IS THE OFFICE OF INTELLIGENCE AND ANALYSIS ADEQUATELY CONNECTED TO THE BROADER HOMELAND COMMUNITIES?

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 29, 2010

Serial No. 111–83

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

66–033 PDF WASHINGTON : 2011

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

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
DINA TITUS, Nevada
WILLIAM L. OWENS, New York
VACANCY
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio
TOM GRAVES, Georgia

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
AL GREEN, Texas
JAMES A. HIMES, Connecticut
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
PAUL C. BROUN, Georgia
TOM GRAVES, Georgia
PETER T. KING, New York *(Ex Officio)*

MICHAEL BLINDE, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
MEGHANN PETERLIN, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

The Honorable Jane Harman, a Representative in Congress From the State of California, and Chair, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment:
Oral Statement 1
Prepared Statement 2
The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment 3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security:
Prepared Statement 12
The Honorable Laura Richardson, a Representative in Congress From the State of California:
Prepared Statement 13

WITNESSES

Ms. Caryn A. Wagner, Under Secretary for Intelligence and Analysis, Office of Intelligence and Analysis, Department of Homeland Security:
Oral Statement 4
Prepared Statement 7

APPENDIX

Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Intelligence and Analysis 21
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Infrastructure Protection 23
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Operations Coordination 24
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Domestic Nuclear Detection Office 24
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Counternarcotics Enforcement 24
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Cyber Security and Communications 24
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Health Affairs 25
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Policy 25
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Office of Risk Management and Analysis 25
Questions From Chairwoman Jane Harman and Ranking Member Michael McCaul for the Science and Technology Directorate 26

IS THE OFFICE OF INTELLIGENCE AND ANALYSIS ADEQUATELY CONNECTED TO THE BROADER HOMELAND COMMUNITIES?

Wednesday, September 29, 2010

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

The subcommittee met, pursuant to call, at 4:10 p.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [Chairwoman of the subcommittee] presiding.

Present: Representatives Harman, McCaul, and Dent.

Ms. HARMAN. The Subcommittee on Homeland Security will come to order. The subcommittee is meeting today to receive testimony on the question: Is the Office of Intelligence and Analysis—called I&A—Adequately Connected to the Broader Homeland Communities?

Let me apologize to our witness for keeping her so long. The House is probably in its last day before the recess until the election, and everything possible is coming up on the House floor, including in a few minutes the intelligence authorization bill, something that I know our witness has great affection for because a few years back she worked on the staff of the House Select Committee on Intelligence.

We are starting now, but our Ranking Member is expected any minute, and I am vamping just slightly so when I finish my opening statement he will be here and can give his, and then we will move promptly into Secretary Wagner's testimony and questions.

Welcome, Under Secretary Wagner. This is a busy time of year for all of us, and the subcommittee greatly appreciates your appearance today to discuss how you are improving I&A's capabilities.

Today's hearing will focus on I&A's relationships with other parts of DHS, the other headquarters elements that need intelligence to carry out their own missions.

We want to know how you are communicating and sharing information with the Science and Technology Directorate, the National Operations Center, and the National Programs and Protection Directorate, among others. Are your relationships with these entities adequate and are you performing as a leader in a constellation of parts of DHS that need intelligence to carry out their missions? Is intelligence adequately shared so that I&A accurately analyzes and

produces timely and useful threat information about terror targets and tactics to its customers?

As you know, your predecessor, Charlie Allen, prided himself on his connections throughout the Government. He was a legend, having spent a half century virtually as one of the leaders of the Central Intelligence Agency, and no one doubted his ability to work horizontally across the Government.

The issues this subcommittee had with your predecessor related not to his ability to work horizontally, but to his ability to work vertically, something that is much improved during your tenure under the leadership of your deputy, Bart Johnson.

So today it appears to us, or to me anyway, that I&A is doing much better with vertical integration outside the Department, from I&A down to State and local law enforcement and back. It is also doing much better with vertical integration within the Department, from I&A to the intelligence elements inside DHS and back to I&A. But what we are concerned about is whether I&A is doing enough with horizontal integration across the Department, from I&A to the other DHS headquarters offices and back. I hope I am being clear.

We have taken a look at the most recent version of the DHS Intelligence Enterprise Strategic Plan, which I might note is dated 2008 and still has Charlie Allen's picture at the front. It says that you as the DHS Chief Intelligence Officer are charged with leading and managing the Enterprise. This includes making sure that information is shared throughout the Department. What is your honest assessment of progress to date?

I want to assure you, Madam Under Secretary, that I am not proposing to move boxes around. I think I have learned a lot about doing that in recent years, and I do not want to just add names of organizations to the list that composes the Enterprise. What I am interested in is making sure that you have what you need to manage the critical relationships of I&A, both vertical and horizontal, to manage them simultaneously without trading one off against the other.

Today we hope to hear the good news stories of cooperation and collaboration, but we also want to hear about the areas that need some work. We want to work as your partner, an offer I made frequently to Charlie Allen, knowing that the better you do your job, the safer our communities will be.

Welcome, and again thank you for your service.

The Ranking Minority Member is now here. I now yield 5 minutes to the Ranking Member for an opening statement.

[The statement of Chair Harman follows:]

PREPARED STATEMENT OF CHAIR JANE HARMAN

SEPTEMBER 29, 2010

Welcome, Under Secretary Wagner. This is a busy time of year for all of us, and the subcommittee appreciates your appearance today to discuss how you are improving I&A's capabilities.

Today's hearing will focus on I&A's relationships with other parts of DHS—the other headquarters elements that need intelligence to carry out their own missions.

We want to know how you are communicating and sharing information with the Science & Technology Directorate, the National Operations Center and the National Programs & Protection Directorate—among others. Are your relationships with these entities adequate?

Is intelligence adequately shared so that I&A accurately analyzes and produces timely and useful threat information about terror targets and tactics to its customers?

As you know, your predecessor, Charlie Allen, prided himself on his connections throughout the Government. He was a legend—and no one doubted his ability to work horizontally across the Federal Government.

The issues this subcommittee had with your predecessor related to vertical information sharing—something much improved during your tenure, under the leadership of your deputy, Bart Johnson.

Today, it appears that I&A is doing much better with vertical integration outside the Department—from I&A down to State and local law enforcement and back.

I&A is also doing much better with vertical integration within the Department—from I&A to the intelligence elements inside DHS and back to I&A.

But this subcommittee is concerned that I&A is not doing such a great job with horizontal integration across the Department—from I&A to the other DHS headquarters offices and back to I&A.

We've taken a look at the most recent version of the DHS Intelligence Enterprise Strategic Plan (which I might note is from 2008 and still has Charlie Allen's picture at the front).

It says that you, as the DHS Chief Intelligence Officer, are charged with leading and managing this Enterprise. This includes making sure that information is shared throughout the Department. What is your honest assessment of progress to date?

I want to assure you, Madam Under Secretary, that I am not interested in moving boxes around in an organizational chart.

And I do not want to just add names of organizations to the list that composes the Enterprise.

What I am interested in is making sure that you have what you need to manage the critical relationships of I&A—both vertical and horizontal—and manage them simultaneously, without trading one for the other.

Today we hope to hear the good news stories of cooperation and collaboration.

But we also want to hear about the areas that need some work.

We want to work as your partner—knowing that the better you do your job, the safer our communities will be.

Welcome, and thank you for your service.

Mr. MCCAUL. Thank you, Madam Chair. I appreciate your patience in waiting for me. I got tied up on an important matter, but nothing is more important to me than this hearing, and it has been a joy to work with you. This may be our last hearing, and I just want to say one thing about the Chair, you always know where you stand, and I appreciate that.

I want to thank Madam Chair for holding this hearing. Welcome, Madam Secretary.

First of all, I want to let you know that the Houston Fusion Center, I had a visit and they wanted connectivity to classified information, SCIF, and you were very responsive in fixing that issue, and I want to thank you for that.

Also, I want to let you know that we have heard that I&A has significantly improved its interactions both within the Department and with State and local fusion centers and I appreciate that. We are all well aware of the problems you inherited at I&A, and it does appear at least to some extent that things are improving.

I do, however, want to raise a few specific concerns with you. I know you recently had to change your plans for the Joint Fusion Center Program Management Office, and I am pleased to learn that you are continuing to move forward with that, that goal to coordinate DHS interactions with the fusion centers. In my judgment, this level of coordination is extremely important.

I am concerned, however, that DHS is not paying the same attention to coordinating its interaction with the States as a whole. I have heard reports that different parts of DHS are going to different State offices with threat information, sometimes cutting the

fusion centers out of the process altogether. In my judgment, the Department should be the shining example for the rest of the Federal Government on coordination and information sharing, and I want to be sure that we are not ignoring stovepipes that may be popping up within DHS, particularly when it comes to interactions with State and locals.

Additionally, when taking a look at the DHS Intelligence Enterprise organizational chart, many DHS elements seem to be missing, in my judgment. As one example, the Office of Cyber Security does not appear as part of the Intelligence Enterprise.

I hope through this hearing we can explore how the Department defines homeland security intelligence and how you distinguish between partners in the DHS Intelligence Enterprise and elements who are not, and how you have prioritized I&A's customers within the Department. So I look forward to hearing your testimony.

Madam Chair, I am aware there were some scheduling conflicts with today's hearing, so we were unable to hear from the other DHS headquarter elements that we will discuss here today. While I know Under Secretary Wagner will do a capable job, I want to be sure that we note that we will only be hearing from one side, Madam Chair, and I hope that we will be able to hear from the other parts of the Department on this topic in the future so that we can really delve into the problem areas and find solutions.

Finally, I have said it before, but I want to reiterate once again that I hope that you will view this as an opportunity for us to discuss the issues, have a constructive conversation, and work together to solve the internal problems at the Department. At the end of the day, I know we all want to see it succeed in keeping the American people safe. In my judgment, DHS needs to get its own house in order before it can hopefully fulfill that mission.

With that, I yield back.

Ms. HARMAN. I thank the Ranking Member. We did have several conversations about who else might testify today and decided for a variety of reasons, including the lateness of the hour, that we would have Under Secretary Wagner but that we will communicate with the other Enterprise elements. I am notifying you, Ms. Wagner, that we plan to send questions in writing as part of our hearing record to those elements so that we have a full record of their views as well as your views about this critical subject. I assume that is all right. Fine.

You are now recognized to summarize your testimony in approximately 5 minutes.

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

Ms. WAGNER. Thank you very much, Madam Chair. Before I start, I wanted to congratulate you on the passage of your legislation, Reducing Overclassification Act of 2009. We enjoyed working with you on that legislation, and we believe it is going to help us in our efforts to prevent overclassification and ensure that we can share critical information with State and locals.

Ms. HARMAN. If I might interrupt, we are all pleased about that. It wasn't just my legislation, it was unanimously reported by our

subcommittee, and it only took 3 years to get it to pass the Congress. Much of that time was spent in the United States Senate, you understand. But at any rate, we are thrilled about this, and are hoping that the President will sign the bill into law at the nearest possible time.

Ms. WAGNER. I am sure he will.

Madam Chair, Ranking Member McCaul, Congressman Dent, and other distinguished Members who may appear later, thank you for the invitation to appear before you to discuss how the Office of Intelligence and Analysis supports the activities of the Department's headquarters elements and thus the Department's larger set of customers and partners.

We have spent some time trying to come up with a vision statement for I&A, which is not as easy as it might seem given the broad and diverse set of missions that the office has. What we settled on was the phrase: "Equipping the Homeland Security Enterprise with the information it needs to keep the Nation safe, secure, and resilient."

The Homeland Security Enterprise, as I have testified before this subcommittee before, is a set of concentric circles. It includes the Department's headquarters elements, its many and varied components, its State, local, Tribal, and territorial partners, and at its widest extent, the American public, who is a key stakeholder in the Homeland Security Enterprise.

I have appeared before you, as you mentioned, to discuss our role in supporting the Department's components, and also the National network of fusion centers. Today, you have asked me to focus on our support and relationships to the headquarters elements. I am happy to do that. I think I have some good news to share, although clearly there are areas where we can improve, and I will highlight a few of those.

I&A is by its nature a service element, and we provide our specific service, tailored intelligence and information, to both the operating elements of the Department, like Customs and Border Patrol, but also to other service elements like ourselves, such as the Office of Policy and the Office of Health Affairs. While the types of interactions and products and services that we provide to the different department elements vary, there are several common themes that underpin our interactions with all of these elements.

First, we provide the entire Department, and by inference its many customers, with a common understanding of the threat. The Department is largely in the business of managing risk, risks from terrorism, natural disasters, chemical and biological agents, cyber attacks, and identifying and analyzing the threat is a key part of the risk management model. So risk is a function of threat, vulnerability, and consequences. I&A owns the threat piece, and we support our partners in assessing vulnerability and consequences to assess the overall risk to the homeland.

Second, we are responsible for facilitating the Department's interaction with our State and local customers via the fusion centers. This goes to Ranking Member McCaul's comments. We are trying to improve this, and I think we are making progress, although we do still have incidences of people kind of getting a little bit off the reservation. I think that is happening less and less as

we improve the representation in our State and Local Program Office and we educate both the fusion centers, the State governments, and our own people on the mission of the State and Local Program Office.

We also use interdepartmental coordination forums, and as I mentioned, liaison personnel, and our most recent detailee to the State and Local Program Office comes from the Office of Health Affairs to better integrate health information into our interactions with State and local governments.

Third, we leverage the intelligence community for the most complete and current information to support our many customers and partners. An example of this is the role that we play in communicating to the Domestic Nuclear Detection Office, the analytic judgments and the collection capabilities of the National intelligence community so that they can factor those in as they develop the global nuclear detection architecture.

So our closest continuing collaborations within the Department are probably with the National Programs and Protection Division, the Office of Operations Coordination and Planning, and the Office of the CIO.

We have an extremely close partnership with the Office of Infrastructure Protection, which resides within the National Programs and Protection Division. We work together in an integrated analytic unit to assess the threat and vulnerability for critical infrastructure and key resources. We are jointly conducting a Risk 101 training course for State and local fusion center infrastructure analysts, and we recently held a joint meeting for fusion center analysts and IP's deployed protective security advisers, another element that for a while was independently dealing with fusion centers and State and local governments, and we have now tried to make that more integrated and coherent, and we have gotten great cooperation.

We also work closely with IP's Office of Bomb Prevention to provide coordinated products to the field on terrorist use of bombs, improvised explosive devices, and other weapons.

The Department's Office of Cyber Security and Communications also resides within the National Programs and Protection Division. I&A analysts are physically embedded in the National Cybersecurity and Communications Center, the NCCC, and in the U.S. Cyber Emergency Response Team, US–CERT. These cyber analysts deliver products and services to the sector coordinating councils, to State and local authorities, and to the private sector, working in close collaboration with our NPPD counterparts. We are working here also to increase the interaction with the fusion centers and the products that we provide.

In the operations arena, I&A as an Intel Watch and Warning Section embedded in the National Operations Center to integrate intelligence into the common operation picture, receive and disseminate intelligence warning information, and provide outreach to the intelligence community to keep the NOC and the DHS leadership advised of breaking events. While the relationship with the NOC is excellent, the physical configuration that we have on Nebraska Avenue is not optimal for integrating the intel and operations pieces, so we are actively engaged with our ops colleagues

to follow best practices in how we integrate intelligence operating at a different classification level with our operations and watch elements when we move to St. Elizabeth's, and that is going very well.

In addition to being Under Secretary for Intelligence and Analysis and the Chief Intelligence Officer for the Department, I am also responsible for information sharing. I chair the Information Sharing Governance Board with representatives from all of the key components and headquarters elements. In order to help the Department move forward in having an integrated information architecture, I formed a strategic partnership with the CIO, Richard Spires, to use the Information Sharing Governance Board to accomplish IT portfolio management responsibilities as well as its broader policy and procedure mandate. He and I also co-chair the National Security Systems Program, a vehicle for joint management of the Department's classified systems. So the relationship with the CIO is strong and growing.

These are just a few of the relationships that we have with elements at the headquarters. I am happy to answer questions about these or any of the others that I haven't mentioned. In the 7 months I have been on the job, I have worked hard to reach out and make it clear that I&A exists to serve the Department and its missions. There is still room for improvement, especially as we bring new people on board and try to introduce them into the ops and planning cycles of all of the various headquarters elements, but I think we are making steady progress, and I hope that we are increasingly being viewed as a constructive member of the DHS team. I personally will continue to focus on improving those relationships.

Thank you for your time.

[The statement of Ms. Wagner follows:]

PREPARED STATEMENT OF CARYN A. WAGNER

SEPTEMBER 29, 2010

INTRODUCTION

Chair Harman, Ranking Member McCaul, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) interfaces, supports, and coordinates with headquarters elements of the Department—the offices and directorates at the headquarters level that report directly to the Secretary, outside of our seven operating components.

Before I address the main topic of this hearing, I must echo the Secretary's testimony from September 22, 2010: The terrorist threat to our country is changing in ways that increasingly challenge law enforcement and the intelligence community. The Department is moving at all levels to address this evolving threat; preventing terrorist attacks in today's dynamic threat environment means working in a unified way across all levels of Government. DHS' intelligence mission, which I am honored to lead, is to sustain a unified and synchronized intelligence enterprise that enables informed decision-making at DHS and in the entire homeland security enterprise. The mission of I&A is to strengthen the Department's and our partners' ability to perform their homeland security functions by accessing, integrating, analyzing, and sharing timely and relevant intelligence and information, while protecting privacy and civil liberties.

THE OFFICE OF INTELLIGENCE AND ANALYSIS STRATEGIC VISION

I&A is charged with leading the Department's efforts to provide intelligence and information in a useful form to Departmental decision-makers, headquarters, and operational components, State, local, Tribal, and private sector partners, and the

National intelligence community. Our job is to serve as the two-way conduit for information that supports protecting the homeland. I&A's programs, projects, and activities align with the core DHS missions designated in the Quadrennial Homeland Security Review (QHSR). To that end, I&A plays a critical role to DHS' success in all of its core mission areas: Preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, safeguarding and securing cyberspace, ensuring resilience to disasters, and strengthening and maturing the Department.

In my last appearance before this subcommittee in May, I addressed the evolution of the DHS Intelligence Enterprise and how it interacts with Departmental operational components. Today, I appear before you to discuss the ways in which I&A supports the headquarters elements of the Department.

INTELLIGENCE SUPPORT TO DHS HEADQUARTERS ELEMENTS

A key reason for I&A's existence is to support the intelligence needs of the Department as a whole. To this end, I firmly believe that I&A must provide the entire Department with a common understanding of the threat. In ascribing to this model, I am dedicated to providing timely, relevant, and vigorous intelligence support to DHS headquarters elements, as well as to the Department's operational components. This, of course, is in addition to our focus on supporting the intelligence and information sharing needs of our non-Federal partners, the National intelligence community, and the Nation's private sector.

I&A interacts with headquarters elements within DHS in accordance with the authorities given to me as the Department's Chief Intelligence Officer. This interaction includes I&A production of analytic products tailored to the needs of DHS headquarters elements. I use my dual authority, as both the Under Secretary and Chief Intelligence Officer, to ensure that Department investments in intelligence programs, projects, and activities are focused on Departmental and National priorities, closing gaps, eliminating redundancies, and ensuring that investments in intelligence are measured for utility and outcome.

I&A supports, interacts, and shares information with DHS headquarters elements in many ways. These include the following elements:

Science and Technology Directorate (S&T)

S&T is one of I&A's principal Departmental customers. I&A provides monthly and ad hoc intelligence briefings to Dr. Tara O'Toole, the DHS Under Secretary for Science and Technology. These customized briefings are designed to meet her intelligence needs. I&A disseminates finished intelligence assessments to specific customers in S&T on a regular basis, and interacts with decision-making and subject matter expert counterparts at least several times a week. I&A participates in and manages intelligence community input to the threat elicitation phase of S&T's Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism Risk Assessments, including the Bioterrorism Risk Assessment, and the Integrated CBRN Terrorism Risk Assessment for the Department.

I&A plays a significant role in supporting the Material Threat Assessments, which were developed by S&T to support the Secretary in issuing Material Threat Determinations pursuant to the Project Bioshield Act of 2004. Members of I&A also serve on the Biodefense Knowledge Center Advisory Board and the National Biodefense Analysis and Countermeasures Center Science Advisory Board.

National Protection and Programs Directorate (NPPD)

I&A has a unique, ingrained relationship with the DHS Office of Infrastructure Protection (IP), which resides in NPPD. As you know, I&A's precursor organization combined the missions of intelligence and analysis with infrastructure protection. Today, I&A provides enduring support through its participation in the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a Departmental fusion center designed to facilitate the sharing of threat and risk information with IP's public and private sector partners in the Nation's critical infrastructure community. I&A also collaborates closely with NPPD's cybersecurity elements, including the United States Computer Emergency Readiness Team (US–CERT).

Support to Infrastructure Protection

Through analysts assigned to HITRAC, I&A has provided regular, steady-state, and incident-specific classified and unclassified briefings and reports to Federal, State, local, and private sector critical infrastructure protection community members; supported the development of the annual National Risk Profile included in the Congressionally-required National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report; and participated in exercises designed to improve public

and private sector responses to current and emerging threats to critical infrastructure. Recent examples include supporting the July 2010 tabletop exercise on reducing the vulnerability of the U.S. food supply to intentional contamination and subsequent Infrastructure Protection Note, as well as a May 2010 five-city classified briefing series on the Nation's evolving threat picture to State and local critical infrastructure partners.

I&A further supports IP's efforts to build critical infrastructure expertise in State and local fusion centers. For example, I&A and IP are jointly conducting a training course for State and local fusion center infrastructure analysts to provide them with an overview of risk analysis trade-craft, including threats to critical infrastructure. I&A and IP are also collaborating to support an exchange program that brings State and local fusion center infrastructure analysts to Washington, DC for threat briefings and training—an iteration of this program is occurring this week. Most recently, I&A and IP held a joint annual meeting for I&A's fusion center analysts and IP's field-deployed Protective Security Advisors to facilitate collaboration and mutual awareness.

I&A and IP work together on additional specialized projects and programs. For example, they are collaboratively developing infrastructure sector-specific intelligence requirements and a comprehensive information requirements process, which will further improve the ability of I&A and the intelligence community to meet the information needs of the Nation's critical infrastructure community. I&A works closely with IP's Office for Bombing Prevention (OBP) on issues related to improvised explosive devices and chemical, biological, radiological, and nuclear (CBRN) and explosive threats, and supports IP's operational programs such as Enhanced Critical Infrastructure Protection security surveys at critical infrastructure facilities and the Regional Resiliency Assessment Program. I&A reviews and provides substantive comments on information reports derived from OBP's Technical Resource for Incident Prevention (TRIPwire), which describe terrorist use of bombs and Improvised Explosive Devices. I&A products are frequently posted on the TRIPwire portal for use by applicable stakeholders.

Support to Cybersecurity

I&A provides substantial and growing support to the cybersecurity and protection activities of the Department. This support includes tactical and strategic threat intelligence analysis for elements of NPPD's Office of Cybersecurity and Communications. I&A delivers tactical intelligence support—situational awareness and early warnings of potential cyber threats that combine all-source analysis with data from EINSTEIN sensors—to the National Cybersecurity and Communications Center (NCCIC), US–CERT, the National Coordinating Center for Telecommunications (NCC), and the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT). I&A publishes Homeland Information Reports derived from intrusion or other exploited cyber data, which identifies cyber-focused collection gaps and generates requirements based on these gaps. I&A further develops and delivers strategic intelligence products and services, such as assessments, briefings, and teleconference support, to numerous customers, including CIKR customers through Sector Coordinating Councils (SCC), Government Coordinating Councils (GCC), and State and local government authorities. These products can relate to cybersecurity or physical cyber-related infrastructure.

Office of Operations Coordination and Planning (OPS)

I&A has a mutually reinforcing relationship with OPS; I&A is the Department's primary intelligence element and OPS is responsible for maintaining full awareness of all DHS activities and relevant developments. I&A's primary support to OPS is in providing needed intelligence and information to the National Operations Center (NOC). I&A maintains an embedded classified-level watch and warning function at the NOC that serves as the immediate conduit for intelligence and information obtained from I&A's myriad customers.

I&A coordinates with OPS to address requirements for the Department's Single Point of Service (SPS) program. This program, consisting of elements from the NOC, I&A, and the DHS Office of Intergovernmental Affairs, processes support requests in a visible, transparent, and accountable manner. Support requests include requests from State, local, Tribal, and territorial partners for support to include Requests for Information, classification downgrades, on-site training, and briefing support. I&A ensures that support requests forwarded by the NOC conform to I&A's authorized missions, qualitative standards, and legal and regulatory requirements; protect individual privacy, civil rights, and civil liberties; are responsive to the requirements of I&A customers; and maintain the integrity of the Departmental intelligence process.

I&A directly supports OPS via its embedded Operations Intelligence staff. For example, our health intelligence team supported OPS' H1N1 Operations Planning Team during the H1N1 pandemic. More recently, I&A's Operations Intelligence staff and chemical and biological threats analysts were fully integrated into developing and implementing Departmental CBRN and health response plans. This was done in close tandem with OPS and other Department elements and components.

Even though the DHS Chief Intelligence Officer is the head of the Department's statutory program to support State and local fusion centers, OPS, mainly through the NOC, has key responsibilities in furthering the Department's commitment to sustain and support fusion centers. I&A appropriately coordinates with OPS in salient areas such as fulfilling support requests received from fusion centers.

Domestic Nuclear Detection Office (DNDO)

I&A provides strategic intelligence assessments that focus on threat actors, their claims, and their plans to attack the United States with radiological and nuclear materials. These assessments support DNDO's policymaking and resource planning efforts. In addition, I&A produces baseline and estimative intelligence products to enable Global Nuclear Detection Architecture (GNDA) planners to anticipate adversaries' future capabilities and intent and develop a better understanding of the future environment in which the GNDA will operate. I&A products support DNDO as the Departmental lead in developing the GNDA, which includes red teaming and reviewing deployment strategies.

Office of Health Affairs (OHA)

I&A's partnership with OHA entails close collaboration at multiple levels. I&A provides tailored monthly briefings for Assistant Secretary and Chief Medical Officer Dr. Alexander Garza to address his key intelligence questions. I&A produces intelligence analysis to meet OHA's unique information needs; for example, I&A recently provided tailored analysis and briefings to support OHA's BioWatch Program. I&A coordinates with OHA to provide the Secretary, DHS elements and components, and State, local, Tribal, territorial, and private sector customers with appropriate products that detail CBRN and health intelligence threat assessments, as well as related medical countermeasures and infectious disease mitigation techniques.

I&A and OHA collaborate closely on the Health Security Intelligence Enterprise (HSIE), a joint initiative to integrate the public health and health care communities into the Department's intelligence and information sharing programs and processes. The HSIE focuses on building multidisciplinary partnerships to facilitate a two-way flow of information among State and local health officials and the National network of State and local fusion centers. The on-going collaboration and coordination for the HSIE initiative represents a valuable partnership between I&A and OHA.

On the programmatic front, I&A coordinates with the National Biosurveillance Integration Center (NBIC) on a regular basis, participating in its daily biosurveillance teleconferences, providing salient finished intelligence products, and responding to NBIC's requests for information on disease events around the world. As part of this partnership, I&A provided the medical intelligence briefing for the inaugural Food Protection Workshop that NBIC cosponsored with the Federal Food Safety and Inspection Service (U.S. Department of Agriculture) this summer.

Office of Policy

I&A provides distinct intelligence support to DHS' Office of Policy in ensuring that its decisions and initiatives are informed by the latest intelligence and threat analysis. This includes focused support on counter-terrorism, watch-listing and screening, National and international information-sharing access agreements, Departmental strategic planning and risk management, and preventing the unauthorized acquisition or use of CBRN materials and capabilities. For example, we provided intelligence that supported Policy's involvement in the implementation of Executive Order 13546, "Optimizing the Security of Biological Select Agents and Toxins in the United States."

Multiple I&A divisions, including its Strategies, Plans, and Policy Division, Information Sharing and Intelligence Management Division, and its Border Security Division, work in close collaboration and cooperation with various elements within the Office of Policy. These engagements ensure that the decisions and initiatives of suboffices within Policy are informed by the latest intelligence.

Our program and intelligence analysts coordinate with the Office of Policy in addressing intelligence requirements for the Visa Waiver Program. Using the mandate from the 9/11 Act, the Director of National Intelligence designated DHS as the lead intelligence community entity responsible for biennial Visa Waiver Program assessments. We independently assess the integrity and security of travel processes and documentation for each country in or applying to the program to address the poten-

tial for illicit actors—including transnational criminals, extremists and terrorists—to exploit travel systems and the security environment that can facilitate unlawful access to the United States.

I&A, as the statutory lead for establishing intelligence policy for the Department's intelligence enterprise, ensures appropriate coordination with the Office of Policy in all our intelligence and information sharing activities. I&A provides direct intelligence policy input to the formulation of Office of Policy strategies and initiatives, such as those associated with our Southern and Northern borders, counterterrorism, screening coordination, and information-sharing with U.S. and international partners.

Office of Security

I&A provides significant support to the Office of the Chief Security Officer on a variety of issues, including the development of implementation guidelines for Executive Orders impacting classified information management. Other pertinent collaborative activities include the issuance of security clearances to non-Federal partners and building and accrediting Sensitive Compartmented Information Facilities, or SCIFs.

Office of Counternarcotics Enforcement (CNE)

I&A provides CNE with analytic and intelligence support for its efforts to coordinate DHS responsibilities to stop the entry of illegal drugs into the United States, and track and sever the connections between drug trafficking and terrorism. I&A is a member of the CNE-led Counternarcotics Coordinating Council, a body that coordinates Department counternarcotics policy and operations.

I&A provides substantial support to the development of National and DHS counternarcotics strategies. Significantly, I&A served as a co-chair, along with the U.S. Drug Enforcement Administration, of the interagency effort to develop the intelligence and information-sharing chapter in the 2009 *National Southwest Border Counternarcotics Strategy.* I&A is responsible for tracking over 100 such interagency initiatives alongside CNE, and is currently assisting CNE in the development of a DHS strategy to combat the links between drug trafficking and terrorism.

I&A supports CNE with subject matter expertise on drug trafficking trends along our Northern and Southern borders, serving as CNE's link to the intelligence community for obtaining information and intelligence on the threats posed by international drug trafficking and on the connections between drug trafficking and terrorism. I&A works closely with CNE to ensure that its information needs are incorporated into the DHS Standing Information Needs (SINs). DHS SINs identify the universe of enduring intelligence needs of the Department, and allow the DHS Chief Intelligence Officer to focus collection, analytic, and reporting activities and efforts based on the distinct needs of the Department and its customers. I&A also facilitates CNE's requests for information to the intelligence community on international drug trafficking and drug-terror nexus issues.

OTHER AREAS OF INTERACTION WITH DHS HEADQUARTERS ELEMENTS

National Security Systems

I&A management of the DHS National Security Systems (NSS) Program provides a significant enabling capability to Departmental decision-makers, including in headquarters elements. The NSS is a joint initiative between I&A and the Office of the Chief Information Officer (OCIO). The Deputy Secretary chartered the NSS in January 2009 to bring a One DHS approach to the management of all classified information technology infrastructure provided by DHS, including networks, secure communications, and enterprise services. This joint initiative institutionalizes a strong mission partnership between OCIO and I&A in the relatively small and specialized—but critical—area of classified information technology capability.

The NSS Program provides clear benefit for DHS headquarters elements, as well as operational components, to ensure their users have appropriate access to classified information technology infrastructure, such as the Homeland Secure Data Network. These benefits include consolidated, enterprise-level management of all classified information technology services; strengthened alignment to Departmental and component mission priorities; coordinated investments for efficiency and interoperability; and improved service delivery and transparency.

Intelligence Training

I&A supports DHS headquarters elements by offering many intelligence tradecraft and other related training multiple times each year. Intelligence training is a critical capability that enables fulfillment of the Department's intelligence mission. We are building on existing intelligence training successes and expanding this

program to establish a culture of disciplined and uniform intelligence capabilities throughout the Department. Strong intelligence tradecraft across the Department serves the dual purpose of making headquarters consumers of intelligence more informed of what intelligence can—and cannot—provide to DHS decision-makers.

STRENGTHENING INTERFACE

In preparing for this hearing, I identified several areas in which I&A can improve its support to DHS headquarters elements. We are making strides in how we provide the Secretary and Deputy Secretary tailored and timely all-source intelligence briefings. We have engaged key decision-makers across the Department and asked them how I&A can better fulfill their requirements. I have found the feedback from these inquiries to be both helpful and substantive.

I&A has used this feedback to accelerate understanding of Departmental policy deliberations and the programmatic activities of DHS headquarters elements. Stronger insight by I&A into Departmental policy and programmatic matters will make us more attuned to the needs of our customers, and thus more focused on the core intelligence questions and needs of DHS decision-makers.

CONCLUSION

Members of the subcommittee, I appreciate the opportunity to appear before you today to discuss how I&A supports and coordinates with headquarters elements within the Department. I&A has made significant strides, and continues to adapt to the current and emerging needs of our partners and customers across the Department. I&A has a vital and unique mission and continues to improve its strategic posture to more effectively support core customers, including DHS headquarters elements.

I&A's efforts to manage, collect, analyze, and share intelligence and information will continue to be guided by the dual imperatives of protecting the country from those who wish to do us harm, and protecting the privacy, civil rights, and civil liberties of our citizens. With your support, the leadership of Secretary Napolitano, and the fine men and women of I&A, I believe we can accomplish our multi-faceted mission and help DHS headquarters elements accomplish theirs. I look forward to keeping the subcommittee and Congress apprised of I&A's continued progress in this important area, as well as our progress in leading and strengthening the critical intelligence mission of the Department.

Thank you for your time, and I look forward to your questions.

Ms. HARMAN. Thank you for your testimony. Let me say for the record that other Members of the subcommittee are permitted to submit opening statements for the record. None of them is here at the moment, but they can do this at a later time.

[The statements of Chairman Thompson and Hon. Richardson follow:]

PREPARED STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

I have been a vocal critic of the way the intelligence community interacts with other agencies outside of their community.

This is the sort of conversation I have heard, and I am confident you have heard it, too, when people are talking about sharing information:

- "What do you have?" "What do you need?"
- "How do I know what I need if you don't tell me what you have?"
- "How can I tell you what I have that can help you, if you don't tell me what you need in the first place?"

And so on.

In the end, those outside of the intelligence community do not know what the intelligence community has and those inside the intelligence community do not have a clear idea of what everyone else needs.

The same thing seems to be happening inside DHS, with offices and agencies throughout the Department needing intelligence but not getting it from I&A—and I&A having intelligence that could be useful to these offices and agencies, but not knowing that they need it.

The way I see it—as a leader—there are some common sense actions that the Under Secretary for Intelligence and Analysis needs to take so that the Department can become more efficient.

First, you need to find out who needs what intelligence, and where they are getting it from, if anywhere.

The answer to that question is pretty clear when it comes to the other intelligence elements in the DHS components, but not so for the headquarters elements.

Second, you need to identify which DHS activities are lacking critical intelligence. I realize this sounds difficult, but it just means taking the time to get to know other people and other organizations, and helping them to see what you can provide.

Third, you need to open your own doors and allow others in, so they can see what you have and determine what might be useful.

I am not talking about sharing intelligence with people who may or may not have a need-to-know. But I am talking about sharing enough information with people so that they can at least try to match their needs with your capabilities.

I do not believe this should be a very difficult outcome to achieve.

For example, every entity within the Department that creates a terrorism risk assessment (such as DHS S&T) should be getting intelligence from or through I&A.

The same holds true for those creating risk assessments and making risk-based decisions (such as the Office of Health Affairs deciding where BioWatch detectors should be emplaced throughout the Nation, based on risk).

I am sure you agree that words and phrases like "threat assessment," "terrorism risk assessment," "threat determination," and "intelligence policy" are pretty obvious indicators.

Under Secretary Wagner, I realize that this is not all on your shoulders. Granted, you have a lot of intelligence professionals working for you, but you should not need for them to have to use their spook skills to find out what is going on in the other headquarters elements.

Secretary Napolitano has a responsibility to act as well. She needs to require every entity in the Department that has any need for intelligence to work with I&A—and for I&A to work with them.

But it is up to you and your peers to make it happen—connecting the dots between intelligence and information sharing.

PREPARED STATEMENT OF HON. LAURA RICHARDSON

SEPTEMBER 29, 2010

Mr. Chairman, thank you for convening this hearing today focusing on the extent to which the Department of Homeland Security's Office of Intelligence and Analysis interacts with other headquarters' elements within the Department. I would also like to thank the Honorable Caryn Wagner, DHS Under Secretary for Intelligence & Analysis and Chief Intelligence Officer, for appearing before the committee today to discuss these very important issues.

The Department of Homeland Security's Office of Intelligence and Analysis (I&A) plays a dual role in ensuring the security of the homeland. First it is charged with collecting and analyzing intelligence information. Second, it is responsible for disseminating that information to departmental units and with intelligence-related functions or activities.

As we've learned from experience, the gathering and sharing of intelligence within and across units of Government is critically necessary to protect this country from potential terrorist attacks. From the failed Times Square car bombing that led to the apprehension of Faisal Shahzad to the disrupted plot to attack New York's subway system, the sharing of information among our intelligence agencies has been, and will continue to be, a crucial tool in either preventing terrorist plots or providing the necessary information to making sure similar plots will not be successful in the future.

However, there continue to be a number of issues with I&A that urgently need to be addressed. For example, it has been documented that where headquarters have not received intelligence by I&A in a timely manner, they have reacted by attempting to obtain it on their own, or develop their own sources, or use open source information that is often unreliable or incomplete. Thus, it is very important to for us to evaluate the timeliness, method, and adequacy by which I&A responds to the legitimate intelligence needs of its headquarters.

I have a special interest in this subject because my district, the 37th of California, contains a number of high-profile airports, rail lines, and refineries that could be considered potential targets for would-be terrorists. Thus, the ability of DHS to communicate and share intelligence effectively is not only critically important to me, but also vital to ensuring the security of the American people.

I am pleased that Chairman Thompson convened this hearing because it provides an opportunity for committee members to understand and evaluate the current state of information sharing within the intelligence enterprise of DHS.

I am particularly interested in discussing at length with the under secretary the ways and means she has identified in strengthening the capacity and performance of I&A.

Thank you again Chairman Thompson for convening this hearing. I yield back my time.

Ms. HARMAN. I thank you for your testimony, and just would note every time I hear the words "DHS Intelligence Enterprise," I think of a battleship in a sci-fi movie. A lot of big words and a lot of huge acronyms. What we are trying to get at, just to be very clear, is whether you are a leader across these elements in this battleship, and are able in real-time to get critical intelligence to the right folks so that it can be used correctly in time to prevent and disrupt plots. That is what we are after. We are not after memorizing an org chart, and we that are not trying to force you to memorize the org chart either. We are trying to be sure you are in a position to lead on intelligence and analysis issues in the departments of Homeland Security. Are you?

Ms. WAGNER. Yes, ma'am, I am, and I think people are looking to me to do that. I am trying to lead the intelligence elements of the Department, to make sure that we are all working together, that we are sharing all the information so that every element the Department is receiving from their intel support people the same information that they can use in their operational missions.

So I would say that I lead the intelligence elements of the Department, but for the other, the operational components and the headquarters elements, I am in a supporting role which I think is appropriate, making sure that they have the information they need to do their missions. So it is a symbiosis, and I think that that is working better. They are more frequently looking to me for that.

Ms. HARMAN. That is what we want to hear. They need to be looking to you. You need to have a seat at all the relevant tables, as the jargon goes, and to make certain that you are respected and consulted, and have input into other elements of your Department that deal with intelligence, right?

Ms. WAGNER. Yes, ma'am, and I feel that that is the case.

Ms. HARMAN. We are trying to help you get there because our goal is not to play gotcha. Our goal is to make certain that you are performing at full capacity so that the I&A function horizontally is what it needs to be, and we are pleased to see its performance vertically improving now that we have someone with a law enforcement background as your deputy.

I want to ask about two current events and just test you a little bit here. If we have time, I want to ask you one wonky organizational question.

The Cyber Storm III exercise is being held this week. Is I&A contributing intelligence analysts to this exercise? Tell us about how you are doing this and your efforts to address the threat of cybersecurity in coordination with other offices within DHS. That is my first question, and I will put them both out so you can answer them both.

Second, news reports as recent as last night, and maybe even today, have made public a terror plot in the United Kingdom and

perhaps in France and Germany in which small teams of terrorists plan to seize and kill hostages similar to the Mumbai attacks in 2008. How have you or do you propose to work with your partners within DHS headquarters to inform and respond to this new development?

Ms. WAGNER. On the Cyber Storm exercise, I am actually attending that tomorrow afternoon, which should be extremely interesting. The analysts that I referred to who are embedded into the NPPD cyber organization have been active participants in developing and implementing this exercise. I and the Chief of my Cyber Analytic Branch, routinely attend the cyber jam sessions that are hosted by Phil Ridinger, who works for Rand Beers, as you know. So I feel we are extremely integrated into this; and, yes, we did participate in the development of the exercise.

On item No. 2, I cannot really confirm anything about what is in the press, which I know will not surprise you because we don't want to compromise or undermine any on-going intelligence activities. I can assure you that we are actively engaged in monitoring on-going threat activity, of which there is always a significant amount, and are working very closely with other elements of the intelligence community and within the Department and with our foreign allies.

We have instituted, just in general, some procedures for ensuring that we are delivering up-to-date intelligence to all members of the headquarters elements. We are now scheduling weekly briefings for all of the key staff elements in addition to having weekly video teleconferences with the components to ensure that we are all on the same page.

So I think we have taken a lot of steps recently to make sure that everybody is in sync.

Ms. HARMAN. I appreciate your care in answering that question. I too am not revealing anything that I have been briefed in a classified setting. But I just said that these news reports also say that the so-called storming operations could occur in the United States. That is your turf, and so I just wanted to be sure you are on it; and you are on it.

My final question. Why aren't any of the other headquarters elements recognized as critical members of the DHS Intelligence Enterprise?

Ms. WAGNER. That is actually a good question, ma'am. I think that they are, and I don't know if you are quoting from the 2008 Intelligence Enterprise.

Ms. HARMAN. That is our last Enterprise, the one with Charlie Allen's picture on it.

Ms. WAGNER. Exactly. We are in the process now of completing actually, and we hope to do so in October, a revised strategic plan. We actually had this conversation the other day, going, well, is it for I&A or is it for the Enterprise. My thought process is that since I am the Under Secretary and the CINT, that our strategic plan ought to be both for the I&A and for the Enterprise, and that should include not just the components but also the headquarters elements that we support.

So I am personally going to make sure that is the case when it is completed. But I do view them as part of the Enterprise. In fact, they are some of our most important customers.

Ms. HARMAN. Well, that is a great answer to my great question, and that is the way we hope you will be thinking about this. Please, no more stovepipes. I think we have had our fill of those. You need to act as the intelligence leader for the Department, obviously working for the Secretary, but the intelligence leader who is involved in all of the active problems out there that could lead to harm of our citizens and our communities. We see you as a very key player here, and we are holding this hearing to make certain that you understand how we view your role and that you take your vitamins.

I now yield to the Ranking Member for his questions.

Mr. MCCAUL. Thank you, Madam Chair.

I think you addressed this in your testimony, but on the vertical information sharing, we were just getting some reporting from some of the fusion centers that DHS was going around it and maybe going straight to the State homeland security coordinator, but you are aware of that and you have taken action to address that?

Ms. WAGNER. Yes. We are trying to synchronize all of those interactions through our State and Local Program Office, and there are a lot of on-going relationships with State and local governments that elements have that have gone back for quite some time. So it is well meaning and we just need to make sure that we are all aware so that we are not coming at the States from multiple, different uncoordinated directions. We are trying to achieve that. I can't claim that we are 100 percent effective yet, but it is steadily improving.

Mr. MCCAUL. That is good to hear.

On the horizontal information-sharing side, I think the last time you testified we talked a little about the National Fusion Center Program Office, and I understand since that time the appropriators have denied that reprogramming. So I was just curious as to what the Department is doing to move forward on that.

Ms. WAGNER. Actually, I appreciate the opportunity to answer that question.

Mr. MCCAUL. Thanks.

Ms. WAGNER. We sort of pitched a concept that was based on the fact that we had two related but distinct responsibilities to fulfill. One was, as you all are terming it, the horizontal sort of relationships within the Department, again addressing your issue, making sure that we are coordinating all Departmental interactions with State and local governments through the fusion centers, and that was going to be the Joint Fusion Center Program Management Office. The National Fusion Center Program Management Office was going to address the larger whole of Government coordination responsibilities that we were assigned by the White House, to include working with the FBI and ONDCP and others.

We still have those two functions to fulfill. We understand that the proposal we made looked overly bureaucratic. So what we have done to move ahead is we have combined those two functions in one office with shared infrastructure, and so it will be a more

streamlined, leaner effort. But we will continue to fulfill both of those sets of responsibilities. At the moment it is still being called the State and Local Program Office, which is what it was before. We are exploring with our Congressional oversight committees whether we could possibly change the name, possibly to the National Fusion Center Program Management Office, but we will have those conversations so that we are completely in sync with our overseers.

Mr. MCCAUL. I guess the appropriators' concerns were that it was two different offices, maybe it was duplicative and it was costing too much money, was that their concern, and your response was to put it within one office?

Ms. WAGNER. I do think that was part of their concern. Also, I am not sure that we explained it completely. We have had subsequent conversations with everybody, and I am hoping that we are all in agreement that the way forward we proposed makes sense.

Mr. MCCAUL. I was looking at the diagram of the DHS Intelligence Council. I think I mentioned this in my opening statement. One entity that is not in here that I was a little surprised with was the cyber piece. Why is that not included in this organizational chart?

Ms. WAGNER. Probably also a good question. Our relationship with NPPD tends to focus mostly on infrastructure protection, and so they are in fact at the table and we do occasionally discuss the issues and they basically represent NPPD at the forum. They are welcome also if there is a cyber-related topic on the agenda, to bring anybody that they would like with them to the HSIC. In fact, we frequently have sort of guest attendees at the HSIC. But I may in fact ask that question myself when I get back.

Mr. MCCAUL. One other entity, the S&T, Science and Technology, is doing threat assessments as well, I saw. I was kind of curious why they are doing that; and if they are, why aren't they part of this as well?

Ms. WAGNER. I am not aware that they are doing threat assessments per se. I may have to take that one for the record.

Mr. MCCAUL. The information I have is that they are. You may want to take a look at that.

Ms. WAGNER. We work with them to do threat assessments that they put out. They do sort of risk assessments in some areas, and we always provide the threat piece of a larger risk assessment. So if that is—and we do interact with S&T and with Health Affairs on those types of risk assessments. I don't think of them as being threat assessments, I think of them as being risk, which as I mentioned before combines the threat vulnerabilities and consequences, and we do participate in those.

Mr. MCCAUL. On infrastructure protection in the private sector, particularly in cyber, the cyber world, that has been very difficult. The ISACs, the Information Sharing Analysis Centers, are out there. Can you give me an update on where the Department is with the sharing of critical information sharing with the private sector for infrastructure protection?

Ms. WAGNER. Generally speaking, we, I&A, partner with Infrastructure Protection to provide information on critical infrastructure, including cyber infrastructure, to the private sector. We do a

lot of that through the Sector Coordinating Councils and other existing mechanisms, such as involving DSACs, Domestic Security Adviser Councils. We also do a lot of table top exercises and those kinds of activities with the private sector to try to help them understand the nature of the threat and terrorist tactics, techniques, and procedures, to help them work through some of these issues. We have recently done one with the hotel industry. In fact, I think we did two. We put a product on that topic as well. Basically, again, we teamed with infrastructure protection to provide the threat and vulnerability information, and then we get the information out, either through written products, conferences, telephone conferences, or some of these exercises that we run and invite key representatives of the various sectors.

Mr. MCCAUL. Is there a two-way flow of threat information between DHS and the private sector and vice versa?

Ms. WAGNER. I think the answer to that is yes, although the flow back to DHS I think is less developed, as it is sort of across the board. We are working with the FBI on the Suspicious Activity Reporting Initiative, which I am sure you are aware of, which would also pertain to the private sector and in fact the public at large. So we are hoping to get more information as that becomes more socialized. So yes, we do get information.

Mr. MCCAUL. What are some of the obstacles that you see that prohibit or discourage the private sector from sharing this information with you?

Ms. WAGNER. I think probably the fact that the private sector is just so large that—I will frequently hear from people, well, the private sector is saying you don't share anything with them. We are trying to increase our level of interaction with the private sector, but it is so huge that you are unfortunately impacting only a small percentage. I think part of the real challenge is just educating them on what we can do and making sure that they know where to come into the Enterprise, if you will, if they have information. They are always free to go to their local fusion center, directly to the JTTF with terrorist information, but we also need to make it clear that there are other avenues for them and educate them. I think that the sheer magnitude of building that relationship is a challenge.

Mr. MCCAUL. Okay. That is all I have.

Ms. HARMAN. Thank you. If you have another question, feel free to ask it. I have one more question and one observation.

I will make my observation first, which is that the key ingredient is leadership. It is not the org chart, but I appreciate the Ranking Member's additions to your org chart. But it isn't the org chart, it isn't the underlying law, it is leadership. As you well know, threats against us are evolving, and while the best we can do is to manage risk, and I agree with that, what risks we manage have to be reconsidered all of the time. So you need to lead the Intelligence Enterprise of the Department of Homeland Security, and that is our hope and expectation.

In that regard, my last question is: Do you need anything from us?

Ms. WAGNER. I really appreciate this committee's support. I think that is all I need, and I feel I am getting it. I feel you all

are clearly motivated to help us succeed, and believe me, that is very much appreciated.

Ms. HARMAN. I appreciate your answer. If you lose, we all lose. Let's understand that. We are in this together. Now my rather old sound bite is the terrorists won't check our party registration before they blow us up. We really are in this together.

So I appreciate the fact that the Ranking Member works closely with me on these things, and I don't think we have had a disagreement about the course or agenda of this subcommittee, not even one.

Let me yield to him for a final thought or observation or question.

Mr. MCCAUL. Thank you, Madam Chair. I also appreciate our close working relationship.

You know, this is a little bit off topic for this hearing, but since we have you held hostage for at least 30 minutes, I am becoming increasingly more concerned not so much about command and control of al-Qaeda, or the threat coming from there, but more these sort of franchise operations, but even more so—and we had a couple of hearings on this, and I appreciate Madam Chair doing it—on internet radicalization. I am becoming more and more concerned about disenfranchised Muslims or even some non-Muslims, people getting on the internet, listening to someone like Awlaki or talking to him like Mr. Hassan did, and suddenly radicalizing and then we have an act of terrorism.

Can you touch that at all or discuss if you see that threat becoming increasingly more of a threat?

Ms. WAGNER. I think we are concerned that that is becoming more of a threat, and the intelligence community is focused on what more can we do to understand the process of radicalization in order to do really two things, to help law enforcement in our communities identify and possibly interrupt that process and also to advise the policy community on what types of engagement or policy interventions might actually be effective.

In the wake of the Christmas day bombing, Rudy and I tasked my office to lead an interagency effort with FBI and NCTC to try to improve our analytic understanding of this problem.

Since the last time I spoke to you, we developed and incorporated an action plan with the community. We did receive some money from the DNI to do this, and we have worked on a series of case studies for some of the people that have been radicalized and performed violent acts that we are now going out and discussing with our partners in the fusion centers and our State and local law enforcement folks, to say, okay, here is what we found out, is this useful to you? What more can you add? Particularly in areas where there may be communities about which the local law enforcement people know a lot and can give us information.

We are also working closely with our allies who have experienced some of these problems to ensure that we understand what their best practices are, both analytically and in things like community policing, those kinds of issues, and obviously with academia as well, because this is partially an intelligence problem and partially a human behavior problem.

I don't want to minimize the difficulty of understanding why some people who are radical or have extremist views—and that is not illegal—take that next step and go into violent manifestations of those views. Difficult to predict, and very difficult to predict if they are sitting in their basement on the internet.

Mr. MCCAUL. One of the magazines, I think it was Inspire——

Ms. WAGNER. Inspire.

Mr. MCCAUL. They had how to make a bomb in your mom's kitchen. I showed it to a group back home, a video of Awlaki I think is on the internet, and they weren't as concerned with him as much they were with the rap video that was very disturbing. That is a clear effort to recruit in sort of a totally different way, that is trying to cater to maybe a younger audience and trying to—you know, it is sort of a hip-hop rap-type video.

Ms. WAGNER. There is clearly an effort to reach out in ways that are consistent with pop culture and that will appeal to people of a certain age and background, so that is a concerning developing. But we are working on this, but it is a difficult problem.

Mr. MCCAUL. Thank you.

Ms. HARMAN. Well, we are working on it, too. We have had a series of careful hearings on this. This rap video and some of these other things were shown to us at one of our hearings.

I would just underscore something you said, Secretary Wagner, which is that radical views are protected by the First Amendment. The forming of our Republic, in many ways, was a radical act. What we are concerned about is that line between holding radical views, which is protected, and engaging in violent behavior, which is illegal.

We are obviously trying to understand what takes a person into that second box. It is a complicated subject and one size does not fit all, but it is urgent business for the United States of America. I think we all agree on this.

I want to thank you for your valuable testimony and thank the Ranking Member for his insightful questions.

As I have mentioned, the Members of the subcommittee may have additional questions for the witness, and we will ask other questions of these elements inside the Department of Homeland Security with which you interact so we get a full picture of these relationships.

We would ask that you respond, that you and they respond expeditiously in writing to those questions. I assume that is acceptable to you.

Ms. WAGNER. Yes, ma'am.

Ms. HARMAN. Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 4:50 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF INTELLIGENCE AND ANALYSIS

Question 1. What do you want your legacy to be when you leave I&A, as far as the rest of the Department is concerned?

Answer. Response was not received at the time of publication.

Question 2. What do you think can and should be done to improve connectivity between I&A and the other headquarters elements?

Answer. Response was not received at the time of publication.

Question 3. We recently learned from the Office of Operations Coordination that I&A often provides a classified annex for their planning documents. Does intelligence from I&A inform all levels of the planning process at DHS?

Answer. Response was not received at the time of publication.

Question 4. Which headquarters elements does I&A interact with significantly? Please expand on what you submitted in your written testimony regarding these interactions.

How does I&A track its interaction with these elements?

Answer. Response was not received at the time of publication.

Question 5. How does the strategic plan for the DHS Intelligence Enterprise address the needs of the headquarters elements?

Do you have processes in place to continuously identify needed improvements and changes to the products and services I&A provides to the headquarters elements?

How important is collaboration with the headquarters elements when it comes to DHS intelligence processes?

Answer. Response was not received at the time of publication.

Question 6. What information does I&A receive from the headquarters elements? What more do you need?

Answer. Response was not received at the time of publication.

Question 7. How can you as Chief Intelligence Officer (CINT), maintain insight into the intelligence needs of non-traditional DHS partners, specifically those who are not formally part of the Intelligence Enterprise?

Answer. Response was not received at the time of publication.

Question 8. Are you confident that you have you identified all parts of DHS that need intelligence or conduct intelligence-related activities? Have you added them all to the DHS Intelligence Enterprise? If not, why not?

Answer. Response was not received at the time of publication.

Question 9. The DHS Intelligence Enterprise organizational chart has some solid lines and some dotted lines, which, according to the chart, indicate offices without key intelligence officials. Would you please expand upon the relationships shown in the chart?

Would you please explain why other DHS elements, such as the Office of Cyber Security and the Office of Health Affairs do not appear as part of the chart?

Answer. Response was not received at the time of publication.

Question 10. Do you believe that it is through your role as CINT or through your role at Under Secretary for Intelligence and Analysis, that you chair the Homeland Security Intelligence Council (HSIC)?

We have heard very good things from component members of the HSIC about the improvements you have made to the Council. Are all members of the HSIC—to include I&A, the components with larger intelligence functions, and those organizations connected by "dotted lines" on the chart—truly equal partners with equal voice? Would you please explain how you are able to ensure full partnership for all members?

Answer. Response was not received at the time of publication.

Question 11. Have you done a complete, end-to-end strategic analysis of all DHS intelligence and intelligence-related activities?

Answer. Response was not received at the time of publication.

Question 12. We have seen the charts showing I&A relationships. How well connected would you say I&A is to all of its Departmental partners? How could these connections be strengthened?

Answer. Response was not received at the time of publication.

Question 13. When organizations do not get the intelligence they need from others, they tend to try to create it themselves. What can I&A do to prevent this from happening in the Department?

Answer. Response was not received at the time of publication.

Question 14. We have seen the problems that I&A and IP have had being together and being apart, organizationally. Have these problems been solved?

What challenges remain with I&A working with IP?

Answer. Response was not received at the time of publication.

Question 15. Who is ultimately accountable for the Homeland Infrastructure Threat and Risk Analysis Center's analytic products, I&A or NPPD? Who publishes the products?

Answer. Response was not received at the time of publication.

Question 16. How well do you think the Homeland Infrastructure Threat and Risk Analysis Center is functioning? What are some areas could be improved?

Answer. Response was not received at the time of publication.

Question 17. In the military, S–2 (intelligence) is almost always paired with S–3 (operations). How is this working between I&A and the DHS Office of Operations Coordination?

Answer. Response was not received at the time of publication.

Question 18. A number of entities within DHS are creating terrorism risk assessments, including DHS S&T. Have you identified all of the DHS entities making similar assessments? Does I&A provide all of them with intelligence?

Answer. Response was not received at the time of publication.

Question 19. I understand that I&A participates in an integrated product team (IPT) to get its information sharing needs met. Would you please describe I&A's participation, and the benefits of your involvement?

Answer. Response was not received at the time of publication.

Question 20. The Office of Health Affairs (OHA) is currently responsible for producing an intelligence-based biodefense architecture. Can you offer some examples of the kind of intelligence that I&A could provide OHA to help in such an endeavor?

Answer. Response was not received at the time of publication.

Question 21. What is the nature of the medical intelligence that I&A provides to OHA?

Answer. Response was not received at the time of publication.

Question 22. The National Biosurveillance Integration Center is an OHA operational entity that uses a great deal of open source information. Do you think there are other types of intelligence that could be of value, which I&A is in a position to provide?

Answer. Response was not received at the time of publication.

Question 23. How does I&A support risk assessments with timely intelligence in various areas of the Department?

Answer. Response was not received at the time of publication.

Question 24. What is the relationship between I&A and the Office of Risk Management and Analysis?

Answer. Response was not received at the time of publication.

Question 25. In which DHS headquarters elements have you embedded I&A analysts?

Answer. Response was not received at the time of publication.

Question 26. It appears that there are three types of relationships that the Under Secretary for Intelligence and Analysis needs to manage: (1) Between I&A and the other members of the intelligence community; (2) between I&A and the other intelligence elements inside the DHS components; and (3) between I&A other DHS headquarters elements. How do you manage those relationships?

Answer. Response was not received at the time of publication.

Question 27. We understand that I&A is going to be developing intelligence doctrine for DHS. DHS may well be the only Department that is creating intelligence doctrine anew. What is the plan for developing this doctrine?

Answer. Response was not received at the time of publication.

Question 28. How does I&A facilitate relationships between non-intelligence organizations within DHS and intelligence organizations outside of DHS?

Answer. Response was not received at the time of publication.

Question 29. DHS, DOD, and the intelligence community are working on bioforensics right now. DOD aside, how is I&A helping to get the intelligence com-

munity to work with DHS—specifically with the DHS National Bioforensics Analysis Center?

Answer. Response was not received at the time of publication.

Question 30. Aside from going to meetings at the White House when he cannot, what kind of support do you, and the Office of Intelligence and Analysis provide to DHS's Chief Counterterrorism Official and vice versa?

Answer. Response was not received at the time of publication.

Question 31. In your testimony, you described how your customers for intelligence could be viewed as a series of concentric circles. How do you prioritize the sharing of intelligence with the private sector specifically, as compared with serving the needs of other DHS components or State and local governments?

How do you balance these competing interests in terms of resources? How many analysts do you have dedicated to the private sector?

Answer. Response was not received at the time of publication.

Question 32. Do you have standard operating procedures or protocols that govern the sharing of information with components and their respective customers and partners?

Specifically, is the way by which intelligence is shared with the private sector done in a consistent way, or is it determined on a threat-by-threat basis?

If it is not consistent, why not? And does this result in delays in the sharing of threat information with the private sector?

Answer. Response was not received at the time of publication.

Question 33. Is it the policy of DHS to put a priority on sharing intelligence with the private sector through fusion centers or through the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)?

Answer. Response was not received at the time of publication.

Question 34. How will I&A's reorganization affect HITRAC? Will HITRAC continue to be a priority after the reorganization?

Answer. Response was not received at the time of publication.

Question 35. What is your vision for HITRAC and in what way does HITRAC enhance your ability to support the private sector specifically?

Answer. Response was not received at the time of publication.

Question 36. How many staff does I&A have dedicated to HITRAC?

Answer. Response was not received at the time of publication.

Question 37. Does the Department include the private sector in determining collection requirements for intelligence?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF INFRASTRUCTURE PROTECTION

Question 1. What do you think can and should be done to improve connectivity between the Office of Infrastructure Protection and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Infrastructure Protection track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Infrastructure Protection obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. We have seen the problems that I&A and IP have had being together and being apart, organizationally. Have these problems been solved?

What challenges remain with I&A working with IP?

Answer. Response was not received at the time of publication.

Question 5. Who is ultimately accountable for the Homeland Infrastructure Threat and Risk Analysis Center's analytic products, I&A or NPPD? Who publishes the products?

Answer. Response was not received at the time of publication.

Question 6. How well do you think the Homeland Infrastructure Threat and Risk Analysis Center is functioning? What are some areas could be improved?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF OPERATIONS COORDINATION

Question 1. What do you think can and should be done to improve connectivity between the Office of Operations Coordination and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Infrastructure Protection track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Operations Coordination obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. In the military, S–2 (intelligence) is almost always paired with S–3 (operations). How is this working between I&A and the DHS Office of Operations Coordination?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE DOMESTIC NUCLEAR DETECTION OFFICE

Question 1. What do you think can and should be done to improve connectivity between the Domestic Nuclear Detection Office and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Domestic Nuclear Detection Office track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Domestic Nuclear Detection Office obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. How does I&A provide the intelligence community's "best judgment" to the Domestic Nuclear Detection Office regarding the terrorist nuclear threat to the Nation?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF COUNTERNARCOTICS ENFORCEMENT

Question 1. What do you think can and should be done to improve connectivity between the Office of Counternarcotics Enforcement and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Counternarcotics Enforcement track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Counternarcotics Enforcement obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. Does CNE get its intelligence regarding links between terrorism and narcotics from I&A?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF CYBER SECURITY AND COMMUNICATIONS

Question 1. What do you think can and should be done to improve connectivity between the Office of Cyber Security and Communications and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Cyber Security and Communications track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does I&A provide intelligence to the Office of Cyber Security? If not, why not?

Are I&A's cyber analysts co-located with other DHS cyber security analysts? How does their role differ from the work being done within the Office of Cyber Security?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF HEALTH AFFAIRS

Question 1. What do you think can and should be done to improve connectivity between the Office of Health Affairs and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Health Affairs track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Health Affairs obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. How could I&A help the BioWatch program improve its risk-based judgments of where to emplace detectors throughout the country?

Answer. Response was not received at the time of publication.

Question 5. OHA is currently responsible for producing an intelligence-based biodefense architecture. Can you offer some examples of the kind of intelligence that I&A could provide OHA to help in such an endeavor?

Answer. Response was not received at the time of publication.

Question 6. OHA is currently responsible for producing an intelligence-based biodefense architecture. Can you offer some examples of the kind of intelligence you believe that I&A could provide OHA to help in such an endeavor?

Answer. Response was not received at the time of publication.

Question 7. What is the nature of the medical intelligence that I&A provides to OHA?

Answer. Response was not received at the time of publication.

Question 8. Do you think there are other types of intelligence that could be of value to the National Biosurveillance Integration Center, that I&A is in a position to provide?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF POLICY

Question 1. What do you think can and should be done to improve connectivity between the Office of Policy and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Policy track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Policy obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE OFFICE OF RISK MANAGEMENT AND ANALYSIS

Question 1. What do you think can and should be done to improve connectivity between the Office of Risk Management and Analysis and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Office of Risk Management and Analysis track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Office of Risk Management and Analysis obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. How does I&A support risk assessments with timely intelligence in various areas of the Department?

Answer. Response was not received at the time of publication.

Question 5. What is the relationship between I&A and the Office of Risk Management and Analysis?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIR JANE HARMAN AND RANKING MEMBER MICHAEL MCCAUL FOR THE SCIENCE AND TECHNOLOGY DIRECTORATE

Question 1. What do you think can and should be done to improve connectivity between the Science and Technology Directorate and the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 2. How does the Science and Technology Directorate track its interaction with the Office of Intelligence and Analysis?

Answer. Response was not received at the time of publication.

Question 3. Does the Science and Technology Directorate obtain intelligence from members of the intelligence community without going through I&A in the first place? If so, why?

Answer. Response was not received at the time of publication.

Question 4. What is the nature of I&A input into the terrorism risk assessments conducted by the S&T Directorate? Aside from chairing the intelligence community advisory group for these assessments, does I&A provide any other input?

Answer. Response was not received at the time of publication.

Question 5. What kind of relationship has S&T had with I&A in developing I&A's next generation of intelligence information systems, such as HSIN 2.0?

Answer. Response was not received at the time of publication.