne terrorist attacks and persons using maritime means to enter the United States illegally for nefarious purposes.

FISTs provide improved intelligence collection and sharing with Federal, state & local agencies; better port-level threat assessments; and enhanced overall maritime domain awareness. We have had great success with FIST personnel actively engaged with other Federal, state and local agencies through participation with local level entities, such as the Joint Terrorism Task Force, Antiterrorism Advisory Committees, Law Enforcement Coordinating Committees and Regional Domestic Security Task Forces.

FISTs report on activities and security in foreign ports using information gathered from ship master and crew interviews. These interviews are used to help identify pertinent issues that impact or have the potential to impact maritime security and trade, and identify/target potential threats arriving to the U.S. from foreign ports of interest/concern.

FIST vessel master surveys and "ship-jumper" (i.e., stowaways, absconders and deserters) interviews help identify patterns in ship-jumper activity, which increase interdiction rates through better targeting. Interviews also help identify threats in the maritime environment, including illicit drug, weapon and human smuggling operations; the threat of sea borne terrorist attacks; and persons using maritime means to enter the U.S. illegally for criminal purposes.

8. One complaint our staff has been hearing is that while State, local and tribal law enforcement reports information up the chain to your respective agencies, officers are less than thrilled with intelligence information that they get back. What are you hearing from sheriffs and chiefs of police on this front, how valid is this criticism, and what – if anything – are you doing about it?

Response: The Coast Guard's partners are at all levels of government (local, state, and federal) and in the private sector. Specific intelligence information, related to homeland security, is facilitated through the Department of Homeland Security's Office of Intelligence and Analysis, when appropriate. The Coast Guard also uses a variety of methods of sharing information:

- Under the Maritime Transportation Security Act, the Coast Guard disseminates intelligence information to state and local officials through Area Maritime Security Committees.
- Coast Guard Field Intelligence Support Teams (FISTs) and Coast Guard Investigative Service (CGIS) Special Agents work closely with state and local law enforcement to share intelligence information.
- In close coordination with DHS I&A, the Coast Guard rapidly disseminates terrorist threat warning information to the maritime industry.
- Some of the coordination between the Coast Guard and state/local governments is formally recognized through memoranda of understanding, but much is also accomplished via informal working relationships.

9. Please explain whether you think it makes sense to create a centralized border intelligence network that offers current, specific, and actionable intelligence to all border security stakeholders across the country – including State, local, and tribal law enforcement officers.

Response: Further improvements in the border intelligence realm are clearly warranted. The multi-jurisdictional aspects alone (i.e., federal, state, local, and tribal) associated with securing our borders, both on land and the water, are highly complex and challenging. A better integrated and more effective border intelligence network would enhance information collection, sharing and dissemination across jurisdictional lines; maximize the scant law enforcement and intelligence resources responsible for protecting our Nation's border; and improve interagency targeting, coordination and response. There are many networks already in place and any new "network" must build upon existing relationships, centers, and infrastructure.

10. In my view, there cannot be effective border security or immigration policy without a thorough understanding of the terrorist threat at the border. That threat cannot be fully appreciated if (1) CBP, ICE, and USCG are not effectively sharing information with each other; and (2) they are not consistently sharing information with State, local, and tribal law enforcement in jurisdictions along the nation's borders who can act as "force multipliers" in the border intelligence process. How are you sharing border intelligence among yourselves, what improvements can be made in this area, and how do you consult with each other and identify what kinds of information would be most helpful for your particular missions?

Response: As a member of the Information Sharing, and Collaboration (ISC) Program, we are part of the overall initiative within the Department that seeks to improve information sharing and collaboration:

- Within each of the Directorates of the Department,
- Between DHS elements,
- Across the cabinet level departments and agencies; and
- With our State, tribal, and territorial, local, and private sector partners responsible for securing the people and infrastructure of this country.

As part of this overall effort, the Department of Justice (DOJ) and DHS information sharing staffs are working to bring the Homeland Security Information Network (HSIN), Law Enforcement On-line (LEO), and Regional Information Sharing System (RISS) together with the goal of making the systems more compatible as quickly as possible.

Both the Coast Guard and DHS have standard connectivity through telephone (both classified and unclassified systems), standard INTERNET connectivity, Non-Secure Internet Protocol Router Network (NIPRNET) connectivity, Secure Internet Protocol Router Network (SIPRNET) connectivity, Joint Worldwide Intelligence Communications System (JWICS), and secure Video Teleconferencing (VTC) connectivity.

The Coast Guard has taken a key enabling role within DHS to ensure that intelligence products are shared rapidly and accurately throughout the federal government. Threat information and reports of suspicious activities gleamed by the Coast Guard from the maritime industry and other maritime stakeholders are shared with appropriate Intelligence Community members, appropriate offices within DHS, and the National Response Center (NRC).

Additionally, the Coast Guard and Navy continue to build an effective joint intelligence partnership to enhance maritime domain awareness. The Coast Guard's Intelligence Coordination Center is co-located with the Office of Naval Intelligence, which together comprise the National Maritime Intelligence Center (NMIC).

The Coast Guard has provided access to its intelligence databases, advice to others developing intelligence sharing architectures, and provided intelligence analysts, exchange personnel and liaison officers with other agencies active in the maritime arena. These liaison officers are located at: National Counterterrorism Center (NCTC), National Reconnaissance Office (NRO), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), Northern Command (NORTHCOM), Pacific Command (PACOM), Joint Terrorism Task Force (JTTF), Department of Justice (DOJ), National Geospatial-Intelligence Agency (NGA), National Security Agency (NSA), Department of Homeland Security/Intelligence and Analysis (DHS/IA), Custom Border Patrol (CBP), Defense Intelligence Agency (DIA), Southern Command (SOUTHCOM), El Paso Intelligence Center (EPIC), Department of Transportation (DOT), and Department of Defense (DoD).

The Coast Guard and CBP have exchanged personnel to enhance data sharing between the CG Intelligence Coordination Center's COASTWATCH (which gathers and analyzes information on ship notice of arrival reports on vessels, people and certain dangerous cargoes approaching U.S. ports) and CBP's National Targeting Center (cargo tracking) process.

11. It seems to me that so much of information sharing between your agencies and with State, local, and tribal law enforcement depends upon personal relationships. I would imagine that the law enforcement in the jurisdictions along the border know the geography of their counties and towns even better than your people do. For purposes of border intelligence, how valuable to each of your agencies are personal relationships with State, local, and tribal law enforcement and what policies and procedures do you have in place to reach out to locals?

Response: The Coast Guard's partners are at all levels of government (local, state, federal and tribal) and in the private sector. The Coast Guard provides timely dissemination of intelligence information related to homeland security. The Coast Guard uses a variety of methods to share intelligence information to state and local officials:

- Under the Maritime Transportation Security Act, the Coast Guard disseminates intelligence information to state and local officials through Area Maritime Security Committees.

- Field Intelligence Support Teams (FISTs) leverage information sharing relationships with federal, state and local government officials and the maritime industry and conduct liaison activities as part of their duties. In coordination with local area Commanders, FIST members attend meetings and perform duties at other agencies, task forces, and committees in order to facilitate their duties.

- Sector Intelligence Officer (SIOs) ensure the appropriate sharing of intelligence and law enforcement information not only between Coast Guard commands and the Department of Homeland Security, but also other federal, state, local and Intelligence Community elements at the port level in accordance with applicable law and policy.

The Coast Guard Investigative Service currently participates in 28 FBI Joint Terrorism Task Forces (JTTFs) located in areas with a direct nexus to Coast Guard maritime operations conducted in support of Homeland Security and Homeland Defense missions. In this liaison role, CGIS agents interact with those first responders, such as Coast Guard operational commanders, local and state law enforcement, and various maritime industry stakeholders.

Border Intelligence in Practice

12. We've heard from law enforcement professional who serve communities along the northern border that there are vast expanses of territory where no CBP or ICE agents are present. Law enforcement is concerned that like drug smugglers and human traffickers before them, terrorists will soon figure out the relative ease with which the northern border can be crossed without detection. To what extent are your respective agencies taking this into account as part of your border intelligence work, and how is this informing a risk-based approach to border security?

Response: There are vast areas of unmonitored northern maritime border. The USCG maritime law enforcement response has been focused on deterrence and partnerships to reduce the maritime risk.

With respect to deterrence, the Coast Guard has mounted automatic weapons on all our multi-mission patrol resources on the northern maritime border. These, along with our traditional maritime law enforcement boardings, serve as deterrence to criminal activities.

The Coast Guard partnerships involve other U.S. Government agencies, but also include a number of Canadian agencies. The Coast Guard is an active member of Integrated Border Enforcement Teams (IBET) having a maritime nexus. IBET is comprised of Coast Guard, ICE, CBP, Royal Canadian Mounted Police (RCMP) and Canadian Border Security Agency (CBSA), along with state, local, provincial and tribal enforcement agencies. The IBET mission is to

enhance border integrity and security at our shared border by identifying, investigating, and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity. There are 15 IBET regions along the northern border, eight of which include vast distances of maritime border.

Additionally, with Canada, the Coast Guard has prototyped a resource multiplier; the shiprider operation. The concept is simple: RCMP officers are placed on board local Coast Guard Station small boats and the RCMP officer has the lead in Canadian waters, while the USCG officer is supporting as directed. The converse is true while in US waters. The shiprider concept has been used on two occasions with Canada. The first was in September 2005 where the Great Lakes Shiprider operation was the first time that armed law enforcement officers from Canada and the United States have conducted joint maritime law enforcement operations in each other's waters. The second operation was conducted for eight days during Superbowl XL to provide integrated maritime security for the many bi-national events hosted in both Detroit and Windsor. After the two week proof of concept in September, the government of Canada initiated an extensive evaluation to formulate their required legislative changes before undertaking long-term steady state operations. The U.S. is still waiting for Canada to take the necessary action to authorize these operations. Depending on the Canadian framework, the shiprider concept could be used by all IBET partners.

Because the RCMP report found that its maritime law enforcement capabilities and competencies need improvement, Coast Guard is helping RCMP develop these skills. The RCMP is currently trying to expand their maritime footprint, but is awaiting funding for additional resources.

In addition, the Coast Guard Intelligence and Criminal Investigations Program conducts activities and shares law enforcement information regarding the security of the northern U.S. border through the following:

- Field Intelligence Teams (FISTs) - The primary missions of the FISTs are port-level intelligence collection and reporting in support of Coast Guard operations and homeland security missions, intelligence training of local Coast Guard personnel, and liaison with Federal, state, local, tribal and industry partners. There are currently 30 FISTs.

- FBI Joint Terrorism Task Force (JTTF) – The Coast Guard currently has representation in 28 FBI JTTF offices located in areas with a direct nexus to Coast Guard maritime operations being conducted in direct support of Homeland Security and Homeland Defense operations.

- District and Sector Intelligence Officers – The focus is at the tactical level assisting in completing a tactical intelligence picture for operational customers.

13. Many of the sheriffs and chiefs of police that our staff has spoken to along the northern border reported that they regularly receive more specific and actionable intelligence information from their Canadian counterparts, who typically meet with them on a monthly basis. At times, the officers added, the Canadians included representatives from the Canadian Security and Intelligence Service (CSIS) at meetings. What guidance, policies, or procedures do each of your agencies have in place to hold regular meeting with sheriffs, chiefs of police, and other local law enforcement to share information? To the extent this is done on more of an informal, ad hoc basis, how might you encourage something more consistent?

Response: Field Intelligence Support Teams (FISTs) leverage information sharing relationships with federal, state and local government officials and the maritime industry, and conduct liaison activities as part of their duties. In coordination with local area commanders, FIST members attend meetings and perform duties at other agencies, task forces, and committees in order to facilitate their duties. It is important to note that they are not assigned a level of involvement that precludes their primary duties of collecting and reporting. Sector Intelligence Officer (SIOs) ensure the appropriate sharing of intelligence and law enforcement information not only between Coast Guard commands and the Department of Homeland Security, but also among other federal, state, and local elements at the port level in accordance with applicable law and policy.

The Coast Guard is an active member of Integrated Border Enforcement Teams (IBET), having a maritime nexus. IBET is comprised of Coast Guard, ICE, CBP, Royal Canadian Mounted Police (RCMP) and Canadian Border Security Agency (CBSA), along with state, local, provincial and tribal enforcement agencies. The IBET mission is to enhance integrity and security at our shared border by identifying, investigating, and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity. There are 15 IBET regions along the northern border, eight of which include vast distances of maritime border. IBET joint management teams from each geographic region meet on a regular basis to coordinate enforcement operations, and to share law enforcement intelligence.

14. Some of the law enforcement executives along the northern border that our staff has talked to tell us that the Canadians have no turf battles or political axes to grind when it comes to information sharing and accordingly are much more willing to share. They blamed the many bureaucracies at the border – CBP, ICE, DEA, FBI, and others – as creating a confusing maze that hampered sharing. What, in your view, would get us closer to more of a Canadian approach and is the Canadian approach more desirable that what apparently exists in the field?

Response: There are two primary federal law enforcement agencies in Canada, the Royal Canadian Mounted Police (RCMP) and Canadian Border Security Agency (CBSA) (whose personnel currently do not carry weapons). The RCMP, comprised of approximately 23,500 personnel, performs the same functions as at least six U.S. federal agencies (USCG, CBP, ICE, DEA, ATF and FBI). Additionally, RCMP does contract law enforcement for certain provincial

and local governments.

RCMP currently has MOU/MOAs with several U.S. federal agencies dealing with each agency's specific authorities. This confuses the information sharing on the U.S. side.

The Canadian enforcement approach is generally regarded as under-resourced, and the RCMP evaluation on the September 2005 Great Lakes Shiprider proof of concept found that its maritime law enforcement capabilities and competencies need improvement. The Coast Guard is helping RCMP develop these MLE skills. The RCMP is currently trying to expand their maritime footprint, but is waiting funding for additional resources.

The Coast Guard's Intelligence Coordination Center (ICC), COASTWATCH and the National Maritime Intelligence Center (NMIC) share a variety of information products with counterpart intelligence agencies in Canada. A regular shared product is NMIC's daily "Vessels of Interest" (VOI) message. The VOI message provides strategic warning about the approach of commercial ships of intelligence or law enforcement interest to the U.S. and the shared maritime border with Canada.

The El Paso Intelligence Center (EPIC) Branch of the Coast Guard ICC maintains around-the-clock communications with the Royal Canadian Mounted Police (RCMP) Operations Center in Ottawa, Canada. EPIC and RCMP exchange tactical law enforcement information to assist federal, state, and local investigation and interdiction of narcotics, alien and other smuggling activities. This responsive interaction has led to a number of successful cross-border maritime and land interdictions of illegal migrants, stowaways and narcotics.

Both the Canadian Unit "TRINITY" and MIFC LANT have coordinated tactical intelligence cueing and information on a vessel with suspect illegal migrants on board transiting along U.S. eastern seaboard en route to Canada. TRINITY provided the initial targeting data and MIFC LANT assisted in the tracking of the vessel up the U.S. eastern seaboard en route to Canada for a successful interdiction by Canadian agencies.

The Role of I&A

15. Its wonderful that your component agencies have a positive working relationship with the Department's Office of Intelligence and Analysis (I&A), but I'm troubled about who is doing what at the Department. I imagine that each of your respective agencies have particular intelligence expertise – CBP with border issues, ICE with immigration information, and Coast Guard with maritime issues. What is the proper intelligence role for your offices versus the proper intelligence role for I&A? Who should be doing operational intelligence analysis in your view and who should be doing the strategic work? How much autonomy do you have to do the work you need to do and get it out to folks, and is I&A a help or a hindrance in that process?

Questions for the Record
House Homeland Security
Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee
"DHS Intelligence and Border Security: Delivering Operational Intelligence"
June 28, 2006
Assistant Secretary Charles Allen, Assistant Commandant for Intelligence James F. Sloan
CBP Intelligence Executive Director L. Thomas Bortmes, &
ICE Acting Director of Intelligence Cynthia O'Connell

Response: The Coast Guard and other DHS intelligence components have a good working relationship and various mechanisms that provide mutual support in ways that reflect respective organizational strengths and mission mandates. There is extensive information sharing between and among the various DHS components.

The DHS Office of Intelligence and Analysis provides direct intelligence support to the Secretary and supports the Chief Intelligence Officer (CINT) in his responsibility to ensure the Department provides strategic all-source analysis to a wide range of homeland security stakeholders, taking full advantage of all intelligence sources, including those of the DHS components, and also through the Chief Intelligence Officer, leading and managing the integration of the DHS Intelligence Enterprise.

Interoperability

16. My question goes to interoperability. While interoperability is not an intelligence issue per se, it appears that even if your agencies wanted to share all of the information you possess with each other and with State, local, and tribal law enforcement along the border, the inability to communicate via radio would prevent your efforts. One sheriff our staff spoke to reported that he actually purchased radios and gave them to CBP officers in his county so he could talk and coordinate with them. How bad is the interoperability problem in your estimation, what would help most to get everyone on the same frequency so to speak, and how can Congress help?

Response: DHS needs to make further improvement in interoperability and has undertaken initiatives in this area. One example relates to computer network connectivity; disparate network domains remain a challenge. At the unclassified level, the .com / .mil. / .gov domains cannot be engineered into a flat network (a network in which all stations can reach other without going through any intermediary hardware devices, such as a bridge or router). Thus it is difficult to effectively share information via data linkages. Under the Homeland Security Information Network (HSIN) program, DHS initiatives are focused on this specific problem to improve unclassified network interoperability with state and local law enforcement entities.

Homeland Security Information Network

17. I note that the Department of Homeland Security's Inspector General publicly released a report about the Homeland Security Information Network (HSIN) – the Department's main point of connection with outside homeland security partners – which detailed some troubling findings, including that (1) HSIN users are confused about its role in relation to other systems with similar functionality and are unsure about which to use and, more specifically, how to most effectively use HSIN; (2) HSIN users are frustrated about Department feedback that information they input into HSIN is not useful; (3) some HSIN users do not trust HSIN to share their sensitive case information; (4) HSIN is not providing the situational awareness that is needed to support counterterrorism work at the local level; and (5) HSIN's Secret portal does not include much

useful information. As a result, the IG found that State and local officials by and large do not rely on HSIN and have resorted to prior ways of sharing – using preexisting information sharing networks, and personal contacts, as alternatives.

• It seems to me that HSIN would be one viable option for your agencies to share border intelligence with each other and with law enforcement. How concerned are you about the IG's findings, what recommendations do you have to address these problems, and would you support a HSIN feature that would address border intelligence specifically?

Response: The Coast Guard Intelligence and Criminal Investigations Program (ICIP) has not reviewed the IG report mentioned above. Recent updates about current HSIN planning presented at the Department of Homeland Security (DHS) Information Sharing Board indicate that DHS is working to evolve the HSIN infrastructure and wide area network capabilities to facilitate the new border initiatives.

Fusion Centers

18. We have been hearing a tremendous amount lately about state and regional intelligence fusion centers, and the law enforcement representatives we spoke to have high hopes that they will serve as a source of border intelligence for them. What presence do each of your agencies have at fusion centers, and how might they help you promote a consistent and far-reaching sharing of border intelligence information? To what extent have you explored the possibility of sending staff to state and regional intelligence fusion centers to promote border intelligence?

Response: The Coast Guard Intelligence Program generally does not participate on a full-time basis with any state or local/regional fusion centers, but instead engage in information sharing with various state, local/regional fusion centers on an ad hoc, case-by-case basis.

However, the Coast Guard Investigative Service (CGIS) currently has representatives in 28 FBI Joint Terrorism Task Force (JTTF) offices located in areas with a direct nexus to Coast Guard maritime operations conducted in support of Homeland Security and Homeland Defense missions. In this liaison role, the CGIS agent interacts with those first responders, such as Coast Guard operational commanders, local and state law enforcement, and various maritime industry stakeholders.

Questions from Representative Bennie Thompson for
CBP Intelligence Executive Director L. Thomas Bortmes

1. At the hearing, Mr. Allen described his campaign plan for border security. He stated that his plans and initiatives that are "on their way" or at least are being planned. To what extent is intelligence that is being developed in your offices being used to inform the campaign plan?

What is Mr. Allen's process for incorporating your office into this planning, and what time frames are you aware of regarding the campaign plan?

Response: The CBP intelligence enterprise has participated, to varying degrees, in the DHS Intelligence Campaign Plan initiative. For example, a Deputy Director from the Office of Intelligence sits on Mr. Allen's Intelligence Campaign Plan working group. CBP intelligence analysts have participated in threat-related working groups. The most recent DHS I&A focus area that CBP is aware of relates to Operation Jump Start and the deployment of National Guard troops to the southwest border.

2. Where, in your view, it the greatest threat at our borders – the northern border with Canada or the southern border with Mexico?

Response: While CBP can provide information for the borders, a comprehensive answer to this question is best provided by DHS and would involve "For Official Use Only (FOUO)" and classified material presented in an appropriate venue.

3. What is "border intelligence" in your view – what should it include, who should be receiving it, and how should it be shared? What obligations do each of you, in your view, have to share "border intelligence" with State, local, and tribal law enforcement officers along the border?

Response: "Border intelligence" is the intelligence required to understand all U.S. borders, all the threats to those borders and to maintain situational awareness of what is occurring on those borders. Its purpose is to enable those responsible for the protection of those borders to effectively respond to potential threats. It results from the fusion and analysis of all related basic/encyclopedic (i.e. geographic, demographic, etc) information, operational reporting and intelligence reporting from all federal, state, local, tribal, private and commercial sources. It is all-source information that has been analyzed or assessed for use by decision-makers at the local, regional, and national levels to determine how best to allocate their resources. Border intelligence should be available to all those who can act on it and to those that can use it to improve their decision making process. Provided appropriate security procedures are adhered to, it should not matter if the recipient is at the Federal, State, or local level. CBP is aggressively pursuing an intelligence structure and process that ensures fusion of CBP-unique and external information and intelligence to provide a complete common intelligence picture that supports all levels of the organization as well as our partners.

4. We currently have more than 10,000 Border Patrol agents stationed along the1,933-mile southern border and 1/10th that number along the 5,525-mile northern border. We haven't heard about any terrorist arrests in Mexico, but we've learned a lot over the last few weeks about a terrorist plot in Canada to use fertilizer bombs to blow up government buildings. It seems to me that "border intelligence" should at least tell us where we should be spending our money to keep

us safe.

- In light of the Canadian arrests, what are your thoughts about where we have our border resources deployed, and how is border intelligence informing those choices? Should we be reconsidering our border security efforts in light of the recent arrests in Canada?

Response: A vital component to achieving CBP's goal of controlling the borders is partnering with other law enforcement agencies. To identify specific border threats, CBP has strengthened its partnerships with Canadian and Mexican law enforcement and intelligence officials as well as with officials from other federal state, local, and tribal organizations by leveraging information and increasing communication and cooperation.

The role of CBP intelligence is to ensure that a comprehensive assessment of border threats is available to CBP leadership so that they have a clear understanding of all border threats, border vulnerabilities, and criminal intent enabling them to make decisions about how and where border resources are best deployed. Although a single security threat (i.e. the Canadian arrests) needs to be considered when developing such assessments, it should be considered in light of the overall border threat environment.

5. There has been enormous discussion about the competing immigration bills in the Congress, and I note that the Sensenbrenner bill that passed the House includes a proposal to build a double set of steel walls with floodlights, surveillance cameras and motion detectors along one-third of the U.S.-Mexican border. Other physical barriers envisioned under the Sensenbrenner bill include radar, satellite, and Unmanned Aerial Vehicles (UAV) to ensure fuller coverage of the border. To what extent have CBP, ICE, and USCG been consulted regarding these investments, and how does the border intelligence available to you inform these priorities? Based on the border intelligence that you have, where along the border is the greatest need for these kinds of investments and why?

Response: Customs and Border Protection believes in a comprehensive solution that puts together the right mix of personnel, technology, and tactical infrastructure to gain control of our borders. The appropriate deployment of personnel, sensors, and vehicle barriers will sometimes be more appropriate and effective than a steel wall. Furthermore, Customs and Border Protection Air & Marine's (A&M) mission is to protect the American people and critical infrastructure by using an integrated and coordinated air and marine force to detect, monitor, intercept, and track suspect conveyances involved with the illegal movement of people, illicit drugs, and other contraband through source, transit, and arrival zones, thereby preventing acts of terrorism arising from these actions. A&M, therefore, supports any efforts to strengthen our borders. A&M believes expanding the Unmanned Aircraft System (UAS) program, including acquiring more Unmanned Aerial Vehicles (UAV), will best serve this mission.

Under the current operational plan, employing all current assets as efficiently as possible, intelligence along the borders shows that there are still gaps in surveillance, which create known areas of vulnerability. A&M can only act upon what it can detect. These areas of vulnerability are constantly changing, as those who wish to infiltrate our borders learn at what border crossing points they can escape detection. As surveillance moves, so do the criminals and their activities. With an expanded UAS force, A&M will be able to better provide complete border surveillance, eliminating these vulnerabilities and drastically reducing the number of illegal border crossings.

UASs provide the airborne technological capability to monitor borders along the southern and northern United States borders. UAVs can provide responsive surveillance and reconnaissance 24 hours a day, seven days a week. This capability is especially vital in areas historically prone to exploitation; UAVs can augment crewed aircraft and vessels to assist in directing ground interdiction agents from all agencies into areas of criminal activity. As with any ground, air, and sea operation, UAVs can provide intelligence to support law enforcement efforts in securing the border and preventing acts of terrorism.

Congress has asked for, and CBP has provided, several briefings about the UAS program and the employment of UAVs in support of crewed aircraft, watercraft, and ground interdiction agents. CBP A&M has further briefed Congress on the UAS concept of operations which include UAV deployment as an aerial platform with multiple collection systems that compliment other CBP interdiction assets.

6. We've heard from staff that in some of the Department's component intelligence offices, information sharing isn't happening from location to location or from sector to sector within your own agencies. In other words, CBP or ICE agents in one area aren't talking to their counterparts in another area. That's ridiculous. How serious is the problem of not sharing within each of your agencies, how are you working to promote information along the border, and what technology solutions would be helpful to promoting a consistent sharing of information across sectors?

Response: While not yet seamless, the situation continues to improve and information sharing becomes more robust. CBP is currently developing recommendations for structure and process improvements and is identifying requirements for an information and intelligence sharing capability that further diminishes stovepipes and provides a CBP-wide common intelligence picture readily accessible to all CBP offices as well as to our partners.

7. I understand that the operational intelligence at the border involves the day-to-day information that your agents and officers in the field come to possess during the course of their everyday activities. How are each of your agencies taking that information and turning it into an intelligence product; how are you consistently sharing those products with your customers; and what of this day-to-day information are you sharing with State, local, and tribal law enforcement

at the border?

Response: CBP recognizes the value of CBP-unique information that is collected by our personnel as they conduct their routine business. The Commissioner has identified as one of his priorities the improvement of structures and process that ensures this information is collected, analyzed, and disseminated throughout CBP and to our partners. CBP's immediate efforts have focused on CBP encounters with terrorism-related suspects. DHS I&A created a "reports officer" program that uses specially trained personnel to glean information of intelligence value from DHS component operational reporting. This information is placed into information reports and disseminated to the greater Homeland Security community. CBP currently has two reports officers assigned to our Headquarters (one physically located at the CBP National Targeting Center – our operational center of gravity for terrorism-related encounters) and they are identifying and reporting back to DHS information of intelligence value on a daily basis. CBP is also exploring a long-term technical solution to collecting and reporting this information. We are working with our Office of Information and Technology to leverage existing operational reporting mechanisms to identify and collect CBP-unique information, in response to customer requirements, in a more automated manner.

8. One complaint our staff has been hearing is that while State, local and tribal law enforcement reports information up the chain to your respective agencies, officers are less than thrilled with intelligence information that they get back. What are you hearing from sheriffs and chiefs of police on this front, how valid is this criticism, and what – if anything – are you doing about it?

Response: State, local, and tribal agencies have long-established, two-way intelligence sharing arrangements with CBP field units. The Office of Border Patrol Field Intelligence Center (BORFIC), Office of Border Patrol Sector Intelligence Units, and Office of Field Operations ports and Field Offices routinely share intelligence bulletins and summaries with other Federal, State, local, and tribal law enforcement agencies. CBP field units participate in a number of forums where there is also State, local, and tribal participation. Some examples include:

- Joint Canadian – U.S. Integrated Border Enforcement Teams (IBETs) on the Northern Border.
- Canadian American Planning Agency (CAPA), founded by the Spokane Sector and the Royal Canadian Mounted Police. CAPA has a bi-national membership that includes 24 State, local, and tribal agencies in addition to 22 Federal and international agencies. CAPA's mission is to promote interagency relationships and foster liaison at the individual officer level.
- High Intensity Drug Trafficking Areas (HIDTA) task forces around the nation.
- Joint Terrorism Task Forces (JTTF) – CBP agents and officers work in JTTFs alongside their State and local colleagues.

CBP continues to work at strengthening information sharing relationships with our colleagues at all levels of law enforcement.

9. Please explain whether you think it makes sense to create a centralized border intelligence network that offers current, specific, and actionable intelligence to all border security stakeholders across the country – including State, local, and tribal law enforcement officers.

Response: To gain operational control of our borders it is critical that current, specific, and actionable intelligence be immediately available to those that have the authorities to act on it. It is also important that all border security stakeholders have access to a common border intelligence picture, while still ensuring appropriate security procedures are followed.

10. In my view, there cannot be effective border security or immigration policy without a thorough understanding of the terrorist threat at the border. That threat cannot be fully appreciated if (1) CBP, ICE, and USCG are not effectively sharing information with each other; and (2) they are not consistently sharing information with State, local, and tribal law enforcement in jurisdictions along the nation's borders who can act as "force multipliers" in the border intelligence process. How are you sharing border intelligence among yourselves, what improvements can be made in this area, and how do you consult with each other and identify what kinds of information would be most helpful for your particular missions?

Response: All CBP intelligence reporting is shared with our DHS colleagues, including ICE and the USCG. Both organizations also have access to all of CBP operational reporting that is consistent with their statutory authorities and mission. Additionally, at the recommendation of the Homeland Security Intelligence Council, a daily secure video teleconference is conducted by DHS I&A that allows DHS intelligence stakeholders to review and discuss current intelligence developments. As part of the DHS I&A managed Homeland Intelligence Integration Board (HIIB), CBP analysts work with all of their DHS intelligence component colleagues on approximately a dozen intelligence working groups to ensure the sharing of all border intelligence.

11. It seems to me that so much of information sharing between your agencies and with State, local, and tribal law enforcement depends upon personal relationships. I would imagine that the law enforcement in the jurisdictions along the border know the geography of their counties and towns even better than your people do. For purposes of border intelligence, how valuable to each of your agencies are personal relationships with State, local, and tribal law enforcement and what policies and procedures do you have in place to reach out to locals?

Response: Personal relationships play an important role in information sharing at all levels of the government. These relationships are especially important at the local level. CBP personnel participate in literally hundreds of local task forces, working groups, and other forums that present opportunities to network and develop collaborative relationships. Equally important are information sharing processes that continue to work even when the personalities involved

change. CBP Office of Intelligence recognizes the importance of policies and technologies that promote information sharing, and is working with our colleagues inside CBP and at DHS on these issues.

Border Intelligence in Practice

12. We've heard from law enforcement professional who serve communities along the northern border that there are vast expanses of territory where no CBP or ICE agents are present. Law enforcement is concerned that like drug smugglers and human traffickers before them, terrorists will soon figure out the relative ease with which the northern border can be crossed without detection. To what extent are your respective agencies taking this into account as part of your border intelligence work, and how is this informing a risk-based approach to border security?

Response: CBP intelligence continues to work with its CBP operational colleagues, DHS partners, and Canadian Border Services Agency (CBSA) partners to develop a better overall understanding of the northern border environment. The border between the U.S. and Canada is over 4,000 miles long and includes extensive water boundaries. At the local and regional level, the CBP intelligence enterprise has robust information sharing practices centered on Integrated Border Enforcement, Maritime, and Intelligence Teams (IBET, IMET, IMIT) that include participation from all levels of U.S. government and our Canadian partners. At the national level, the CBP Office of Intelligence is developing a strong collaborative relationship with our intelligence colleagues at CBSA. Senior managers have met as part of the Heads of Intelligence (HINT) group, which currently includes customs intelligence directors from Australia, Canada, New Zealand, U.K., and U.S., to include ICE, and is being expanded to include our international immigration intelligence counterparts. Analysts from the CBP Office of Intelligence have met with their counterparts in Canada, and are aggressively exploring opportunities for joint intelligence products. CBP is also working with DHS I&A to establish a technology solution to enable more efficient collaboration with all our foreign partners.

13. Many of the sheriffs and chiefs of police that our staff has spoken to along the northern border reported that they regularly receive more specific and actionable intelligence information from their Canadian counterparts, who typically meet with them on a monthly basis. At times, the officers added, the Canadians included representatives from the Canadian Security and Intelligence Service (CSIS) at meetings. What guidance, policies, or procedures do each of your agencies have in place to hold regular meeting with sheriffs, chiefs of police, and other local law enforcement to share information? To the extent this is done on more of an informal, ad hoc basis, how might you encourage something more consistent?

Response: Intelligence and information sharing initiatives have been in place along the northern border for many years. Some are formally established, some more of an ad hoc nature. Customs and Border Protection field officers and agents participate in a number of U.S. and U.S.-Canada collaborative efforts. Examples of these include:

- All CBP Office of Border Patrol sector intelligence units are members of one or more Integrated Border Enforcement/Intelligence Teams (IBET/IBIT) on the northern border. These teams include representation by our other Federal partners, State and local partners, and Canadian agencies.
- The Canadian American Planning Agency (CAPA) includes membership from twenty-four state, local and tribal agencies in addition to twenty-two federal and international agencies. Three northwest states and two Canadian provinces are also represented. CAPA meets quarterly, and periodically includes representation by Canada's CSIS.
- In many locations along the border there are state and local law enforcement agencies that hold weekly or monthly "intelligence group" meetings. CBP field personnel routinely participate in these initiatives.

As discussed above, CBP intelligence is diligently working to improve our capability to share information with all of our partners on all of our borders.

14. Some of the law enforcement executives along the northern border that our staff has talked to tell us that the Canadians have no turf battles or political axes to grind when it comes to information sharing and accordingly are much more willing to share. They blamed the many bureaucracies at the border – CBP, ICE, DEA, FBI, and others – as creating a confusing maze that hampered sharing. What, in your view, would get us closer to more of a Canadian approach and is the Canadian approach more desirable that what apparently exists in the field?

Response: As discussed in response to earlier questions, CBP intelligence is diligently working to improve our capability to share information with all of our partners on all of our borders. CBP is also not aware of any situation in which there was a need to share information but that a "turf battle" or "political axe" prevented the exchange of that information from occurring.

The exchange of information between the United States and Canada is governed by the information sharing laws and policies of both nations. It has been CBP's experience that Canadian privacy laws are generally stricter than those in the US; consequently, situations have arisen in which Canadian officials were prohibited from sharing specific information with their U.S. counterparts, although the U.S. would have been able to share that same information with Canada, had the situation been reversed.

The Role of I&A

15. Its wonderful that your component agencies have a positive working relationship with the Department's Office of Intelligence and Analysis (I&A), but I'm troubled about who is doing what at the Department. I imagine that each of your respective agencies have particular intelligence expertise – CBP with border issues, ICE with immigration information, and Coast Guard with maritime issues. What is the proper intelligence role for your offices versus the proper intelligence role for I&A? Who should be doing operational intelligence analysis in your

view and who should be doing the strategic work? How much autonomy do you have to do the work you need to do and get it out to folks, and is I&A a help or a hindrance in that process?

Response: CBP is responsible for managing, controlling and protecting our borders. The CBP intelligence enterprise, in order to assist our decision makers in gaining operational control of the borders, must provide CBP with a common border intelligence picture with the goal of gaining total border awareness – of all threats at all borders. To accomplish this, CBP intelligence must focus on tactical and operational intelligence focused at our front-line offices. CBP employs the nation's subject matter experts on border issues; this is our area of expertise.

CBP intelligence must also provide high-level operational intelligence analysis along with strategic intelligence analysis to our senior leadership, ensuring they have the strategic intelligence view they need to effectively manage and guide an agency of over 40,000 employees with broad law enforcement and regulatory responsibilities.

CBP intelligence provides our assessments of the borders to DHS I&A as they create the broader strategic view of the threats facing the Department as a whole. The Assistant Secretary for Intelligence and Analysis, in his role as Chief Intelligence Officer (CINT), also has responsibility for leading and managing the integration of the DHS Intelligence Enterprise. The DHS I&A role is to ensure that component intelligence organizations have the capability to receive, disseminate, and share our unique information and analyzed intelligence throughout the Department and to enable analytical collaboration on threats that are common to more than one DHS component. DHS I&A ensures the Department has sound intelligence policies and processes, adequate technology solutions to information management challenges, intelligence training appropriate to the component and Department mission, and robust sharing relationships with the Intelligence Community, other Federal Departments, and our State, local, and tribal colleagues. Finally, I&A supports the CINT in his responsibility to advise the Secretary and Deputy Secretary on the resources needed to support an integrated Departmental Intelligence Enterprise.

Interoperability

16. My question goes to interoperability. While interoperability is not an intelligence issue per se, it appears that even if your agencies wanted to share all of the information you possess with each other and with State, local, and tribal law enforcement along the border, the inability to communicate via radio would prevent your efforts. One sheriff our staff spoke to reported that he actually purchased radios and gave them to CBP officers in his county so he could talk and coordinate with them. How bad is the interoperability problem in your estimation, what would help most to get everyone on the same frequency so to speak, and how can Congress help?

Response: CBP continues to work with its DHS and external partners to ensure required interoperability and the proper movement of information. As a note, CBP Office of Intelligence does not utilize radio communications.

Homeland Security Information Network

17. I note that the Department of Homeland Security's Inspector General publicly released a report about the Homeland Security Information Network (HSIN) – the Department's main point of connection with outside homeland security partners – which detailed some troubling findings, including that (1) HSIN users are confused about its role in relation to other systems with similar functionality and are unsure about which to use and, more specifically, how to most effectively use HSIN; (2) HSIN users are frustrated about Department feedback that information they input into HSIN is not useful; (3) some HSIN users do not trust HSIN to share their sensitive case information; (4) HSIN is not providing the situational awareness that is needed to support counterterrorism work at the local level; and (5) HSIN's Secret portal does not include much useful information. As a result, the IG found that State and local officials by and large do not rely on HSIN and have resorted to prior ways of sharing – using preexisting information sharing networks, and personal contacts, as alternatives.

• It seems to me that HSIN would be one viable option for your agencies to share border intelligence with each other and with law enforcement. How concerned are you about the IG's findings, what recommendations do you have to address these problems, and would you support a HSIN feature that would address border intelligence specifically?

Response: CBP intelligence has stated, on many occasions, our requirement for robust information sharing technology at both the unclassified and classified level. This system should be accessible by all who require access, should provide effective collaboration tools, and should be user-friendly. At this point, CBP Office of Intelligence is working with CBP's Office of Information and Technology to develop the most effective IT infrastructure, to include HSIN, to share intelligence with stakeholders and partners.

Fusion Centers

18. We have been hearing a tremendous amount lately about state and regional intelligence fusion centers, and the law enforcement representatives we spoke to have high hopes that they will serve as a source of border intelligence for them. What presence do each of your agencies have at fusion centers, and how might they help you promote a consistent and far-reaching sharing of border intelligence information? To what extent have you explored the possibility of sending staff to state and regional intelligence fusion centers to promote border intelligence?

Response: CBP Office of Intelligence currently has no physical presence at any of the fusion centers. DHS I&A is working to develop a Department level presence in these fusion centers, and to ensure the proper sharing of DHS developed intelligence.

Other Matters

19. Mr. Bortmes, in our conversations with law enforcement at the borders, most officers

described good working relationships with local CBP officers but felt that "higher ups" within CBP were blocking the flow of information that may be helpful to law enforcement. One officer explained that some at CBP feel that local law enforcement is a competitor, and that when locals arrested someone coming over the border illegally, it was a "black eye" to CBP. Other officers stated that CBP had advised them that the information they could share was limited because they feared that "corrupt cops" would tip off smugglers and others about CBP operations.

- How are CBP agents in the field trained about information sharing and what would your response be to a local sheriff who would like more border intelligence from CBP?

Response: CBP Officers are provided initial and recurrent training and guidance pertaining to the sharing, dissemination, and proper use of border information. As a matter of practice, CBP officers and agents routinely reach out to local law enforcement partners to both obtain needed information and to share CBP information. The CBP Office of Rulings and Regulations, Disclosure Law Branch has, on numerous occasions, issued policy and guidance clearly stating that CBP will share information with state, local, and other law enforcement agencies. It should be noted that state and local law enforcement agencies can access CBP TECS data (e.g. subject records, MOIRs, lookouts, and incident reports, via interface with the El Paso Intelligence Center, or "EPIC. In fact, CBP records are routinely accessed and utilized by state and local law enforcement agencies across the country by means of this interface.

- What concerns do you have about sharing information with local law enforcement?

Response: Effective information sharing is a proven "best practice" for effective operational collaboration. Information sharing must be guided by need-to-know practices and applicable regulations and laws. Actionable intelligence must be readily available to those with the authorities and in the best position to act in response. Consequently, border security stakeholders should be provided with a common awareness of border threats in their geographic area.

20. Mr. Bortmes, I understand that CBP plans to renew the Operation Stonegarden program – one that makes funding available to pay State, local, and tribal law enforcement officers to overtime so they could patrol the borders when CBP is absent. Some of the feedback we've gotten from law enforcement on that program was that they were happy to get the overtime funds in the original operation the first time around, CBP provided them with no direction about where to go or what to do or – more importantly – what to look for. According to some, it was a nice way for cops to make a buck but did nothing for border security. One sheriff our staff spoke to mentioned that Stonegarden II would have much more value if he could pair up his officers with CBP agents in the field. That way, both camps could learn from each other and build the personal relationships that do not always exist from department to department or even officer to officer.

- What do you think of this suggestion, and will Stonegarden II offer State, local, and tribal law enforcement officers this opportunity?

Response: During the original Operation Stonegarden, individual Border Patrol Sectors were in charge of ensuring that state, local, and tribal (SLT) agencies used overtime to further the goal of enhancing overall border security. As set forth by the Department of Homeland Security Office of Grants and Training in current and past Operation Stonegarden guidelines, SLT agencies must continue to work normal patrol duties. The only distinction is that these duties are conducted at, near, or with a nexus to the border. SLT agencies are in no way considered immigration officers during Operation Stonegarden and no immigration authority is conveyed to, nor assumed by, SLTs.

The Border Patrol develops operational plans in conjunction with SLTs to ensure all operations are properly integrated and coordinated and to facilitate SLT officers' ability to know where to go and what to look for. This coordination enables SLT agencies to understand exactly what is expected of them and where they will work their overtime hours. The Border Patrol studied the feasibility of pairing SLT officers with Border Patrol Agents and determined it would not be legally feasible because SLT officers are not immigration officers and Border Patrol Agents are not peace officers in many states. Instead, SLT agencies will work in the same areas as Border Patrol Agents and will have direct access to Border Patrol Agents if the need arises. Teaming agents with officers in the same vehicle is not a force multiplier. Many Border Patrol Sectors invite SLT officers to attend Border Patrol musters before going to the field thus burgeoning positive personal relationships that do not normally transcend from department to department.

- How will mission plans be conveyed to law enforcement to ensure the work they are doing is adding value at the border?

Response: Mission plans will be conveyed to state, local, and tribal (SLT) agencies through co-jointly written operation plans by Border Patrol and SLT agencies. Because the threat-based operation plans are premised upon one of three intelligence scenarios – intelligence, risk, or vulnerability of border areas and routes of egress from the border – SLTs are afforded the opportunity to identify their own threats and input these threats into the overall operation plan, thus ensuring a more comprehensive border security operation. The Border Patrol encourages this input by SLTs and recognizes that border security is a shared concept that is better achieved through the assistance of SLTs.

22. Mr. Bortmes, I understand that Stonegarden II – the successor to the Operation Stonegarden program that CBP managed last year – will offer funding to local departments not only for overtime pay but also for training and hiring intelligence analysts. The officers we spoke with stated that while they welcomed the opportunity to hire an intelligence analyst under Stonegarden II, they worried that (1) the funding would dry up after one year, and it would be

unfair to bring someone on just for that amount of time; (2) there would not be enough for an intelligence analyst to do; and (3) they could not spare an officer to go through the training apparently required for the intelligence analyst position. The money would be better spent, they believe, on directing specific and actionable information to their particular jurisdictions and/or establishing workable interoperable communications with CBP, ICE, and others.

- How do you respond to these concerns, and why is money spent on intelligence analysts for police departments money well spent?

Response: Authorized fund disbursement for Operation Stonegarden includes overtime, travel, and per diem for state, local, and tribal agencies and does not include the hiring or training of intelligence analysts. To ensure funds are not disbursed to items or activities other than those mentioned above, all operations plans submitted from the field are reviewed by both Headquarters Office of Border Patrol and Department of Homeland Security Office of Grants and Training.

Questions from Representative Bennie Thompson for
ICE Acting Director of Intelligence Cynthia O'Connell

1. At the hearing, Mr. Allen described his campaign plan for border security. He stated that his plans and initiatives that are "on their way" or at least are being planned. To what extent is intelligence that is being developed in your offices being used to inform the campaign plan? What is Mr. Allen's process for incorporating your office into this planning, and what time frames are you aware of regarding the campaign plan?

Response: ICE Intelligence reporting related to the Intelligence Campaign Plan for Border Security (ICP) is shared with Mr. Allen's team, which is responsible for drafting the ICP. This reporting includes threat assessments and tactical, operational, and analytical reporting. ICE representatives have been involved in the development of the ICP and continue to participate in its development through working groups, discussions at the Homeland Security Intelligence Council, and other collaborative efforts.

2. Where, in your view, it the greatest threat at our borders – the northern border with Canada or the southern border with Mexico?

Response: While ICE can provide information for both the northern and southern borders, a comprehensive answer to this question is best provided by DHS and would involve "For Official Use Only (FOUO)" and classified material presented in an appropriate venue.

3. What is "border intelligence" in your view – what should it include, who should be receiving it, and how should it be shared? What obligations do each of you, in your view, have to share "border intelligence" with State, local, and tribal law enforcement officers along the border?

Response: ICE considers "border intelligence" to be any information on threats that may affect the border, including violators who operate in the border area, their identities, and the characteristics and vulnerabilities of violator organizations. Such information can and should be shared with any law enforcement entity that can make legitimate use of it with appropriate safeguards.

4. We currently have more than 10,000 Border Patrol agents stationed along the1,933-mile southern border and 1/10th that number along the 5,525-mile northern border. We haven't heard about any terrorist arrests in Mexico, but we've learned a lot over the last few weeks about a terrorist plot in Canada to use fertilizer bombs to blow up government buildings. It seems to me that "border intelligence" should at least tell us where we should be spending our money to keep us safe.

- In light of the Canadian arrests, what are your thoughts about where we have our border resources deployed, and how is border intelligence informing those choices? Should we be reconsidering our border security efforts in light of the recent arrests in Canada?

Response: The recent arrests in Canada do raise serious concerns. The primary mission of ICE Intelligence is to support ICE law enforcement. As best we can, we work with other intelligence components, both domestic and foreign, to watch for northern border threats and indicators of new threat patterns. We concentrate on those areas where the available intelligence and known activity indicate. The recent arrests may be indicative of a shift in the nature of extremist operations on this continent, but it is too soon to tell whether a large-scale shift in border resources is warranted.

5. There has been enormous discussion about the competing immigration bills in the Congress, and I note that the Sensenbrenner bill that passed the House includes a proposal to build a double set of steel walls with floodlights, surveillance cameras and motion detectors along one-third of the U.S.-Mexican border. Other physical barriers envisioned under the Sensenbrenner bill include radar, satellite, and Unmanned Aerial Vehicles (UAV) to ensure fuller coverage of the border. To what extent have CBP, ICE, and USCG been consulted regarding these investments, and how does the border intelligence available to you inform these priorities? Based on the border intelligence that you have, where along the border is the greatest need for these kinds of investments and why?

A long-term analysis of radar and overhead collection could identify vulnerable areas and therefore be beneficial to ICE. However, because CBP is the unified border agency within the

Department of Homeland Security, with primary responsibility for managing, controlling, and protecting the Nation's physical borders, ICE defers to CBP for this response.

6. We've heard from staff that in some of the Department's component intelligence offices, information sharing isn't happening from location to location or from sector to sector within your own agencies. In other words, CBP or ICE agents in one area aren't talking to their counterparts in another area. That's ridiculous. How serious is the problem of not sharing within each of your agencies, how are you working to promote information along the border, and what technology solutions would be helpful to promoting a consistent sharing of information across sectors?

ICE Intelligence offices routinely exchange information through a variety of formal and informal channels. This could be by telephone, computer communications, agency systems, exchange of reports or other intelligence products, and personal contact. This kind of sharing is part of our professional culture and occurs among intelligence components as well as the operational personnel we support. Regarding technology solutions, the most immediate need from an intelligence perspective is a widely deployed system for the timely exchange of classified information in all formats, including text, data, and imagery.

7. I understand that the operational intelligence at the border involves the day-to-day information that your agents and officers in the field come to possess during the course of their everyday activities. How are each of your agencies taking that information and turning it into an intelligence product; how are you consistently sharing those products with your customers; and what of this day-to-day information are you sharing with State, local, and tribal law enforcement at the border?

The information gathered during day-to-day operations at the borders is exploited by both CBP and ICE and is shared with appropriate personnel. The information is vetted through several federal, state, and local databases, which facilitates the development of information into actionable intelligence and provides law enforcement personnel with actionable leads. This information, which would affect state, local, and tribal law enforcement agencies' areas of responsibility, is shared with appropriate customers through computer uploads, electronic means, task force settings, and one-on-one sharing of intelligence.

Through the sharing of information, cases are developed, smuggling groups are identified, and illegal activity is deterred. Some information gathered from concerned citizens is passed to law enforcement officers in their jurisdiction, while some will result in joint investigations.

8. One complaint our staff has been hearing is that while State, local and tribal law enforcement reports information up the chain to your respective agencies, officers are less than thrilled with intelligence information that they get back. What are you hearing from sheriffs and chiefs of

police on this front, how valid is this criticism, and what – if anything – are you doing about it?

Response: The ICE Office of Intelligence routinely receives requests for information from state and local agencies. We strive to provide value-added feedback on intelligence provided by all law enforcement authorities. The Field Intelligence Units participate in numerous task forces and working groups at which intelligence information is routinely exchanged. We are also moving toward integrating the Homeland Security Information Network (HSIN) into our Field Intelligence Units as a way to share classified intelligence in a more timely and efficient manner with state and local law enforcement authorities.

9. Please explain whether you think it makes sense to create a centralized border intelligence network that offers current, specific, and actionable intelligence to all border security stakeholders across the country – including State, local, and tribal law enforcement officers.

Response: This is sensible in principle. However, such a system would be installed alongside other networks and systems that already exist, which would complicate the landscape with yet another learning curve, set of procedures, and security regime that would, of necessity, have multiple levels (e.g., classified vs. unclassified, investigative vs. operational). If a decision is made to create a centralized network, care must be taken not to allow theoretical value to overtake operational efficiency.

10. In my view, there cannot be effective border security or immigration policy without a thorough understanding of the terrorist threat at the border. That threat cannot be fully appreciated if (1) CBP, ICE, and USCG are not effectively sharing information with each other; and (2) they are not consistently sharing information with State, local, and tribal law enforcement in jurisdictions along the nation's borders who can act as "force multipliers" in the border intelligence process. How are you sharing border intelligence among yourselves, what improvements can be made in this area, and how do you consult with each other and identify what kinds of information would be most helpful for your particular missions?

Response: Terrorist-related intelligence is shared with DHS component agencies in a variety of ways. ICE Intelligence participates in the DHS daily secure video tele- conferences (SVTC), various working groups including the Homeland Security Terrorist Integration Group (HSTIG), the Homeland Security Intelligence Council, and the Content Management Board.

Although ICE Intelligence has a strong working relationship with all of the DHS component agencies, we always look to improve or participate in programs that would further enhance our ability to share terrorist-related information. Resources play a pivotal role and have a direct effect on our ability to collect critical terrorism-related intelligence along our southern and northern borders.

11. It seems to me that so much of information sharing between your agencies and with State, local, and tribal law enforcement depends upon personal relationships. I would imagine that the law enforcement in the jurisdictions along the border know the geography of their counties and towns even better than your people do. For purposes of border intelligence, how valuable to each of your agencies are personal relationships with State, local, and tribal law enforcement and what policies and procedures do you have in place to reach out to locals?

Response: Relationships with state, local and tribal law enforcements play a critical role in ICE's ability to share information and determine intelligence gaps that exist in various regions. Our Field Intelligence Units participate in numerous task forces and working groups, which include members from state, local and tribal law enforcement agencies.

Border Intelligence in Practice

12. We've heard from law enforcement professional who serve communities along the northern border that there are vast expanses of territory where no CBP or ICE agents are present. Law enforcement is concerned that like drug smugglers and human traffickers before them, terrorists will soon figure out the relative ease with which the northern border can be crossed without detection. To what extent are your respective agencies taking this into account as part of your border intelligence work, and how is this informing a risk-based approach to border security?

Response: Based upon threat assessments, the ICE's primary focus has traditionally been the southwest border, though we continue to recognize potential threats along the northern border. Three Field Intelligence Units closely monitor potential and on-going threats to northern border security, especially the potential for terrorist mobility and activities. Additionally, ICE participates in numerous northern border task forces and working groups at both the headquarters and field levels.

13. Many of the sheriffs and chiefs of police that our staff has spoken to along the northern border reported that they regularly receive more specific and actionable intelligence information from their Canadian counterparts, who typically meet with them on a monthly basis. At times, the officers added, the Canadians included representatives from the Canadian Security and Intelligence Service (CSIS) at meetings. What guidance, policies, or procedures do each of your agencies have in place to hold regular meeting with sheriffs, chiefs of police, and other local law enforcement to share information? To the extent this is done on more of an informal, ad hoc basis, how might you encourage something more consistent?

Response: Members of our Field Intelligence Units routinely meet and work closely with Canadian counterparts and local law enforcement officers on a formal and ad hoc basis. These meetings include local task forces with representatives from Canada, and working groups focused on information sharing and operational issues. In addition to these working groups, the ICE Intelligence participates in the HSIN working group. We hope to incorporate HSIN into our

Field Intelligence Units as a way to further enhance communication with state and local authorities.

14. Some of the law enforcement executives along the northern border that our staff has talked to tell us that the Canadians have no turf battles or political axes to grind when it comes to information sharing and accordingly are much more willing to share. They blamed the many bureaucracies at the border – CBP, ICE, DEA, FBI, and others – as creating a confusing maze that hampered sharing. What, in your view, would get us closer to more of a Canadian approach and is the Canadian approach more desirable that what apparently exists in the field?

Response: ICE Intelligence's experience with Canadian counterparts has been generally positive in terms of information sharing. However, Canada has MOUs in place with federal agencies that can restrict ICE access to certain types of information. In addition, Canadian law and disclosure requirements at times are barriers to sharing information related to ongoing undercover investigations or sharing information received from ICE confidential informants.

The Role of I&A

15. Its wonderful that your component agencies have a positive working relationship with the Department's Office of Intelligence and Analysis (I&A), but I'm troubled about who is doing what at the Department. I imagine that each of your respective agencies have particular intelligence expertise – CBP with border issues, ICE with immigration information, and Coast Guard with maritime issues. What is the proper intelligence role for your offices versus the proper intelligence role for I&A? Who should be doing operational intelligence analysis in your view and who should be doing the strategic work? How much autonomy do you have to do the work you need to do and get it out to folks, and is I&A a help or a hindrance in that process?

Response: Generally speaking, operational intelligence analysis is driven by mission priorities, subject matter expertise, and operational interest. This leads to individual agencies conducting the type of analysis that supports their own operational mandates. Each component agency has expertise in operational and strategic intelligence, which results in actionable leads. Strategic intelligence is required to develop intelligence-driven investigations, but component agencies should conduct both types of intelligence collection for their respective mission priorities. ICE Intelligence has autonomy to fulfill its responsibilities, but other requests at times divert resources that would otherwise be employed for ICE projects.

Interoperability

16. My question goes to interoperability. While interoperability is not an intelligence issue per se, it appears that even if your agencies wanted to share all of the information you possess with each other and with State, local, and tribal law enforcement along the border, the inability to communicate via radio would prevent your efforts. One sheriff our staff spoke to reported that he actually purchased radios and gave them to CBP officers in his county so he could talk and

coordinate with them. How bad is the interoperability problem in your estimation, what would help most to get everyone on the same frequency so to speak, and how can Congress help?

Response: Although the issue of Interoperability affects the ability to pass information between law enforcement agencies on all levels, ICE Intelligence uses its presence on law enforcement task forces to disseminate critical intelligence information to the broadest possible audience, within appropriate parameters, through local communication networks.

Homeland Security Information Network

17. I note that the Department of Homeland Security's Inspector General publicly released a report about the Homeland Security Information Network (HSIN) – the Department's main point of connection with outside homeland security partners – which detailed some troubling findings, including that (1) HSIN users are confused about its role in relation to other systems with similar functionality and are unsure about which to use and, more specifically, how to most effectively use HSIN; (2) HSIN users are frustrated about Department feedback that information they input into HSIN is not useful; (3) some HSIN users do not trust HSIN to share their sensitive case information; (4) HSIN is not providing the situational awareness that is needed to support counterterrorism work at the local level; and (5) HSIN's Secret portal does not include much useful information. As a result, the IG found that State and local officials by and large do not rely on HSIN and have resorted to prior ways of sharing – using preexisting information sharing networks, and personal contacts, as alternatives.

• It seems to me that HSIN would be one viable option for your agencies to share border intelligence with each other and with law enforcement. How concerned are you about the IG's findings, what recommendations do you have to address these problems, and would you support a HSIN feature that would address border intelligence specifically?

Response: Once sufficient information is populated into HSIN, it would be a viable option. ICE Intelligence participates in the HSIN working group and hopes to integrate HSIN into our Field Intelligence Units in the near future.

Fusion Centers

18. We have been hearing a tremendous amount lately about state and regional intelligence fusion centers, and the law enforcement representatives we spoke to have high hopes that they will serve as a source of border intelligence for them. What presence do each of your agencies have at fusion centers, and how might they help you promote a consistent and far-reaching sharing of border intelligence information? To what extent have you explored the possibility of sending staff to state and regional intelligence fusion centers to promote border intelligence?

Response: ICE Intelligence does not currently participate in any state and local fusion centers with dedicated staff and does not anticipate having the ability to do. However, our Field

Intelligence Units do coordinate with state, local and tribal law enforcement agencies on a regular basis and participate in cooperative groups at the field level.

125

○