THE DHS INTELLIGENCE ENTERPRISE: PAST, PRESENT, AND FUTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 1, 2011

Serial No. 112–27

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE
72–237 PDF WASHINGTON : 2012

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

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
MO BROOKS, Alabama

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
VACANCY
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
PETER T. KING, New York *(Ex Officio)*

JACKIE SPEIER, California
LORETTA SANCHEZ, California
HENRY CUELLAR, Texas
BRIAN HIGGINS, New York
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ALAN CARROLL, *Subcommittee Clerk*
STEPHEN VINA, *Minority Subcommittee Director*

CONTENTS

THE DHS INTELLIGENCE ENTERPRISE: PAST, PRESENT, AND FUTURE

Wednesday, June 1, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:00 p.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Cravaack, Quayle, Speier, and Cuellar.

Mr. MEEHAN. The Homeland Security Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today to hear testimony on "The DHS Intelligence Enterprise—Its Past, Present, and Future." I want to express my deep appreciation to each and every one of you for coming forward today and your prepared testimony.

We are dealing with the realities of Congress right now and the vote schedule, so we are going to do our best to try to get in as much as we can in the form of your direct testimony. Ideally, we will be able to see what it takes with regard to what should be a quick vote procession, and then I know I will return and I suspect others. Hopefully we can ask if you would stay for any questions that may arise on this very, very important topic.

So I would like to welcome today's witnesses to discuss the growth and future of the DHS Intelligence Enterprise.

Before we begin today, I would like to take a moment to send my heartfelt condolences to one of our subcommittee members—I know that he is here today; I don't know if he is going to be able to make the hearing—Billy Long from Missouri.

Representative Long represents Joplin, Missouri. I know many of you who deal with homeland security are very well aware of the devastation by that tornado last week. I know I speak for all Members of the subcommittee when I say our thoughts and prayers are with Billy and the people in his district and the great people throughout Joplin in this difficult time.

As we all know, the Department was created in response to the 9/11 attacks and consisted in the merging of 22 different agencies. There has been great progress on solidifying our homeland, but more work remains.

I have personal experience with the DHS Intelligence Enterprise, having been sworn in as United States attorney for the Eastern

District just days after 9/11. I worked closely with many of the DHS entities on a variety of issues during my time in office.

With four terrorist attacks against our homeland since 9/11, multiple disrupted plots, and dozens of individuals indicted on terrorism charges, the threat to our homeland remains at an all-time high and is more diverse than ever. Even with the death of Osama bin Laden, we continue to face serious threats from terrorist groups, who are attempting to deploy foreigners and Americans to our homeland to conduct attacks.

In addition, today we face a significant threat from radicalized individuals in the United States, including United States citizens who have lived here their entire lives and yet are still drawn to the ideology and conduct attacks. Most notable among these include U.S. Army Major Nidal Hasan, Times Square bomber Faisal Shahzad, and the New York City Subway bomber Najibullah Zazi.

In today's 112th Congress, this subcommittee has been threat-focused. Members have learned about the terrorist threat from Yemen, Pakistan, and counterterrorism ramifications of unrest in the Middle East and North Africa. Today, I look forward to learning more about what the men and women in the Department of Homeland Security, on the front lines, are doing in this war against terrorism.

Our Customs and Border Patrol officers and Border Patrol agents are charged with preventing foreign terrorists and weapons from illegally entering the country. TSA officers are tasked with preventing terrorists from boarding our aircraft, which is the obsessive target of al-Qaeda since its inception. In fact, both myself and Ranking Member Speier have major international airports in our districts, so we know first-hand the challenges facing aviation security.

The ICE agents are responsible for ensuring individuals who remain in the country illegally are apprehended and removed. The Coast Guard is tasked with protecting ports and other critical infrastructure, including an oil refinery and other critical assets in my own area, the Delaware River in my district.

The men and women of DHS law enforcement, the boots-on-the-ground operators, rely heavily on intelligence to help them do their jobs, which includes everything from identifying suspicious individuals to tracking hundreds of thousands of shipping containers around the world. Ensuring a robust system of collaboration, information sharing, and analytic excellence across the Department Intelligence Enterprise is critical.

The DHS Intelligence Enterprise has developed and changed dramatically over the years, and we are here today to understand where we have been, where we are today, and where we should be going. My hope is that this will be an in-depth discussion of the strengths and weaknesses of the DHS Intelligence Enterprise so that Members leave here with an understanding of the positive developments, of which there have been many, and a sense of the challenges that still remain.

Through the course of today's hearing, I also hope to learn about the level of cooperation and coordination among the component intelligence elements, how law enforcement and intelligence informa-

tion is being shared and fused to create first-rate homeland security intelligence projects.

Just on a last note, Secretary Wagner, I know that you are aware that I sent a letter to Secretary Napolitano, DNI Clapper, and Attorney General Holder with various questions regarding the treasure trove of intelligence gathered in the UBL raid. I want to do everything to ensure this college library of intelligence gets to the State and locals and on the front lines of the operators of DHS. I look forward to receiving a written response to that letter. But please let me know how we can help you in any way in moving forward on that important issue.

So I look forward today to hearing from today's witnesses.

I would like now to recognize the Ranking Minority Member of the subcommittee, the gentlewoman from California, Ms. Speier, for any statement she may have.

Ms. SPEIER. Thank you, Mr. Chairman, for holding this hearing today on the Department of Homeland Security Intelligence Enterprise. I look forward to working with you to continue the subcommittee's long history of oversight over the critical mission to coordinate the intelligence and information-sharing activities of the Department.

This enterprise brings together the intelligence capabilities of the entire Department, from headquarters to the Office of Intelligence and Analysis to analysts in the field working on various components. We are here to examine the progress that the Intelligence Enterprise has made since its creation and to identify areas needing improvement.

Although we have come a long way to shore up intelligence gaps within the Department, several incidents over the past few years have revealed vulnerabilities and driven home the importance of maturing the Intelligence Enterprise. Does DHS have the funding it needs to continue building its intelligence architecture? Does it have the buy-in from the intelligence community and senior leadership across the Government?

The chief intelligence officer of the Department, Under Secretary Caryn Wagner, leads the DHS Intelligence Enterprise. I am pleased that she is with us today to discuss how the enterprise is maturing.

Some challenges the chief intelligence officer and the Intelligence Enterprise face appear deceptively simple, like developing a common lexicon for all intelligence professionals to use Department-wide.

Once you do that, please share that with us, because I, for one, continue to be challenged by many of the acronyms.

Other challenges seem more complex, like bringing together components with distinct and sometimes competing priorities to serve the Department's large customer base.

To what extent is intelligence analysis and information sharing a priority in each component? How is the Department reducing duplication and redundancy of effort within DHS and between DHS and other elements the intelligence community? How much money should we be devoting to this, and can be it done better and more efficiently?

I am looking forward to hearing from all of the intelligence chiefs assembled here today to get answers to these questions and to see how all of you work together in this constrained budget environment to address the many threats to our homeland security.

Documents combed through in the aftermath of the bin Laden operation have underscored how critically important it is for all the components, even with their unique missions, to work together. Letters attributed to bin Laden and his lieutenants have identified targets in major cities from coast to coast, and we know al-Qaeda was looking at our rail, aviation, and energy sectors.

Do we have the right policies in place to permit the sharing of sensitive information while also protecting the privacy and civil liberties of U.S. citizens? Do we have the right technologies to allow the components to adequately communicate with their partners within DHS and the intelligence community, as well as State, local, and Tribal partners and the private sector?

After this hearing, we expect to have a much better picture of the accomplishments and current capabilities of the DHS Intelligence Enterprise and, more importantly, how we can help you address your critical needs and meet your goals in the future.

I would like to thank all the witnesses for being here today. While many of your accomplishments are designed to go unnoticed, know we appreciate your tireless efforts to keep America secure.

I yield back.

Mr. MEEHAN. I thank you, Ms. Speier.

Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have five distinguished witnesses before us today on this very, very important topic. So let me remind the witnesses that their entire written statement will appear in the record. I hope you will allow us to understand the most critical points of your testimony and do your best to try to work with us on the time deadlines, as well.

Today's first witness is Under Secretary and Chief Intelligence Officer Caryn Wagner from the Department of Homeland Security's Office of Intelligence and Analysis.

Under Secretary and CINT, we call it, Wagner—that is—how do you—it is CINT? Okay. I just need to make sure—was confirmed in her present post by the Senate in February 2010.

Before that, she led a storied and distinguished career as a public servant, first as the signals intelligence and electronic warfare officer in the United States Army and, later, on the staffs of the House Permanent Select Committee on Intelligence, at the Defense Intelligence Agency, and the Director of National Intelligence.

Under Secretary Wagner also holds a Bachelor of Arts degree in English and history from the College of William and Mary and a Master of Science degree in Systems Management from the University of Southern California.

Under Secretary Wagner, you are now recognized to summarize your testimony.

STATEMENT OF CARYN A. WAGNER, UNDER SECRETARY, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

Ms. WAGNER. Thank you, Mr. Chairman.

Chairman Meehan, Ranking Member Speier, and distinguished Members of the committee, I am honored to appear before you today to discuss the DHS Intelligence Enterprise in the company of some of my key colleagues from the Homeland Security Intelligence Council. I view this hearing as a valuable opportunity for us all to update you on how we increasingly operate as a partnership to provide the best possible intelligence support to the Department, the intelligence community, and our many and varied external customers.

Let me start with a few definitions since this can get confusing. I think you already have it, but the DHS Intelligence Enterprise consists of all elements of the Department that are engaged in directing, collecting, reporting, processing, analyzing, and disseminating intelligence and information in support of the Department's many missions, as outlined in the Quadrennial Homeland Security Review.

The Homeland Security Intelligence Council, or HSIC, acronym No. 2, is basically the board of directors of the Intelligence Enterprise. It is comprised of the heads of the intelligence elements of the components and other key members of the Intelligence Enterprise, such as the National Protection and Programs Directorate, which is responsible for infrastructure protection and cybersecurity.

I chair the HSIC in my role as the chief intelligence officer, or CINT, for the Department, a role that was created in 2005 and formalized in legislation in the implementing recommendations of the 9/11 Commission Act of 2007. As the CINT and as chair of the HSIC, I am responsible for overseeing the Intelligence Enterprise and performing a few key functions:

First, reviewing the intelligence budgets of the components to ensure that they are adequate and not duplicative and advocating for component intelligence needs within the larger Department budget bill; second, identifying areas where the enterprise would benefit from standardized policies, practices, and procedures, and working with the HSIC members to develop and implement them; and, third, leveraging the expertise of the HSIC members to collectively address crosscutting intelligence topics and issues in support of Department missions.

To speak very briefly to each of these functions, I recently received the fiscal year 2013 budget briefings from the key components, and I am working on crafting my response and my input to the Secretary for the Department's resource allocation plan. Because I wear another hat—in addition to Under Secretary for Intelligence and CINT, I am also the Department's information-sharing executive—I have the opportunity to weigh in on both the information-sharing and intelligence portfolios as part of the budget build. As you know, those two portfolios are closely related.

The review process allows me to identify and act on capability gaps. As an example, in the fiscal year 2012 budget request that is currently on the Hill, I have put an initiative in there to provide additional personnel for U.S. Citizenship and Immigration Serv-

ices, a member of the HSIC who is not with us today, to assist them in reviewing the voluminous holdings of immigration data in response to a growing number of requests from law enforcement and National security queries.

As for the standardized policies and processes, I want to highlight just a couple of those. First is our collective effort to standardize and improve our Homeland Security Intelligence Reports, or HIRs. After much discussion and examination of the varying processes across the enterprise, we developed a phased approach for transitioning to an enterprise process that will standardize thresholds, time lines, and training, and streamline the review and clearance process while ensuring compliance with all existing laws and policies.

Improving HIR production across the board is important because HIRs are our primary method for getting the information that we gather in the course of performing our many missions to our partners in the law enforcement and intelligence communities, who can then use them in support of their own missions. You may hear more about HIR reporting from Mr. Chaparro because ICE is an enterprise best practice in terms of HIR reporting.

We are also using the HSIC to develop a Department-wide counterintelligence strategy—something that, unfortunately, we were lacking in the past. We have created a counterintelligence working group under the HSIC which is made up of the Department's CI representatives. In some cases, these representatives are the first ever in their components. So this group is going to report back to the HSIC on the strategy and develop plans for phased implementation of a new CI strategy across the Department.

Another area where we are developing an enterprise approach is production management. As Congresswoman Speier asked, we are frequently asked about duplication and redundancy in the Department. It is, in fact, hard to have too much duplication because the missions of the various components are so distinct. But in the area particularly of CT threat, we definitely do need to coordinate and deconflict our efforts.

So we produced our first program of analysis in 2010, which laid out our 17 key intelligence questions and the planned analysis and production in response to those questions. The first one was drafted by I&A and coordinated with the components, but it was largely an I&A document. The second one that we are kicking off now is intended to be a true enterprise document, developed collaboratively from the beginning, and articulating who is going to produce what on the full range of Department missions and threats to homeland security.

Finally, a couple of examples in the area of collaborative focus on specific intelligence issues. Without going into classified details, we have put teams together on an ad-hoc basis to focus on things like spikes in the apprehension of specific groups along the border arriving without documentation, to try to figure out why and how they have arrived at the border and what their origins and motivations are. We had a very successful working group that focused on capabilities and gaps in discovering tunnels under the Southwest border. We have also put together a group to red team terrorist tactics, in cooperation with our interagency partners, as a way of en-

suring that we and our State and local partners were planning for and implementing the most effective protective measures.

The bottom line is that the HSIC and the DHS Intelligence Enterprise are force multipliers. We all do a better job when we work together, and we are getting better at working together. We also take it to the next level and work closely with our interagency partners, particularly at NCTC and FBI.

Finally, I would just say, if you forgive my analogy, homeland security is a team sport, and I am pleased to be here with my colleagues and teammates to answer your questions.

[The statement of Ms. Wagner follows:]

PREPARED STATEMENT OF CARYN A. WAGNER

JUNE 1, 2011

Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss my role as the Department of Homeland Security (DHS) Chief Intelligence Officer (CINT) and the collaborative efforts of the DHS Intelligence Enterprise.

DHS is a complex organization with a broad, diverse set of missions. Intelligence is an important supporting factor in most, if not all, of these missions. Departmental intelligence programs, projects, activities, and personnel—including the intelligence elements of our seven key operational components, as well as the Office of Intelligence and Analysis (I&A)—make up the DHS Intelligence Enterprise (IE). I&A is charged with ensuring that intelligence from the DHS IE is analyzed, fused, and coordinated to support the full range of DHS missions and functions, as well as the Department's external partners. The operational components, most of which predate the creation of the Department, have intelligence elements that provide support tailored to their specialized functions and contribute information and expertise in support of the Department's broader mission set.

The Homeland Security Act of 2002 made the then-Assistant Secretary for Information Analysis responsible for establishing intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department. As part of the Department's 2005 Second Stage Review, the Assistant Secretary was designated as the DHS Chief Intelligence Officer (CINT) to accomplish that mandate. The Assistant Secretary was subsequently elevated to Under Secretary for Intelligence and Analysis (U/SIA) by the Implementing Recommendations of the 9/11 Commission Act of 2007, which also strengthened the influence of the CINT role.

The CINT is responsible for leading and managing the activities of the DHS IE, and furthering a unified, coordinated, and integrated intelligence program for the Department. One of the CINT's first leadership actions was to develop Management Directive (MD) 8110, which delineates the CINT's authorities to oversee, define, and evaluate the Department's intelligence activities and services. As a result of the Implementing Recommendations of the 9/11 Commission Act of 2007, the heads of DHS intelligence components are required to advise and coordinate with the CINT to support the mission of the Department.

The CINT provides planning and programmatic guidance to the IE, conducts programmatic reviews, and provides formal input to the Secretary regarding intelligence-related budget requests from the Components. The CINT's planning and programmatic guidance focuses Departmental resources and efforts toward priority intelligence and information-sharing needs to expand enterprise capabilities, develop capacity, and improve intelligence support to the DHS IE. In 2012, the CINT focus areas are training, secure connectivity, and collaboration across the IE.

To ensure the DHS IE works together to support the DHS mission, the CINT regularly engages with the Components through weekly secure video teleconferences (SVTCs) to coordinate on threat reporting and planned production. Perhaps the most important and successful integration mechanism the CINT employs, however, is the Homeland Security Intelligence Council (HSIC).

The HSIC was created in 2005 to serve as the DHS IE's decision-making and implementation oversight body. The HSIC is composed of the heads of DHS's intelligence components. HSIC members provide advice and assistance; coordinate the implementation of programs; and report to the CINT on intelligence matters related to: (a) Strategy and policy, (b) leadership and coordination, (c) training and career

development, (d) budget, management, and implementation, and (e) evaluation and feedback. The HSIC is empowered to establish subordinate boards and working groups to accomplish its oversight and program coordination responsibilities.

The HSIC meets monthly to discuss current issues, receive strategic-level information briefings, and provide guidance. This forum provides a regular opportunity for HSIC members to inform and solicit feedback from their counterparts on new initiatives and to provide updates on existing programs. Subordinate working groups provide periodic updates on their progress and accomplishments.

HSIC working groups are established as needed to address the dynamic requirements of the DHS IE. Chaired by the members of the DHS IE, the working groups are charged with developing action plans based on guidance from HSIC. Working groups can be short- or long-term, and focus on systemic and programmatic issues or on substantive intelligence topics. For example, the HSIC helped develop specific questions for U.S. Customs and Border Protection (CBP) officers to ask certain types of travelers or border crossers, and to identify intelligence and technology gaps to support counter-tunnel investigations and operations. In addition to coordinating the monthly HSIC meeting and following up on HSIC working group programs and activities, the CINT staff collects input from the DHS IE for compilation into two reference tools, the Intelligence Enterprise Catalog (IEC) and the Homeland Security Intelligence Priorities Framework (HSIPF).

The IEC contains information on DHS IE assets, capabilities, and resources around the country and the globe. While not yet comprehensive, it serves as a useful reference point for the CINT and DHS IE when making decisions related to resource planning and current operations. The HSIPF aggregates the DHS IE's intelligence priorities for the CINT to help the HSIC make informed IE-wide planning decisions. It serves much the same purpose for the DHS IE as the National Intelligence Priorities Framework (NIPF) does for the National intelligence community. We continually refine the HSIPF to ensure it accurately captures DHS IE priorities and aligns most effectively with the NIPF.

As post-9/11 operational necessity drove DHS' formation from disparate legacy agencies, complex new departmental responsibilities obliged us to work together in enterprise fashion and forge a collaborative OneDHS intelligence culture. The DHS IE leaders represented on the HSIC have contributed their operational component experience and perspective to shape innovative intelligence methods in support of Departmental policy, programs, and operational needs. The following initiatives and programs are outgrowths of the cooperative, collegial spirit of the DHS IE as embodied in the HSIC.

DHS TERRORISM TASK FORCE (DTTF)

The acting CINT stood up the DHS Terrorism Task Force (DTTF) to bring together representatives from across the DHS IE to rapidly disseminate information, garner feedback and/or solicit input to strategic-level issues.

The DTTF, which is led by U.S. Immigration and Customs Enforcement (ICE), ensures that all information resident in each of the Components' unique systems is identified and shared within the Department and the IC. The DTTF hosts a weekly SVTC to discuss current intelligence and threat updates, ensuring that the DHS IE is operating in unity to achieve the Department's mission.

The DHS Watchlisting Cell (WLC) was established within I&A in October 2010 to serve as the focal point for Department-wide watchlist nominations to the National Counterterrorism Center and the Terrorist Screening Database (TSDB). The WLC reached full operational capability on January 31, 2011. The WLC was placed in the DTTF to leverage established channels of communication with the Components and because of the time-sensitive aspect of watchlisting.

The WLC is an improved construct to fulfill requirements directed by Homeland Security Presidential Directive 6, which states that every department or agency in the Executive branch must have a mechanism in place to nominate for watchlisting all identifying and/or derogatory information on known or suspected terrorists in its possession. The WLC leverages intelligence and operations elements throughout DHS to ensure that all nominations are comprehensive; transmitted in a timely, coordinated, and standardized manner; and meet established criteria for submission to NCTC.

HOMELAND INTELLIGENCE REPORTING

In 2010, the HSIC established the Homeland Security Intelligence Report Working Group (HIRWG) to evaluate and optimize the production, review, and publication process of the Department's intelligence reports. Until the establishment of the working group, there was no DHS-wide policy for intelligence reports addressing

component-specific limitations, statutory obligations, mission-specific needs, or production prioritization methods. DHS IE components noted that reporting thresholds were being applied inconsistently or subjectively, often hampering reporting time lines, production rates, and collaborative efforts. Additionally, there were no standardized or written processes for the writing, production, submission, or clearance of intelligence reports. Through a phased approach, the HIR–WG completed a comprehensive review of the existing HIR program, processes, and policies gathered from existing documentation, working group meetings, interviews, and surveys. Additionally, the HIR–WG examined the efficiency and effectiveness of the current operating models, the review and clearance process, reporting thresholds and definitions. Subsequent findings have led to the formation of 13 recommendations designed to establish training/certification, dissemination, auditing, and reporting threshold standards across the DHS IE. These improvements championed by the HSIC help to guarantee that our internal and external stakeholders receive key threat information in a timely manner, while ensuring compliance with all applicable laws and policies. Intelligence reports are our primary vehicle for communicating information collected by the DHS IE to the broader intelligence community for incorporation into all-source products.

CTAB AND NTAS

The Counterterrorism Advisory Board (CTAB) is the Department's mechanism for coordinating and integrating all aspects—intelligence, operations, and policy—of its counterterrorism mission, which spans operational components and headquarters elements. The Secretary appoints a Coordinator for Counterterrorism to chair the CTAB—currently the Under Secretary for the National Protection and Programs Directorate—while the Under Secretary for Intelligence and Analysis/CINT and Assistant Secretary for Policy are vice-chairs. The CTAB is also responsible for recommending to the Secretary that an alert be issued under the National Terrorism Advisory System (NTAS). The CINT, working with the DHS IE, is responsible for monitoring threats to the homeland to determine if it reaches a level of specificity that might merit convening the CTAB to discuss issuing such an alert. When that happens, the CINT will consult both internally and externally to the Department before recommending that the CTAB be convened. The HSIC will serve as the mechanism for ensuring that key components are fully involved in the threat recommendation to the CTAB.

COUNTERINTELLIGENCE WORKING GROUP

The HSIC Subcommittee on Counterintelligence (the CI Working Group or CI–WG) supports the development of CI policies and procedures across the Department. Component representatives meet monthly to identify those areas requiring immediate attention and to establish necessary DHS-wide CI policy, instructions, and procedures. By integrating the analytical and operational elements of DHS's CI Program, the CI–WG postures the Department to effectively identify, understand, and counter foreign intelligence activities.

The Secretary has directed I&A to lead the Department's counterintelligence program. The CIWG is working in concert with the Office of the Director of National Intelligence to establish a CI-focused Insider Threat Program, which includes an IT-enabled audit/monitoring capability, and is standardizing CI awareness training. The CI–WG has also developed a CI Program Directive, codifying the Secretary's decision to consolidate the Department's CI effort, and drafted a CI Implementing Instruction and CI Security Classification Guide. These documents will further help integrate Component efforts and execute an effective CI program across the Department.

INTELLIGENCE CAREER FORCE MANAGEMENT BOARD

The Intelligence Career Force Management Board (ICFMB) is comprised of both human capital and professional development personnel from across the DHS IE. Charged with providing strategic direction and guidance in managing the DHS intelligence workforce, the board successfully produced a plan of action to address the Department's high intelligence workforce turnover rates, uneven training, and lack of career development tools. The plan of action includes 11 initiatives aimed at re-energizing and refocusing the workforce through the establishment of cross-component career paths, common hiring standards, integrated training and training resources for common functions, and shared career development tools. These initiatives continue to support and move the DHS IE closer to its vision of a unified, diverse, agile, responsive, trained, and mission-ready DHS IE workforce, capable of supporting the many missions and operations of the Department, as well as the De-

partment's State, local, Tribal, territorial, private sector, and intelligence community customers.

Currently, the Board is working to complete a DHS IE curriculum assessment, which will provide a 3-year outlook on course offerings, training requirements, and required resources for DHS IE leadership planning and budgeting purposes. The Board is also developing a baseline GS–0132 job description and a standard, anonymous exit interview that will give managers across the DHS IE greater insight into how, as an enterprise, we can strengthen our workforce.

THE FUTURE OF THE DHS IE

The next frontier for the DHS IE is to begin to undertake enterprise-wide planning. This year will mark the first time the entire DHS IE will collaborate to produce a single Program of Analysis, which will help to ensure that, with respect to analytical efforts, redundancies are avoided, opportunities for collaboration are identified from the outset, and any overlap is carefully considered in light of the different approaches each Component may choose to take on a specific issue. The goal is to ensure that the DHS IE expends its intelligence resources in an effective and efficient manner and that all mission requirements are adequately covered. Also, as recommended by CBP, we are currently exploring the feasibility of a Departmental intelligence doctrine.

The development and acquisition of new intelligence tools and systems is an area for additional collaboration. We are making great strides retrofitting existing databases and networks to interoperate across the DHS IE; the next step is to more closely coordinate our planning for new systems to ensure they are built from the ground up to be more collaborative.

CONCLUSION

Since the establishment of the DHS CINT, Departmental intelligence integration and efficiency has continuously improved, providing increasingly unified intelligence support to the DHS mission. Key to these improvements has been the HSIC, which serves as the main unifying and integrating body of the DHS IE. Using this forum, senior intelligence leaders from across the Department have worked to educate each other on the individual intelligence component missions and functions to better identify areas of improvement and opportunities for cooperation. The HSIC allows the DHS IE to synergize our missions, especially in the areas of counterterrorism and border security. Working with our partners in the intelligence community, the CINT leads and manages the activities of the DHS IE, and furthers a unified, coordinated, and integrated intelligence program for the Department. It is through the collaborative efforts of the DHS IE that we leverage our collective strengths and proactively provide intelligence that supports the Department's mission to secure the homeland. This partnership is a valuable asset that we must vigilantly cultivate and promote to ensure its success.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions you may have at this time.

Mr. MEEHAN. Thank you, Under Secretary Wagner, for your testimony.

Our next witness will be Rear Admiral Thomas Atkin of the United States Coast Guard.

The assistant commandant for intelligence and criminal investigations, Rear Admiral Atkin previously served as assistant commandant for operational policy and planning. He has also held the post of acting assistant commandant for marine safety, security, and stewardship.

As an admiral in the Coast Guard, he additionally served as special assistant to the President and senior director for transborder security on the National Security Staff and first commander of the U.S. Coast Guard Deployable Operations Group, following a number of operational assignments throughout the United States.

He is a graduate of the United States Coast Guard Academy with a Bachelor of Science degree in mathematical sciences and also holds a Master of Science in management science from the University of Miami.

I also understand you may have a little interest in how the Coast Guard lacrosse program is doing this year.

Well, Rear Admiral Atkin, you are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF REAR ADMIRAL THOMAS ATKIN, ASSISTANT COMMANDANT FOR INTELLIGENCE AND CRIMINAL INVESTIGATION, U.S. COAST GUARD

Admiral ATKIN. Thank you, sir.

Good afternoon, Chairman Meehan, Ranking Member Speier, and distinguished Members of the committee. Thank you for the opportunity to provide testimony on the Coast Guard Intelligence Enterprise and how we work closely with our DHS Homeland Security Intelligence Council partners, the DHS Intelligence and Analysis staff, the Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration.

As you said already, I am Rear Admiral Tom Atkin. I am the assistant commandant for intelligence and criminal investigations.

The Coast Guard is the lead U.S. agency for maritime homeland security. We are the largest maritime law enforcement agency in the country, and we are an intelligence community member. We are on watch 24 hours a day. No other department or agency has the authorities or jurisdiction like the Coast Guard that allows us to touch the maritime domain in every area.

For more than 220 years, the Coast Guard has safeguarded the Nation's maritime interests on our rivers, in our ports, along the coastal regions, on the high seas, and around the world. We protect those on the sea, we protect America from threats delivered by the sea, and we protect the sea itself.

The Coast Guard's persistent presence in the maritime domain, due to our diverse mission sets and broad legal authorities, allows us to fill a unique niche within the intelligence community. As a member of the Armed Forces, the Coast Guard is at the intersection between homeland security and National defense. As a Federal law enforcement agency and a National intelligence community member, the Coast Guard is also positioned as a bridge between these two important groups.

Because of our unique access, our emphasis, and our expertise in the maritime domain, an area where other U.S. Government agencies are typically not present, we collect and report intelligence that not only supports our missions but supports the National security objectives.

In August 2010, the motor vessel Sunsea, a 188-foot stateless bulk cargo carrier, crossed the Pacific carrying 492 illegal Sri Lankan migrants en route to Canada. As the vessel transited the Pacific, the Coast Guard Intelligence Enterprise played a key role by enabling Coast Guard operational and tactical commanders to closely monitor the case, prepare contingency plans, and effectively position response forces in the event the ship attempted to reach a port in the United States or conditions on board deteriorated and an at-sea interception was required.

This vessel was of particular concern because the smugglers included members of the terrorist group Tamil Tigers.

Working with our international, Federal, and State partners, including the Department of Defense, we monitored the vessel's movements, especially as it approached U.S. territory. We leveraged and integrated capabilities with our National intelligence and law enforcement counterparts. We analyzed similar past cases to make boarding teams aware of the conditions and the responses they might encounter if they were given the order to interdict the vessel. We assessed the potential threat posed by the crew and passengers. At any time, this vessel could have turned into a major search-and-rescue case or a significant interdiction event.

The vessel was ultimately intercepted by Canadian forces off the coast of British Columbia. We provided effective, timely, accurate, and usable intelligence to ensure our forces were well-informed and ready to take action. This example highlights our unique maritime expertise, allowing us to lead and assist our law enforcement National intelligence and international partners to identify a potential threat and work toward a positive solution to protect our Nation.

To support homeland security, the Coast Guard screens ships, crews, and passengers for all vessels required to submit a 96-hour advance notice of arrivals to a U.S. port. In 2010, we screened more than 257,000 ships and 71.2 million people.

We work closely with Customs and Border Protection to utilize their automated targeting system, which enables real-time database checks and allows us to more easily identify suspected entities engaged in nefarious activities within the maritime domain. Our collaboration with CBP has been so successful that, earlier this year, we moved most of our screening effort to the National Targeting Center to better integrate our efforts with interagency personnel performing similar duties.

Following screening, any informations on persons discovered with possible terrorism links are shared with other DHS components, the Department of Justice, and the intelligence community.

I have only scratched the surface describing the broad capabilities and diverse relationships that define the Coast Guard Intelligence Enterprise. In our intelligence pursuits, the Coast Guard draws on our long and rich maritime history and experiences that result from our unique status as an armed service, a law enforcement agency, a Federal regulator, and a National intelligence community member.

Each of the components that form the DHS Intelligence Enterprise brings something different to the table. We have made great strides in our collaboration through the Homeland Security Intelligence Council under the leadership of Secretary Wagner. We all understand that we are strongest when we stand together. We have worked to make significant progress in aligning our capabilities toward a common purpose: Defending the safety and security of the American people.

Thank you for inviting me here to discuss the Coast Guard Intelligence Enterprise, DHS, and the HSIC. I look forward to your questions.

Mr. MEEHAN. Thank you, Rear Admiral Atkin, for your testimony.

Our next witness is Mr. Daniel Johnson, the assistant administrator for intelligence at the Transportation Safety Administration.

Mr. Johnson began as assistant administrator for intelligence earlier this year and, prior to that, served in the United States Air Force. With 26 years' experience at the Air Force Intelligence, Surveillance, and Reconnaissance Agency, most recently as wing and mission commander, he stands as leader on National and theater ISR operations and is a seasoned staff officer.

He also worked at the Pentagon on the Joint Chiefs of Staff as deputy director for joint requirements, oversight council, and targets.

That must be quite a business card, when you have something like that.

In that role, he provided intelligence support to the Chairman of the Joint Chiefs of Staff and Secretary of Defense.

Mr. Johnson graduated from the Air War College at Maxwell Air Force Base in Alabama with a Master of Strategic Studies, received a Master of Public Administration from the University of Oklahoma, and a Bachelor's degree in public administration and policy from Eastern Connecticut State University.

Mr. Johnson, you are now recognized to summarize your testimony. Thank you.

STATEMENT OF DANIEL JOHNSON, ASSISTANT ADMINISTRATOR FOR INTELLIGENCE, U.S. TRANSPORTATION SECURITY ADMINISTRATION

Mr. JOHNSON. Thank you, sir.

Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee, thank you for this opportunity to be before you today to discuss the role of the Transportation Security Administration within the larger scope of the DHS Intelligence Enterprise.

Since coming on board this January, I have had the opportunity and privilege to work closely with Under Secretary Wagner and my colleagues at the United States Coast Guard, Customs and Border Protection, and Immigration and Customs Enforcement, improving our internal and external collaboration and information sharing.

As the assistant administrator for intelligence for TSA, I oversee three primary mission threads: Indications and warning; predictive analysis; and incident response. In accordance with the transportation security authorities, the TSA Office of Intelligence can receive, assess, analyze, and disseminate intelligence information for transportation security purposes that helps protect the 1.7 million passengers per day that use civil aviation, the 47,000 miles of highways, the 147 million maritime ferry passengers per year, the 29 million passengers per day that use mass transit, the 1.6 million tons per year traveled by freight rail, and then, last, over 2.5 million miles of natural gas and hazardous liquid pipelines.

In my role as the head of intel for TSA, I am often asked what keeps me up at night. The answer is the global threats with a regional focus, coming primarily from al-Qaeda and its affiliate groups, who continue to pose a serious threat to transportation security.

Al-Qaeda in the Arabian Peninsula, or AQAP, continues to threaten U.S. interests abroad and in the homeland. In particular, the group is fixated on aviation as a means to inspire fear and eco-

nomically cripple the United States and Western interests. Through four editions of *Inspire* magazine, AQAP has referenced the October 2010 cargo plot, wrote about Abdulmutallab's heroism and sacrifice as the Christmas day bomber, and even featured an article of how to make a bomb in the kitchen.

Additionally, in light of the successful Osama bin Laden roll-up, we continue to track seized material being exploited from his compound in Abbottabad and monitor existing transportation threat streams from al-Qaeda and its affiliates who may seek to accelerate existing plots, prove their mettle, and/or legitimize their causes.

TSA stakeholders include the passengers that are out there every day, field operations, and key critical infrastructure security owners and operators. Our mission is to provide them with the highest-confidence threat reporting on the various modes of transportation. In order to do this, we must work closely with the Homeland Security Intelligence Council to form an internal and external bench that enables collaboration and transparency for all our reporting.

Over the past 6 months, I have reached out to the HSIC team, along with the intel and law enforcement communities, to internally collaborate on various threat assessments, along with reaching out externally and leveraging existing analysis being done by partners at the National Counterterrorism Center, the sector government coordination councils, fusion centers, private trade associations, and the National Joint Terrorism Task Force.

Additionally, under the leadership of Under Secretary Wagner, we have worked closely with DHS I&A on professional development and training. Within my office, we have created a development path that ranges from new hires to seasoned analysts that enables a continuous career progression. Similarly, we are on the ground floor of standing up our counterintelligence section. This will enable us to work closely with DHS on CI policies, instructions, and procedures.

I look forward to continue to work with our intelligence partners to evolve the Intelligence Enterprise that not only shares data but collaborates among headquarters and components to enable higher confidence reporting to our stakeholders in the field. Within TSA, once again, there are passengers, our field operations, key infrastructure owners and operators.

Thank you for this opportunity to address the subcommittee, and I am happy to answer any questions.

Mr. MEEHAN. Thank you, Mr. Johnson. I am grateful for your testimony.

Our next witness is James Chaparro, who is the assistant director of intelligence for the United States Immigration and Customs Enforcement.

Mr. Chaparro's public service includes 20 years' experience, most recently as Deputy Under Secretary for Operations in the Office of Intelligence and Analysis. Mr. Chaparro also has served as the director of the Human Smuggling and Trafficking Center, special agent in charge of the ICE Denver field office, and held the position of interim director of immigration interior enforcement for ICE, upon the creation of DHS.

Before that time, Mr. Chaparro worked with the Immigration and Naturalization Service as deputy assistant commissioner for

investigations, director of anti-smuggling, and assistant district director for investigations and special agent.

Mr. Chaparro also holds a Bachelor of Arts degree in political science from California State University at Long Beach.

Mr. Chaparro, you are now recognized to summarize your testimony. Thank you.

STATEMENT OF JAMES CHAPARRO, ASSISTANT DIRECTOR FOR INTELLIGENCE, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

Mr. CHAPARRO. Thank you.

Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee, on behalf of Secretary Napolitano and Director Morton, I would like to thank you for the opportunity to discuss ICE's efforts in supporting the DHS Intelligence Enterprise. I hope to offer the subcommittee somewhat of a unique perspective because I have had the privilege—actually, the honor—of serving in leadership roles in both I&A and ICE, one of the larger components of DHS.

ICE is uniquely positioned to advance the DHS mission. We do this through intelligence production, through law enforcement investigations focusing on terrorism, human smuggling, human trafficking, financial crimes, trade fraud, weapons proliferation, drug smuggling, illegal tunneling, and other illicit activities, and also through the outstanding work done in our Office of Enforcement and Removal Operations.

As the DHS component with the most expansive investigative authorities, ICE has people assigned in over 200 U.S. cities and in 70 offices in 48 countries around the world. ICE is both a vital contributor to the DHS Intelligence Enterprise and a voracious consumer of its products and services.

The ICE intelligence program is structured along three major lines. We have the headquarters office of intelligence; we have field-based intelligence teams that support our field offices directly; and then we also have intelligence liaisons, who we have strategically placed with interagency partners around the law enforcement and intelligence community. Together, this combined approach really allows us to have people who will help serve and make sure that we have the right information going to the right people at the right time.

In her opening statement, Under Secretary Wagner provided an expansive overview of the DHS Intelligence Enterprise. I would like to focus on how collaboration within that enterprise is progressing from the ICE perspective.

The Homeland Security Intelligence Council, or HSIC, as previously mentioned by my counterparts, in my opinion, serves as an excellent venue to really coordinate on large strategic initiatives as well as making sure that we are working together on common threats.

For example, ICE has leveraged the HSIC to advance important initiatives in the coordination of counter-tunnel investigations and operations. We have worked on our collaborative capabilities to determine and identify illicit smuggling pathways bringing people and goods to the United States illegally. Through our participation

in the HSIC, ICE facilitates a bi-directional information flow between our field components, between our headquarters elements, and between our external partners, both domestic and overseas.

ICE plays a critical role in support of the National intelligence community, as well. ICE is the leading producer of DHS Homeland Intelligence Reports, or HIRs, which provide valuable intelligence reporting from ICE operations. We disseminate those externally to our partners. So far in fiscal year 2011, ICE has accounted for about 58 percent of the Department's production of HIRs.

Perhaps more importantly, however, is the fact that 54 percent of those HIRs were evaluated by the customers as either "high value" or "major significance," which is very, very substantial in the intelligence world. The success rate of our reporting of HIRs I think is a commitment not only to the people producing them, but it is also a commitment to show that ICE is really committed to making sure that we are putting out our most valuable information so others can use it to strengthen National security efforts.

ICE also has the leadership role in the DHS Threat Task Force, or DTTF. This is an interagency DHS entity that sits in the Office of Intelligence and Analysis that works to ensure that DHS leadership maintains situational awareness on a continually and rapidly evolving terrorist threat stream picture. We do this through the enabling of counterterrorism threat coordination and by producing sensitive intelligence assessments. ICE's participation in the DTTF also helps serve our needs at ICE because we are able to very rapidly glean information held by other DHS intelligence components, other DHS components, as well as the National intelligence community, and share that with our special agents on the ground who are working in JTTFs around the country to combat terrorist threats.

ICE also plays an important role in the DHS information sharing with our Federal, State, local, and international law enforcement partners. We do this primarily through the Law Enforcement Information Sharing Initiative, or LEISI. Since its inception, the LEISI has entered into eight significant law enforcement information-sharing agreements on behalf of the Department of Homeland Security.

This includes an agreement recently signed with the International Justice and Public Safety Network. This is an important point because this will enable us to share information with 785,000 State and local law enforcement officers around the country. This is something that I am very proud of, and I think it is an initiative that will really help the boots on the ground, not just in the Federal community but also in the State and local community.

The importance of integrating intelligence into our investigations and operations cannot be overstated. Since 2006, DHS has leveraged the Border Enforcement and Security Task Forces, or BEST teams, which combine Federal, State, Tribal, and local and foreign law enforcement intelligence and law enforcement resources to synchronize efforts to combat existing threats. ICE intelligence provides strategic and operational support to the BEST teams, and we are working with I&A to increase the overall support addressing threats to the Southwest border, the Northern borders, as well as the maritime borders.

ICE's Office of Intelligence also serves an important role in coordinating oversight of ICE's intelligence functions, and we serve as the primary conduit for the DHS Intelligence Enterprise from ICE and also from ICE operations into the intelligence community.

In a rapidly changing threat environment, however, we cannot be complacent with our successes. We are moving forward by increasing our strategic intelligence production——

Mr. MEEHAN. Mr. Chaparro, I am really—I actually am very focused on your testimony, and I appreciate it. But I am going to ask if what you can do is just sum it up very, very quickly so I can get to Ms. Mitchell. We will try to get to Ms. Mitchell, if she can do 5 minutes. Then that will allow us to conclude this part. We will go do our votes and then get back as quickly as we can.

Can you give me your concluding sense on this?

Mr. CHAPARRO. Certainly, Mr. Chairman.

In sum, ICE is a valuable partner with the DHS Intelligence Enterprise. We take great advantage of the services that are provided by our partners. We utilize the information in our day-to-day operations.

I look forward to answering any questions that committee Members may have for me. Thank you.

Mr. MEEHAN. Thank you, Mr. Chaparro.

We would like to identify our final witness, Ms. Susan Mitchell, the deputy assistant commissioner for the Office of Intelligence and Operations Coordination at Customs and Border Protection.

I hope you will allow me the privilege of not sharing the same introduction as I did before, in the interest of time, but allow you to get right to your testimony.

STATEMENT OF SUSAN MITCHELL, DEPUTY ASSISTANT COMMISSIONER, OFFICE OF INTELLIGENCE AND OPERATIONS COORDINATION, U.S. CUSTOMS AND BORDER PROTECTION

Ms. MITCHELL. Thank you.

Good afternoon, Chairman Meehan, Ranking Member Speier, and distinguished Members of the subcommittee. It is a privilege and honor to appear before you with my colleagues and to discuss CBP, or Customs and Border Protection's intelligence efforts and evolution.

First, I would like to just highlight that, with almost 60,000 employees, CBP makes up the largest law enforcement organization in the Nation and has been given the responsibility to protect the United States from terrorists, weapons of mass effect, drug and human smugglers, agricultural disease, among other threats, all while fostering our Nation's economic security and competitiveness through facilitating lawful international trade and travel.

CBP provides a layered defense along nearly 7,000 miles of land border and along 95,000 miles of shoreline in partnership with the U.S. Coast Guard.

At the core of CBP's mission is to detect and deter the movement of foreign terrorists and terror-related materials across the U.S. border. I will give you two quick examples that highlight CBP's efforts on this front.

First, on December 14, 1999, CBP officers at Port Angeles, Washington, prevented the entry into the United States of the so-called

millennium bomber, an Algerian al-Qaeda member named Ahmed Ressam, who was transporting explosive materials and plotting an attack on Los Angeles International Airport on New Year's Eve and was identified by behavioral analysis detection and physical examination of the vehicle he was driving.

More recently, as you mentioned earlier, on May 3, 2010, CBP's National Targeting Center worked with CBP officers at JFK Airport to apprehend the Times Square bomber, Faisal Shahzad, as he was attempting to flee the United States on a flight to the Middle East.

Months earlier—and that really is the key—months earlier, he had hit on several of our targeting rolls for Pakistan travel. On that trip, he changed drastically from his normal patterns of traveling with his family, staying and documenting his stay at his home, versus the documents showing on this trip a Motel 8, traveling alone, and changing his return, coming back weeks after he originally booked his return flight. We were the first to identify him as a certain level of concern and fully document his travel and his admission interview.

After the attempted bombing, we then provided the FBI with the keystone to link the phone number from the person who sold the car to the actual suspect, providing the FBI with his name, picture, and address. The phone then had been obtained and documented during that arrival process months earlier. We then posted a lookout in our system, while the former watch-listing process was occurring. Sure enough, he hit in our targeting systems when he attempted to flee the country.

Our targeting worked both on the inbound process and the outbound attempt. We worked closely with our DHS partner TSA and our local partners at JFK Airport to stop that departure, as he had already boarded the flight. In this case, every second mattered, and it highlighted the need for real-time targeting and cooperation between Federal, State, and local partners.

In the interest of time, I will discuss targeting more when you get back. I just wanted to hit on—CBP's Office of Intelligence and Operations Coordination was established in 2007, merging the former offices of Anti-Terrorism and Intelligence, as well as components of the Office of Field Operations, Border Patrol, and Information Technology. OIOC serves as the coordinating facilitator that integrates and leverages all CBP's diverse intelligence capabilities into a single, cohesive Intelligence Enterprise to create that intelligence-driven organization.

We support the agency's extended zone of security through the use of a multilayered approach to address threats to our borders, consisting of collecting advance traveler and cargo information, the use of enhanced law enforcement technical collection capabilities, and productive intelligence-sharing relationships with Federal, State, and local/Tribal agencies that also maintain a law enforcement presence at our border.

I will talk about targeting when you get back.

Mr. MEEHAN. Thank you, Ms. Mitchell. Thank you kindly for summarizing your testimony in that fashion.

So we have a series of three votes on the floor right now. The subcommittee will stand in recess until 5 minutes following the last vote in the series.

[Recess.]

Mr. MEEHAN. The committee will come to order.

I want to say thank you again for your patience. I thank you for your testimony, as well.

So, at this point in time, what I would like to do is to begin the questioning. I hope what we can do is do 5 minutes for each of us, and then, at the conclusion, if we have some remaining questions as well, because I think there is an awful lot of material to go through.

So I will begin the questioning.

Under Secretary Wagner, I am very grateful for your being here and for the role that you have undertaken in an agency in which there has been a great deal of, not just collaboration necessarily, but of course the role in which a number of agencies have been put together in an effort for us to more effectively and efficiently respond to the multiple challenges. That is difficult at any point in time. When you are talking about the sharing of intelligence across agencies, as well, difficult. I think we have made a great deal of progress in terms of breaking through some of the old stovepiping that existed, as well as some of the agency's tendency to want to hold on to, you know, their role and their information.

So I am grateful for the progress that has been made, but, of course, we still live in a very active world in which information flows and the threat is immediate. So I am certainly aware that one of the challenges that each of us has is the prioritization. Some elements of our infrastructure are defended in-depth against attack; others, not quite so much. We are always constantly worried about the ability of terrorists to adapt to what we have to do, as well.

We are also quite aware that there were 12 homegrown-inspired jihadist terrorist plots just in the last year. Two attacks and 10 plots by American citizens—lawful, permanent residents of the United States—were included in that. By comparison, over 7 years from the 9/11 attacks, there were an average of only about 2 such plots a year. So we are really in a period of enhanced concern.

You discussed the Department of Homeland Security's Threat Task Force, the DTTF, which is being brought to bear against, you know, specific incidents or National security investigations. I would really like to know what role that group is playing now, in light of the information that we have purportedly received from overseas and others with specific threats against some of our infrastructure.

Ms. WAGNER. Thank you, Mr. Chairman.

I want to first just make clear that the name "DTTF" sometimes causes some confusion because it sounds suspiciously like the FBI's JTTF, but they really do very different things.

The DHS Threat Task Force was created by my Principal Deputy, who was then the Acting Under Secretary, in the wake of the Zazi and Headley cases. As Jim Chaparro mentioned, it was created largely as a way to pull together all of the disparate pieces of information that were in the Department and all of the expertise

in the Department to make sure that the Department leadership was up to speed on rapidly evolving threats.

Since then, we have expanded the mission of the DTTF a little bit to be sort of the focal point of following emerging threats to the homeland and making sure that we have pulled all the right strings, touched all the right data sets, have reached out to our partners at FBI and the CTWatch and at NCTC to make sure that we are all up to speed and that we are doing what we need to do and everyone is on the same page. The DTTF is actually staffed by a mixture of I&A and component people. Currently, it is headed by someone from ICE.

We beefed up the DTTF recently, on a surge basis, to be the focal point for dealing with the information that was flowing from the exploitation of material captured during the UBL raid. We appreciate the fact that we got extra people in from the components to help us deal with that. We were using the DTTF to be our focal point for reviewing that information and determining when we needed to request tear lines, working in partnership with FBI and NCTC, so that we could get information out to our State and local customers.

Mr. MEEHAN. Are you satisfied that you are able to analyze in this treasure trove of information, that you have the capacity to be able to make some discretionary calls, but to be able to distinguish from among that trove of information and that there is a capacity to communicate that down appropriately to the local level?

Ms. WAGNER. Absolutely. I think I have rarely seen such a good interagency effort on this, the task force that the CIA is leading, on which we as a department have, I believe, seven people participating who are linguists, who are helping with the gisting and translating. There are people from all over the community participating in that.

We pulled together a group to work the tear-line issue. I am confident that we are getting the information that we need that needs to be shared with our State and local partners and with our critical infrastructure sectors. It has actually been going relatively smoothly, considering the volume of information.

We have been working jointly with the FBI to put out most of the information that we have put out. We have put out probably about 12, I think, joint intelligence bulletins at various classifications levels and to various audiences—that is, based on this information and in combination with other information that is still coming in through regular intelligence channels.

Mr. MEEHAN. Okay. Well, thank you. My time has expired, so, at this point in time, I will turn to Ranking Member Speier for questions she may have. Thank you.

Ms. SPEIER. Thank you, Mr. Chairman.

Thank you all for your testimony. As you were all speaking, I was thinking once again that you really are the unsung heroes who do this work, go unnoticed, and yet make sure that our country is safer because of it. So, thank you.

Let me start by asking you, the House is presently considering a $1 billion cut to the DHS budget. How will this impact your specific intelligence functions within your departments and agencies?

If you could just go right across the line as quickly as you can, but make your points.

Ms. WAGNER. I will start by saying that I think that we, my office specifically, has fared reasonably well, and we are appreciative of the mark that we received from the appropriators. I will defer to the others on any issues that they have.

Admiral ATKIN. Thank you.

My understanding is our budget has fared fairly well, as well, and that we aren't anticipating any major cuts at this time. Certainly, any major cuts would have significant negative impact on our ability to collect and report information.

Ms. SPEIER. Thank you.

Mr. JOHNSON. Ma'am, the same from TSA's perspective; we are doing really well.

Mr. CHAPARRO. From the ICE perspective, I think that we are doing well.

I would want to make sure that there are a couple of critical pieces that are in there. One is, we had an annualization of some positions for our Southwest border supplemental. As you know, the work we are doing on the Southwest border is critical. I would not want to see that falter. So far, we are good, and I would like to hopefully keep it that way.

Thank you.

Ms. MITCHELL. CBP's intelligence capability actually also fared well and received a small bump up for our targeting capabilities, which—I think one of the things you heard today is that the CBP targeting capabilities really do support all of our partner agencies.

Ms. SPEIER. So the billion dollars is not from any of your budgets?

Ms. WAGNER. If I could just add one thing that is not specifically an intelligence issue, but I think we are concerned about potential cuts to the grants, because the FEMA grant program is the source of a lot of funding for our State and local partners. While that is not specifically in my budget, we obviously are interested in ensuring that they receive enough funding to continue to be active participants in the homeland security enterprise.

Ms. SPEIER. Are any of your agencies involved with reviewing the bin Laden treasure trove, as we tend to refer to it?

You are all nodding your heads? So every one of you has a role in reviewing the materials. Okay.

This is a diagram of this entity that you are all part of, with Under Secretary Wagner in the middle. It is somewhat confusing because there are straight lines and then there are dotted lines. It is very difficult to bring 22-plus agencies together under one roof that have been independent and have everyone work well together. So I am sure there have been many challenges, probably none of which you would like to discuss in public.

But, as you have moved to adapt, I want to know whether or not there are still areas that we should be aware of, in terms of assisting you in unifying as a single agency?

Ms. WAGNER. One of the areas that we, I think, still struggle with as a department is in integrating our information systems. As we came from a bunch of different places, we have a lot of different legacy systems. The Department has a great deal of data—travel

data, immigration data, cyber data. A lot of that data is resident in different little stovepipes.

So we are working very, very diligently with the components and with the Department's chief information officer and then in my capacity, as the information-sharing executive, to work through how to do a better job internally of ensuring we have appropriate access to our data and that we are not having to redo functions multiple times, check individuals multiple times against multiple databases because they are all more linked.

We have a ways to go before we get to that goal, and that is something that we are still, you know, basically working on.

But I would offer anyone else the opportunity to comment, if you are interested.

Mr. CHAPARRO. No, I agree with Under Secretary Wagner. I think one of the biggest challenges we face is the vast volume of data that we have to sift through in order to identify these sometimes very vague or amorphous threats. Having the data tools and the connectivity to be able to look at TSA data or to be able to look at intelligence community data or travel data and to able to do that in an integrated fashion I think is a challenge that we all face day-to-day.

Ms. SPEIER. Anyone else?

Mr. JOHNSON. There is a tremendous amount of collaboration that needs to occur, and you have to have those collaborative tools that are out there. How many different documents we have to go through every day and the analytical tools that could be out there to help us provide diffused products and put them into an analytic product at the end of the day could be very helpful.

Admiral ATKIN. In the essence of time, I will concur with my colleagues.

Ms. SPEIER. Okay.

Ms. MITCHELL. The only one point I would like to add is we also need that ability to go from the high side to the unclass side, as well. Our systems need to be able to do that.

Ms. SPEIER. All right. Thank you.

I yield back.

Mr. MEEHAN. Thank you, Ranking Member Speier.

At this point in time, I would like to recognize the gentleman from Minnesota, Mr. Cravaack.

Mr. CRAVAACK. Thank you, Mr. Chairman.

Thank you, also, to the witnesses, and thank you for your service to the country. You are the unsung heroes. You are the guys that don't get the medals or the ribbons, but we appreciate all the things that you do and your troops do. So, thank you very much for that.

My quick question is: Admiral, sir, could you please tell me what keeps you up at night? What is the main threat to your ability to do your job?

Admiral ATKIN. Sir, as you know, right now we don't have any imminent threat in the maritime domain. Being the new guy on the block, I am still learning quite a bit about what the intelligence community for the Coast Guard, the Intelligence Enterprise, is working on.

But I think my biggest concern is two-fold. One, it is the safeguarding of the Coast Guard personnel themselves. How do we provide the right force protection for those folks and the right intelligence support for that force protection? Then the next piece would be those transnational threats, whether they be criminal or terrorist organizations, and how they are trying to get into the country and attack the American people.

So, not having a specific threat right now. It is really trying to identify, working with the colleagues here in DHS but across the intelligence community, to identify how they are coming into the country and then how to stop that.

Mr. CRAVAACK. Thank you, Admiral. I do feel your pain when it comes to being the new guy on the block.

Mr. Johnson, according to TSA, how would—you have kind of alluded to it in your opening testimony. Can you kind of expound upon that a little bit?

Mr. JOHNSON. Yes, sir. We had that closed-door session with you a couple of months ago. It continues to be AQAP and threats to aviation, followed closely by mass transit and different threats that are out there that are being espoused from a global threat perspective and providing a regional focus into the United States.

Mr. CRAVAACK. Thank you.

Mr. Chaparro, could you kind of allude to it also, as well?

Mr. CHAPARRO. The short answer is, my BlackBerry keeps me up at night.

But all kidding aside, ICE has, you know, a very wide breadth of things that we cover. It is the violence from drug cartels, it is the pedophiles, it is the transnational criminal organizations that we investigate, it is the threats in the cyber world.

So I think there are many, many things that we have to focus on in order to make sure that our citizens are safe. To be honest, I wish it were only terrorism. But it is that and, unfortunately, much, much more.

Mr. CRAVAACK. Thank you for that. Thank you for being by your BlackBerry.

Ms. Mitchell, could you expound, as well?

Ms. MITCHELL. Sure. Thanks.

I think for CBP the biggest thing that we are concerned with is kind of the unknowns. We believe we have a good handle on identifying those that we know are bad, but to ensure that our systems also have that predictive modeling capability that allows us to pick up on those travel patterns that should be of concern, kind of picking up on the clean skins.

Also, the impact of global security, that we are partnering with a lot of the foreign governments to ensure that they are picking up on that same thought process for targeting as we have here.

Mr. CRAVAACK. Have you found the international community to be assisting you on that quite a bit, or is it more of a challenge?

Ms. MITCHELL. I think, as they are finding that they, themselves, are targets, as well, and we can show some success stories in our targeting methodology, they are becoming much more willing partners.

Mr. CRAVAACK. Okay. Thank you.

Ms. Wagner.

Ms. WAGNER. I think, listening to what everyone else has said, I think the one thing that keeps me up at night the most is having there be an attack on the homeland and discovering that we had data in the Department that was relevant to it.

That is why I focus so much of my efforts on trying to make sure that we have the procedures in place to make sure that we are tapping every piece of information that we have, so that I hope never to be in that position.

Mr. CRAVAACK. I hope you never are, as well, ma'am.

Two years ago, Secretary Napolitano asked the I&A to coordinate with the DHS in interaction with State and local fusion centers, where—you know, a lot of the genesis comes from the boots-on-the-ground level. I am from Minnesota. Because of an alert pilot that was giving instruction to a guy who wanted to take off in a 747—not know how to land, just wanted to be able to fly the plane—that is how some critical information could have flowed up the chain of command.

Would you just kind of please update us on that progress?

Ms. WAGNER. I think we have made a great deal of progress in the last few years in building a network of National fusion centers that share information both upwards with the National intelligence and law enforcement communities and sideways with each other, which is a really important regional aspect of this.

What we are trying to do, both in I&A—but I&A basically is leading the efforts of the Department that includes all of the component participation—is to provide information, training, anything that we can do to help the fusion centers achieve a level of ability to analyze their own information, report on it, and understand what information is valuable to others so that it can be effectively shared.

We have IOs, intelligence officers, out at all the fusion centers. There is also component representation at many of them. We provide training courses in writing, reporting, protecting civil rights and civil liberties. I think that we are seeing from most of the fusion centers improved levels of situational awareness and products coming out of them. We have a great interchange with them on a daily basis.

We are focusing on implementing, with the Department of Justice, the National Suspicious Activity Reporting Initiative. The fusion centers are a key element of that.

The Secretary has also been, as I am sure you are aware, promoting the "See Something, Say Something" campaign. That is a way for us and the fusion centers then to leverage the American public to be on the lookout for information, behaviors that might potentially allow us to detect and disrupt activities.

So, between the "See Something, Say Something" campaign and the National Suspicious Activity Reporting Initiative that is feeding both us and the FBI's eGuardian system and just the constant interaction that we have, I think we are in a very good position to use those guys as the first line of defense in detecting and deterring homegrown violent extremism.

Mr. CRAVAACK. Thank you very much, ma'am.

I am over my time, sir. I apologize. I will yield back.

Mr. MEEHAN. Thank you, Mr. Cravaack.

Now the Chairman would recognize the gentleman from Arizona for 5 minutes of questioning, Mr. Quayle.

Mr. QUAYLE. Thank you, Mr. Chairman.

Under Secretary Wagner, we hear a lot about the need to improve the level of information sharing between the various Federal agencies, but we don't often hear about how that is done within each individual department. So, at DHS, what are you doing to improve kind of the intelligence collaboration and information sharing within the DHS Intelligence Enterprise?

Ms. WAGNER. Well, actually, we are doing multiple things, because there is not a single silver bullet to solve information sharing or communications.

So we start with the Homeland Security Intelligence Council that we discussed earlier. These are some of the key members. We meet regularly on a monthly basis in person, we have weekly teleconferences to make sure that we are all on the same page about the emerging threats and any other things that we are trying to address collaboratively.

But, at the same time, we have multiple daily levels of interaction. For example, these folks have representatives on the DHS Threat Task Force, which is, again, keeping everybody up to speed on emerging and evolving threats. Our analysts work together on a daily basis to produce joint products, some of which go in the Secretary's daily briefing book, many of which are shared with our State and local partners and with the rest of the intelligence community.

So it is multiple interactions across the board. We also work closely on collection requirements, as well as on analysis and on developing analytic tools.

So I can't even discuss all the levels of interaction there are, but we have been trying to significantly improve the cooperation and the communication, and I think we have made a lot of progress.

Mr. QUAYLE. Great. Thank you.

Mr. Chaparro, you said the drug cartel activities have been keeping you up at night sometimes. What are we doing from an intelligence standpoint to able to apprehend and to make sure that we are not seeing these drug cartels continue to move across our border?

Mr. CHAPARRO. I think, as we have seen the drug cartel threat and violence evolve, particularly in Mexico but elsewhere as well, I have seen a higher level of emphasis placed by the larger intelligence community. I would say very candidly that they are being very responsive to our requests for information and support.

It is a strain. I know that we have wars going on in Iraq and Afghanistan, and the intelligence community is stretched very thin. But this is a threat this is very close to home, and it impacts our communities tremendously.

So we are doing everything that we can possible from a law enforcement perspective to bring the cartel members to justice but also to make sure that information that is coming out of our operations, as we understand the cartel structure—where they are operating, how they are operating, how they are communicating—we are making sure that we are passing that information to the intelligence community to help them better sharpen their focus, as well.

Mr. QUAYLE. What is the ability to work with your counterparts on the Mexican side? Has that been fruitful? Have you been able to glean a lot of information and have a fairly good working relationship with them?

Mr. CHAPARRO. I have been in this business a long, long time, and, in all honesty, I think the cooperation has never been stronger. I think, for example, when Special Agent Jaime Zapata was murdered in Mexico last February, the support that we received from the Mexican government as well as the U.S. law enforcement intelligence community was just unprecedented.

So, the cooperation is good. You can always build and make things better, but I have never seen it as good as it is today.

Mr. QUAYLE. Thank you very much.

Mr. Chairman, I yield back.

Mr. MEEHAN. Thank you. Thank you, Mr. Quayle.

I hope that I might ask just one more round of questions myself, and the Ranking Member may have a few questions.

Ms. Wagner, this sort of may seem counterintuitive because we spend a lot of time, in the intelligence field, trying to develop as much information as we can on emerging threats, which means we develop a lot of information about a lot of things, a lot of people. You are building a sophisticated network with fusion centers that are touching each and every one of our communities, and we have a broad spectrum of agencies that are simultaneously participating. So, within our treasure trove of information, there is information about a lot of people, including American citizens, among others.

You know, in my own State of Pennsylvania, before I was elected, but I was very aware of information that was developed by one of our entities that was let out into the mainstream to the benefit of somebody that was really—it was a private entity that took advantage of that intelligence information.

What are we doing to assure that the civil liberties and privacy protections are in place so that we access information appropriately but guard against inappropriate uses of that information?

Ms. WAGNER. Thank you for that question, because that is something that we focus on a lot.

For all of us who are sort of intelligence activities, we have intelligence oversight that is embedded in our organizations. You know, it flows from the Executive Order 12–333 and the guidelines within which we operate. So we have pretty well-defined ways of training our people, of double-checking to make sure that we are following the rules, and periodically going through all of our reports and seeing how we are doing.

For the National network of fusion centers, this is a new world in which they are operating. So we have focused a lot of time and effort and resources on training them to understand the rules regarding privacy and civil rights and civil liberties and Constitutionally-protected activities.

We have worked with them to ensure that every fusion center has a privacy policy in place. We work with them to make sure that those are adequate, that everyone who is in the fusion center has been trained on what is in those policies, and that those policies are being followed.

We work very closely with our civil rights and civil liberties office to provide training teams out to the fusion centers to make sure that they are fully trained on all the same things that we all have grown up——

Mr. MEEHAN. Do they then take that and reach out, as well, within their communities to local police and otherwise?

Ms. WAGNER. Yes, they do. So I am confident that we are very much leaning forward to build in protection of privacy, civil rights, and civil liberties at the front end of all of our engagements with the fusion centers and in all of the products that we are putting out.

Mr. MEEHAN. Thank you for that and for your work on that. It is very, very vitally important, I think, as part of our mission, and often overlooked.

Mr. Chaparro, you touched on a variety of things. As a former United States attorney, I used to stay up at night thinking about a lot of different issues and always, you know, is there something we could be doing better?

You touched on one area in which agencies like yours might be the only people that have an opportunity to reach out and be a lifeline to some victims who live a horrible existence, and these are these victims of human trafficking go and others who are then put down into the system. How are we doing in that battle?

Mr. CHAPARRO. I think that human trafficking is an area where ICE has really stepped out in front to take a leadership role in not only rescuing victims but aggressively going after and prosecuting the horrific criminals that commit these crimes.

But, equally important, we have victim witness assistance coordinators in every single one of our field offices to ensure that the victims of human trafficking are able to get the help that they need in order to be able to recover.

Similarly, we are working very closely with the community organizations, the nongovernmental organizations, and we are working both domestically and overseas to combat human trafficking.

Mr. MEEHAN. How about with our local police departments and others? Because one of the things that used to be of concern to me is that you would often have local police departments that might come in, make an investigatory stop, look at somebody, realize, "Well, this is an immigration violation but not necessarily worth my making an arrest for some particular purpose," but they are looking past signals that may indicate that there is something more going on.

Are we training local police to be able to identify the signs, to ask the appropriate questions, and then to come back to experts like you or partners?

Mr. CHAPARRO. Absolutely. A big part of our efforts is the outreach that we do, including working in local human trafficking task forces around the country so that, as local authorities, as you said, identify signs that may be an indicator, they know to ask the right question, they know to go that step further. The outreach that we have is both in terms of formal training as well as various conferences, passing out brochures. Then there is no substitute for working hand-in-hand on the local task forces so that they can really understand what it is that they face.

Oftentimes, the signs are very hard to detect. The victims are often very scared to come forward. It really takes a lot of work sometimes to undercover these violations.

Mr. MEEHAN. Thank you. My time has expired.

I will turn it to the Ranking Member, Ms. Speier.

Ms. SPEIER. Thank you, Mr. Chairman.

I, too, have an abiding interest in the whole human sex-trafficking issue, so much so that I convened a workforce locally and have had the district attorneys, the U.S. attorney, the FBI, local police, all part of a training. We have met now five or six times. There was an all-day training just a couple weeks ago.

But I will tell you this, that we really have just scratched the surface. While we may on a Federal level make resources within your jurisdiction available, we need to do much, much more.

Just in the short time that we have been working on this issue, our local DA has gone back and recognized that two domestic violence complaints that came in on the same person with different complainants turned out to be a sex trafficker. It didn't dawn on him until he had started participating in this program.

So I bring it up only because I think we need to do more. I know that you are already taxed, but it is a horrific problem. The sex trafficking of those under the age of 18 is somewhere close to 300,000 in this country alone. So I hope that we can see new initiatives come out from within your various agencies to help in that regard, as well.

I have just one last question. It would appear, based on what we have been able to glean from the information that bin Laden had in his Abbottabad location, that rail was a very interesting target for them. I happen to have traveled with my daughter over spring break on a college tour along the East Coast, and we did it by train. I thought about it a lot, because I think the trains are incredibly porous. I don't know what we have under way to try and address that issue, but I think that it is just ripe for some kind of an attack that will come from a lone wolf who is, you know, homebound right amongst ourselves.

So if any of you have any thoughts that we would like to share with us on what we can or should be doing relative to rail, I would appreciate hearing it.

Ms. WAGNER. I will just say one thing and then turn it over to Dan, since it is a TSA issue, just to say that we have obviously known, based on looking at events overseas, that rail has been a target of interest to terrorists and al-Qaeda affiliates if we just look at what has happened in London and Madrid and Moscow.

So we have been publishing on the tactics and techniques that have been used in these attacks on rail to our law enforcement and public-sector partners to help them think through the appropriate protective measures for some time.

But I will turn it over to Dan for any specifics.

Mr. JOHNSON. We have specific analysts that look at rail specifically and also passenger rail, freight rail. They do annual assessments, both at the classified and unclassified level. It probably would be better if we went ahead and we had a closed-door session and walked you through the classified findings that we have within

the rail assessments that we have out there, especially in light of bin Laden's roll-up.

Ms. WAGNER. We want you to feel confident that we have been looking at this for quite a while.

Mr. JOHNSON. Absolutely.

Mr. MEEHAN. Well, I want to express my deep appreciation to this very, very distinguished panel, first, for your patience; second, for your excellent testimony and the preparation that went into it; but, last and most importantly, for your service. I think all of us appreciate that you are on the front line, and you are on a front line in what is now a very precarious time for our country. Yet, at the same time, you know, I don't like to be alarmist because I think the work that you are doing is making a big difference.

We have seen, over the course of the last year, an increase in real threats to our Nation, but simultaneously, if you were to have looked at this 10 years ago from September 11 and had predicted what may have been, I think there are few who would argue that we have not been vigilant and had some genuine successes. But no one goes to sleep at night and says, "Okay, because tomorrow is another day, and I know it is not on my watch."

So I want to thank you for your work, but more important, your service to our Nation.

The Members of the committee may have some additional questions. I hope that if they do those that you will do your best to be as responsive as can you in writing. The hearing record will be open for 10 days.

So, without objection, the subcommittee stands adjourned. Thank you.

[Whereupon, at 4:13 p.m., the subcommittee was adjourned.]

○