AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

MOVING BEYOND THE FIRST FIVE YEARS: EVOLVING THE OFFICE OF INTELLIGENCE AND ANALYSIS TO BETTER SERVE STATE, LOCAL, AND TRIBAL NEEDS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

APRIL 24, 2008

Serial No. 110–108

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

42–866 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
BILL PASCRELL, JR., New Jersey

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
TODD GEE, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chairwoman*

NORMAN D. DICKS, Washington
JAMES R. LANGEVIN, Rhode Island
CHRISTOPHER P. CARNEY, Pennsylvania
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DAVID G. REICHERT, Washington
CHRISTOPHER SHAYS, Connecticut
CHARLES W. DENT, Pennsylvania
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Director and Counsel*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Senior Professional Staff Member*

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 1
The Honorable David G. Reichert, a Representative in Congress From the State of Washington 2

WITNESSES

Mr. Matthew Bettenhausen, Executive Director, California Office of Homeland Security, State of California:
Oral Statement 5
Prepared Statement 7
Ms. Juliette N. Kayyem, Under Secretary for Homeland Security, Executive Office of Public Safety and Security, Commonwealth of Massachusetts:
Oral Statement 16
Prepared Statement 18
Mr. Frank J. Cilluffo, Director and Associate Vice President, Homeland Security Policy Institute, George Washington University:
Oral Statement 25
Prepared Statement 28

MOVING BEYOND THE FIRST FIVE YEARS: EVOLVING THE OFFICE OF INTELLIGENCE AND ANALYSIS TO BETTER SERVE STATE, LOCAL, AND TRIBAL NEEDS

Thursday, April 24, 2008

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 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Jane Harman [chairwoman of the subcommittee] presiding.

Present: Representatives Harman, Carney, Perlmutter, Reichert, and Dent.

Ms. HARMAN. The subcommittee will come to order. Good morning everyone. The subcommittee is meeting today to receive testimony on Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs. After a string of missteps by the current administration, the next one must get information sharing right. "Success" means figuring out what data to share, putting the technology in place to do so, and establishing the right rules for access. Of course, each step must happen within the bounds of privacy laws and constitutional protections. This is crucial, because it is unlikely that the next President, a DHS Secretary, FBI director or someone in the wider Intelligence Community will prevent the next terrorist attack.

Instead, a diligent police or sheriffs officer somewhere in America during the course of his or her daily work will see something or someone out of place and guided by timely, accurate and actionable information will connect the dots that will unravel a plot in the making. My ranking member did something just like that, it wasn't a terror plot, but it was a very serious crime in his area some years back.

To this end, this subcommittee has made it an imperative to improve intelligence and information sharing for our first preventers. If we don't make it work for these people and for the State Homeland Security advisors who work with them, some of whom are facing me, then we will have failed to do what we set out to do 5 years ago in the Homeland Security Act. As the Department of Homeland Security faces its first Presidential transition, we find its Office of Intelligence and Analysis at a crossroads.

DHS has taken positive steps to forge a more constructive and responsive relationship with State, local and tribal customers it serves. Positive steps have been taken. In Minneapolis, on a Monday, for example, I learned from MNJAC, the Minnesota Joint Analysis Center of a weekly conference call from DHS to link Fusion Centers together. This is very positive. Unfortunately, we never heard about it from DHS, but one of the local Fusion Centers.

But on the other hand, it has been a struggle to integrate fully local law enforcement representatives into the Interagency Threat Assessment Coordination Group or ITACG. The Department and specifically, the Office of Intelligence and Analysis, seems to have pursued a variety of missions without a clear focus.

In my view, this is not entirely the Department's fault. What was originally envisioned by many of us who were co-authors of the legislation as a robust intelligence shop for the Department in 2002 was restructured by President Bush in 2003 when he set up the Terrorist Threat Integration Center, TTIC, later to become the National Counterterrorism Center, outside of DHS.

Having lost the key function shortly after its creation, I&A has struggled to redefine its intelligence mission. It advertises itself as the primary provider of Federal Homeland Security information to State and local customers, claim to go create a new kind of Homeland Security intelligence.

I&A also claims to play the role of educator, rolling out a basic level intelligence training course for department intelligence analysts and their State and local customers with mid- and senior-level courses on the horizon. But the aggressive schedule that Under Secretary Allen and his team have described of deploying department analysts and liaisons to State and local Fusion Centers around the country has so far been only moderately successful.

In addition, in my view, DHS has approached management of the National Applications Office, the NAO far too casually. Let me be clear, as a member who has fought for years to assure that foreign intelligence surveillance complies with strict legal safeguards, I will not permit the Department to task the Nation's spy satellites for domestic purposes unless and until it provides a clear legal framework to Congress.

It is our job today to assess the Department's progress and to help the next administration get it right. The witnesses before us, all of whom are good friends of mine, and I am so happy to see you all hail from State government and academia. Each will address how DHS and its intelligence shop can make improvements to get it right now and after January 20, 2009.

I hope the Department of Homeland Security is listening. The benchmarks that the witnesses describe for us today will guide the oversight work of this subcommittee for the remainder of this session and through the transition to next year. Let me welcome you and tell you how pleased I am that you are here and how important this hearing is, and I now yield to the ranking member for any opening remarks.

Mr. REICHERT. Thank you, Madam Chair. Good morning, and thank you for taking some time to be with us this morning. I just came from a briefing down the hallway on the upcoming Olympics

in Canada, just above the Washington, Canadian border. So my district is east of Seattle so it is of interest to me.

This morning they talked about, you might be familiar with some of the terminology that we are using here in the U.S. integrated security, and an integrated planning, a partnership between the State's officials, the local officials and the RCMP and Federal. I have had opportunities to work with most of those in my previous career. So we are not the only ones trying to work on this and find the answers to gathering people together to protect the citizens of the United States, and of course, the citizens of Canada, who are our good friends.

Today's hearing is a part of a series of hearings—Moving Beyond the First Five Years. The theme is about improving the Department's efforts to secure our homeland through integrated cooperation. I believe that is why and what we in the Department are working to do everyday. I want to thank you and all the members of the Department of Homeland Security for what you do each and every day to keep this Nation safe.

While the first 5 years, the Department has seen some uneven progress and that is to be expected, the fight against terrorists has not been without success. The Department and Federal agencies have made significant progress in information sharing and standing up such institutions as the National Counterterrorism Center, NCTC, partially because of these efforts are Federal, State and local governments have been successful at preventing planned attacks on the United States and against the United States's interests.

Aside from the obvious successes there have been substantial internal improvements over the years at DHS and in the Office of Intelligence and Analysis. While examining this process, it is important to note that this is an office that was created from scratch 5 years ago and was substantially reorganized just 2 years later.

Additionally, last year, this office was again given new direction in the 9/11 Commission Recommendations Act. In other words, after being created from scratch, the office was reorganized and then subjected to major legislation. According to a press release from Chairman Thompson these series of hearings are also focused on preparing for the next administration and the future of the Department.

It is clear to me that what the Office of Intelligence and Analysis needs is to have some time to focus on its core mission without another major reorganization by the next administration. The Department of Homeland Security has a clear State and local mission, and must have some stability in order to ensure these missions are carried out.

One thing that Congress should do to help the Department of Homeland Security with their mission is to consolidate oversight with over 80 committees and subcommittees that have oversight, over components at the DHS, it is a wonder that the Department of Homeland Security has been able to achieve anything over the past 5 years.

While this subcommittee has been working to oversee some of the legislative improvements that we recently implemented, the Department is looking internally at its own flaws. One example of

this that is often cited is CENTRA, the CENTRA Report, that was commissioned by Under Secretary Allen himself to help improve the Office of Intelligence and Analysis' outreach and service to the State and local communities.

Furthermore, Under Secretary Allen recently began the Homeland Security State and local community of interest which is a virtual intelligence group that has won praise within the State and local community as major improvement in information sharing. While these are but a few recent efforts, I would like to hear today from our witness on improvements that they have seen and what improvements still need to be made.

Thank you again for being here, thank you, Madam Chair for the time and I yield.

Ms. HARMAN. I thank the ranking member. Other members of the subcommittee are reminded that under the committee rules opening statements may be submitted for the record.

It is now my pleasure to introduce our witness. Our first witness, Matt Bettenhausen, is the Homeland Security security advisor to California Governor Arnold Schwarzenegger and is the director of the California Office of Homeland Security. He previously served as the Department of Homeland Security's first director of State and territorial coordination where he directed the Department's efforts with State, territorial and tribal governments.

He served on several White House senior policy coordinating committees and worked on implementing Homeland Security presidential directives. From January 2000 to January 2003, Mr. Bettenhausen served as the deputy governor of Illinois. As that State's Homeland Security director, he is someone I work with often and enjoy. I would love to report to everybody that California is a bit safer because Matt is in the position that he is.

Massachusetts is fortunate that our second witness, Juliette Kayyem, who just completed the Boston Marathon in a little over 4 hours—that makes me upset—is the first Under Secretary for Homeland Security for the Commonwealth. She serves as the liaison between the Governor's Office and all Federal, State and local agencies on Homeland Security. She is responsible for developing State-wide policy with a focus on preventing, protecting, responding to and recovering from any and all critical incidents. She also has direct oversight over the Massachusetts National Guard.

Ms. Kayyem comes from her position from Harvard's John F. Kennedy School of Government, where she has been a lecturer in public policy. Since 2001, she has been a resident scholar at the Kennedy School's Belfer Center for science and international affairs, serving most recently as executive director for research. She is an expert in homeland security and terrorism, I know this, and teaches courses on law, homeland security and national security affairs.

She and I served together on the National Commission on Terrorism, which before 9/11, reviewed how the government could prepare better for the growing terrorist threat and predicted a major attack on U.S. soil which sadly came to pass.

Our third witness, Frank Cilluffo, who is here with his daughter, on Take Your Daughter To Work Day—Where is his daughter? We want to welcome you—He leads George Washington University's

homeland security efforts on policy, research, education and training. He directs the Homeland Security Policy Institute, which has a research agenda that has spanned domestic terrorism radicalization, disaster management, emergency preparedness, pandemic influenza, intelligence and information sharing. Along my travels in the security field, he is someone who is always part of the panels we put together to try to learn the subject matter better.

Mr. Cilluffo joined GW in April 2003 from the White House where he served as special assistant to the President for Homeland Security. Shortly after the 9/11 attacks he was appointed by the President to the newly created office of homeland security and served as the principal advisor to Governor Tom Ridge.

Prior to his White House appointment, Mr. Cilluffo spent 8 years with CSIS in senior policy positions with a Homeland Security focus.

Ms. HARMAN. Without objection, all of your full statements will be inserted in the record. I now ask Mr. Bettenhausen to summarize your statement for 5 minutes. There is a time clock, so it will start blinking red just as you get to 5 minutes. Welcome.

STATEMENT OF MATTHEW BETTENHAUSEN, EXECUTIVE DIRECTOR, CALIFORNIA OFFICE OF HOMELAND SECURITY, STATE OF CALIFORNIA

Mr. BETTENHAUSEN. Thank you, Chairwoman Harman, Ranking Member Reichert, members of the subcommittee. We greatly appreciate the opportunity to have this discussion and conversation today about information sharing and terrorism prevention. We certainly are proud to call you one of California's very best and very own, Madam Chairwoman. We appreciate all of your support and leadership as well as the entire committee for their encouragement for support and leadership which has happened not only over the course of tragic events of 9/11, but since then, with the creation of the Department.

Ms. HARMAN. We will give you an extension of time if you want to continue to talk about how great the subcommittee is.

Mr. BETTENHAUSEN. Thank you, I appreciate that.

I think and I agree with the ranking member in my conversation with Chairwoman Harman before the committee too, we have to be careful as we look at the 5 years, and we move through the elections and the transition that we don't continue to reorganize and shake these things up. We have got to start solidifying actual action and implementation, and that is one of the things that I would like to emphasize here today.

This is all about cooperation and partnerships. I got into Washington, DC late last night having spent some time with our friends and partners in Canada in British Columbia. Governor Schwarzenegger has recognized that he wants to have a close, and cooperative, and collaborative relationship with them and certainly with the upcoming winter Olympics that is critical.

Borders are to longer defined simply by geography. California is on the border with Canada. Our ports of entry in Los Angeles, our airports, the shared maritime interests that we have in trade is the key to the Asian Pacific corridor and the ports that we share in

bringing goods into the United States and driving the economy are critical.

That idea of cooperation, coordination and collaboration is the emphasis that I would like to have in my overall remarks, because this is a philosophical point that we need to continue to emphasize with our Federal partners. Prior to 9/11 terrorism prevention, terrorism prosecution, terrorism internationally was exclusively the province of our Federal Government. We realized after 9/11, terrorism prevention is everybody's business. It is State and local government, it is across disciplines, it is individual citizen's business.

I have given a number of examples in my written testimony from individual citizens. The worker at the Circuit City who noticed a training video and reported it in. The idea of "See something, say something." That attack on Fort Dix.

We also have State and local officers in Torrance, California who are investigating convenience store robberies which they were committing as it turns out in a model of Federal, State and local cooperations. A cell that was operating, committing the convenience store robberies to get the financing in order to do attacks on Jewish synagogues, military recruiting depots and National Guard Armories in Los Angeles. It was terrorism prevention in action. But it was the action of States and locals that uncovered this. They are the most important first responders and first preventers in a terrorism prevention. Until we truly and fully treat them as full and equal partners in the terrorism prevention mission, we are not going to be successful.

So what I would like to talk about in terms of how we do this in making sure that State and locals are full and equal partners, I do go back to the theme of enlist, entrust and empower. We must enlist our local first responders and first preventers. There are only tens of thousands of Federal law enforcement agencies in this country across all the Federal agencies. But there are hundreds of thousands, nearly a million sworn law enforcement officers, security guards who are doing this. These locals are excellent and capable.

We have to overcome the fact that our Federal agencies are not used to even working with each other, the walls that we have broken down, but most importantly working with us, and understanding what we can provide. It is not just that we have information requirements, we are probably their most important information producers. We have to collect and connect the dots if we are going to prevent the next terrorist act.

We must entrust. We have to approve security clearances. We have to have a presumption of sharing information. It has to be not just about prosecution, it has to be just not about law enforcement. You need to value what we have, it should not be that we are considered as a nuisance to this mission. We must be brought in as full and equal partners in this collaborative relationship. Trust us, entrust us.

Finally empower us. I think the President's national strategy on information sharing is a step in the right direction. Your 9/11 implementation bill lays the foundation, both for the finishing of this administration and the next administration, but it is critical for sustainment and funding for these things to encourage us to have the analysts to support our front line first responders who are out

there day in and day out protecting the public and preventing terrorism.

I see that my time is up, so I thank you for the opportunity to be here and I look forward to your questions.

Ms. HARMAN. Thank you very much, Mr. Bettenhausen.

[The statement of Mr. Bettenhausen follows:]

PREPARED STATEMENT OF MATTHEW BETTENHAUSEN

APRIL 24, 2008

Chairwoman Harman, Ranking Member Reichert, and Members of the subcommittee, thank you for the opportunity to appear before you this morning to discuss the critical role State and local public safety agencies play in preventing terrorism and how the Office of Intelligence and Analysis can do more to enlist, entrust and empower our first preventers.

Let me begin by taking a moment to acknowledge the Chairwoman's commitment to enhancing the preparedness of local communities for both intentional and natural disasters. Your leadership and role in overseeing the Department of Homeland Security has paid significant dividends. You and your colleagues have not been afraid to ask the difficult questions and the sense of urgency this committee has brought to homeland security issues has been a catalyst for productive change within the Department and at the operational level.

This morning, I want to share with you why we need to enlist, entrust and empower State and local preventers and how invaluable fusion centers are to California's homeland security strategy. The progress being made by the Department of Homeland Security and the Department of Justice in this effort is noteworthy. Congress has also provided sound policy direction and the resources to ensure an effective network of fusion centers is built with the capability of protecting our communities and critical infrastructure from terrorist attacks. It is also important to recognize that our best efforts to share information will be in vain without a firm commitment at all levels of government to ensure fusion centers and analysts institutionalize policies to protect privacy and civil liberties. Finally, I want to highlight some of the areas where the Department's Office of Intelligence and Analysis can do more to enhance the effectiveness and sustainability of fusion centers.

STATE AND LOCAL FIRST PREVENTERS

Prior to 9/11, State and locals were all too often an afterthought in counterterrorism efforts. This has proven to be a hard mindset to change. Many of our Federal partners underestimate the unique capabilities of State and local public safety agencies. There has been progress on enfolding locals into the counterterrorism effort, but we are not there yet. For this reason, I take every opportunity to remind my Federal partners that, as counterterrorism efforts evolve, we must work with our first preventers to uncover the recruitment, fundraising (money-laundering), networking and operational planning of Islamic extremists in the United States.

Early in my career, I realized the need to enlist State and locals in our counterterrorism efforts. It was in the wake of the Oklahoma City bombing in 1995, while I was serving as a Federal prosecutor in Chicago. My colleagues and I in the U.S. Attorney's Office were busy looking through international flight data for a global nexus. In the meantime, an Oklahoma Highway Patrol trooper stopped a yellow 1977 Mercury Marquis without a license plate. The driver of the car was Timothy McVeigh. The alert trooper arrested McVeigh for carrying a loaded firearm. Three days later he was identified as the man being sought in the nationwide manhunt.

The Olympic Bomber case is another example of the critical role of local preventers. As the committee knows, Eric Rudolph conducted a series of bombings across the southern United States, which killed three people and injured at least 150 others. He declared that his bombings were part of a guerrilla campaign against abortion. Despite the efforts of the FBI, Rudolph was ultimately arrested by a local police officer in North Carolina who was on a routine patrol and observed Rudolph scavenging for garbage in a dumpster behind a Save-A-Lot store.

In a more recent case, the Fort Dix Six, a group of six radical Islamist men allegedly plotting to stage an attack on the Fort Dix military base in New Jersey, were arrested by the FBI on May 7, 2007. They were subsequently charged with planning an attack against U.S. soldiers. The alleged aim of the six men was said to be to "kill as many soldiers as possible." Local law enforcement was alerted to the group

when one of the suspects requested that a neighborhood electronics store convert a video tape to DVD that depicted the suspects firing weapons and shouting jihadist slogans in the Poconos. Store employees notified law enforcement, which identified and monitored the suspects until arresting them.

Closer to home for the Chairwoman is the Torrance Case. In this case, Kevin James, a Muslim convert, founded a radical Islamic group called Jam'iyyat Ul-Islam Is-Saheeh (JIS), Arabic for Assembly of Authentic Islam, from his cell in Folsom Prison in California. James recruited fellow inmates to join a prison based terrorist cell and recruit both released inmates and new recruits to join his mission to kill those he considered infidels in the Los Angeles area. The break in the case came when local police officers in Torrance, California, arrested two men in connection with a string of armed robberies at convenience stores. During the investigation, the local police officers noticed Islamic extremist materials during one of their searches. With this new evidence, authorities began to unravel their more sinister intentions to attack military recruiting stations and Jewish sites in Los Angeles. Late last year, Kevin James pled guilty to "conspiracy to levy war against the United States through terrorism" and faces up to 20 years in Federal prison upon release from State prison.

International cases also rely on leads generated by local preventers. As was the case when local police in the United Kingdom discovered suspicious U.S. Navy information after arresting Babar Ahmad, the leader of a terrorist support cell and a computer specialist working on the now defunct Azzam.com, an Islamist extremist website. The previously classified information, planned movements of a U.S. Navy battle group, was found in Ahmad's room at his parent's home in London. After the discovery of these documents, officials in the United Kingdom alerted the FBI. U.S. authorities subsequently issued search warrants upon e-mail accounts associated with the Azzam.com websites and discovered e-mail communications from Abujihad (formerly known as Paul Hall) dating from late 2000 and the Fall of 2001 from his personal and military based e-mail accounts. Information gleaned through the original search ultimately led to the arrest of Abujihad.[1] During the investigations of Abujihad, and his onetime roommate, Derrick Shareef,[2] investigators learned of a discussion between the two to carry out a sniper attack on a military installation in San Diego.

These are just a few of the many cases where State and local public safety officials have been at the center of our national and international counterterrorism efforts. These examples underscore how State and locals are in the best position to discover and disrupt Islamic extremist activity in our communities.

CALIFORNIA'S STATE TERRORISM THREAT ASSESSMENT SYSTEM

To determine an accurate depiction of our adversaries, their intentions, and their capabilities, California moved quickly after 9/11 to establish a Terrorism Threat Assessment System. The State Terrorism Threat Assessment System (STTAS) is responsible for regional and statewide information collection, analysis and sharing activities. The STTAS is comprised of four Regional Terrorism Threat Assessment Centers (RTTAC) and one State Terrorism Threat Assessment Center (STTAC). The RTTACs are located in San Diego, Los Angeles, San Francisco Bay Area and Sacramento. These locations mirror the Federal Bureau of Investigation areas of responsibility within California and are comprised of a mixture of State, local, and Federal public safety agencies.

The State fusion center is designed to provide California's senior leaders with: situational awareness of identified threats; visibility of, and coordination with, the critical infrastructure of the State; and constant access to the latest local, State and national information analysis products and assessments. The STTAC provides: statewide assessment products; information tracking and pattern analysis; geographic reporting linkages; and connections with the latest national information from the FBI, DHS and other Federal agencies.

The Regional fusion centers: integrate the intake, analysis, fusion, and synthesis of intelligence information with an emphasis on terrorist threat intelligence; identify patterns and trends that may be indicative of emerging threats; and provide relevant, timely and actionable intelligence products for the region. The RTTACs establish policies to share and exchange terrorism-related information and intelligence

[1] Abujihad was convicted March 5, 2008, of providing material support to terrorists and disclosing classified national defense information. His sentencing is set for May 2008 and he faces up to 25 years in Federal prison.

[2] On November 29, 2007, Shareef changed his original plea and pled guilty to plotting a grenade attack on a Rockford, Illinois mall.

products with public and private sector organizations having public safety and infrastructure protection responsibilities.

There are currently 15 personnel assigned, or pending assignment, to the STTAC from a mix of State agencies, including the State Office of Homeland Security, the California Highway Patrol and the California National Guard. The regional fusion centers vary in size from 15 individuals in the Sacramento and San Diego RTTACs, 40 individuals in the Los Angeles RTTAC, and 44 individuals in the San Francisco Bay Area RTTAC.

The State and regional centers are supported by a network of Terrorism Liaison Officers (TLOs) and a secure web-based information sharing system to distribute and receive information. The TLOs serve as the local public agency and private entity point of contact for all terrorism-related issues. At the local level, law enforcement and public safety agencies are designating TLOs who are trained in the review and assessment of local reporting and in conducting outreach to other public safety agencies, critical infrastructure operators and community groups. The TLO is the local agency point-of-contact for all terrorism-related alerts and suspicious activity reports, requests for information, warnings and other notifications from regional, State or Federal homeland security agencies. The TLOs review local-agency reports, manage local reporting and initiate or respond to requests for information. The TLOs have an ongoing relationship with other local agencies, especially those with daily contact in the community, and develop relationships with critical infrastructure sites within their respective jurisdictions, establishing a personal connection with their security and management staff.

California has trained over 4,300 TLOs through a formal training program, approved and certified by both DHS and California Commission on Peace Officer Standards and Training (POST). We have also expanded the TLO program to include an initial group of over 70 individuals representing State agencies in Sacramento who will be connecting State government directly to the STTAC.

With the support of the Federal homeland security grants, our future investments will include: (1) expanding the existing threat assessment analytical capabilities at the fusion centers; (2) expanding the training of Terrorism Liaison Officers; (3) expanding the existing State-wide information sharing technology platform; (4) expanding law enforcement counter-terrorism case de-confliction efforts; and (5) enhancing public and private sector information sharing partnerships.

STATE AND LOCAL FUSION CENTERS NEED FEDERAL SUPPORT

I first want to recognize the initiative the Department of Homeland Security has taken to embed DHS Intelligence Analysts in State and regional fusion centers. This effort is to be applauded. Similarly, I would be remiss if I did not recognize the contribution of the FBI Special Agents in Charge in California for their partnership and support of California's fusion centers. In particular, cooperation by the Los Angeles FBI office resulted in space being donated to house the Los Angeles area analysts. This collaboration continues, as the Los Angeles RTTAC is being ably led by Ms. Leslie Gardner of the FBI. I cannot underscore enough the value of these partnerships to the overall success of our fusion centers.

The National Strategy for Information Sharing (Strategy) is also praiseworthy, as it provides clear and concise direction to all levels of government. The Strategy recognizes the critical role of State and local first responders and first preventers in preventing acts of terrorism. Being enfolded by this strategy validates the unique perspectives of State and local public safety agencies and represents a much needed change away from a Federal-centric approach to combating terrorism.

We are committed to quickly implementing the Strategy and I am pleased to report that one of the key elements—suspicious activity reports—is being piloted in California by the Los Angeles Police Department (LAPD). The goals of the pilot program are to standardize internal processes and institutionalize counter-terrorism throughout the LAPD. The collection of this data will enable the LAPD, and other departments, to develop a measurement tool for terrorism-related behavior and activities to identify indicators of emerging threats.

The establishment of the Interagency Threat Assessment and Coordinating Group (ITACG) is another positive step being taken by DHS. The ITACG has the potential to bring a State and local perspective to products produced by the Intelligence Community. The ITACG also has the potential to enhance our ability to turn information analyzed at the national level into action at the operational level. However, more work needs to be done to better define the information requirements of the Intelligence Community from State and local public safety agencies. Locals need clearer direction on the types of information that should be shared.

At the operational level, fusion center analysts have been pleased with the Department of Homeland Security's deployment of the Homeland Security Information Network (HSIN), a system for sharing sensitive analytical products. Under Mr. Charlie Allen's leadership, the Department has improved both the timeliness and the quality of the HSIN products. Responses to requests for information from State and local agencies have also been more timely.

Another positive development has been the establishment of the Homeland Security State and Local Intelligence Community Interest (HSIN–SLIC). The HSIN–SLIC provides a secure forum for analysts from over 43 States and 6 Federal agencies to directly share information with each other. The forum is also supported by weekly threat teleconferences. Early feedback has indicated that this is one of the more promising venues to share information horizontally and to identify emerging national threats.

FUSION CENTERS' ROLE IN PROTECTING CRITICAL INFRASTRUCTURE

Fusion centers should also be leveraged to enhance critical infrastructure and prevention capabilities. DHS should act on the recommendations made by the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) to establish the critical infrastructure and key resource desks (CIKR Desk) at State fusion centers. (see attachment). As the SLTTGCC noted, the key function of the CIKR Desk in fusion centers would be the integration of threat, vulnerability, and consequence data to develop information products for public safety and private entities with security responsibilities.

In California, fusion centers are being utilized to extend training to our private sector partners. At the Governor's direction, the requirements for licensed security professionals were modified to mandate enrollment in a 4-hour terrorism-awareness training program. This common sense policy change will ultimately provide terrorism training to the approximately 400,000 licensed security professionals in California. We have also implemented a terrorism-awareness training program amongst professional and trade associations to ensure that they have current trend and pattern information, threat assessments and connectivity to their RTTAC. Additionally, the State fusion center is working closely with the agricultural industry to protect this critical resource by formulating an initiative with the California Department of Food and Agriculture to deliver a 1-day TLO course to each of the 58 county agriculture commissioners. Furthermore, a partnership is being formed with the State's Rural Crime Task Force to train its members in terrorism awareness and California's information sharing protocols.

The RTTACs have been working closely with my office to identify, prioritize and protect the State's broad array of critical infrastructure and key resources (CI/KR). These efforts have been closely coordinated with a broad group of private-sector partners—those entities that own and operate the bulk of the State's assets and resources. Such partnerships include site owners and operators, first responders, public and private organizations and associations, and other levels of government, including local, State, Federal, and tribal partners.

The Automated Critical Asset Management System (ACAMS) is a Web-enabled information services portal which helps our State and local governments build critical infrastructure/key resource (CI/KR) protection programs. ACAMS provides a set of tools and resources that help law enforcement, public safety and emergency response personnel: collect and use CI/KR asset data; assess CI/KR asset vulnerabilities; develop all-hazards incident response and recovery plans; and build public/private partnerships. ACAMS is a secure, online data base and data base management platform that allows for the collection and management of CI/KR asset data; the cataloguing, screening and sorting of this data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans. The Department of Homeland Security provides ACAMS for free and ACAMS is used in more than 32 States and territories.

PROTECTING PRIVACY AND CIVIL LIBERTIES

In all of these efforts, we are fully committed to protecting California's residents and respecting their privacy, civil rights and civil liberties. Our fusion centers must comply with our Federal and State Constitutions, laws, regulations and policies regarding the protection of privacy, civil rights and civil liberties. Because protecting these rights is so fundamentally important to our democracy and our office's mission, we established the State Terrorism Threat Assessment Advisory Group (STTAAG) to provide independent and informed advice. The STTAAG is comprised of a broad and diverse membership of Californians who bring a wide range of expe-

riences including public safety, national security, community service, communications, and academia.

The STTAAG Chair is Elizabeth Rindskopf Parker, Dean of the Pacific McGeorge School of Law and a former CIA and NSA General Counsel. The Vice Chair is Craig Manson, who previously served as Assistant Secretary for Fish, Wildlife and Parks in the U.S. Department of the Interior and as a Judge in the Sacramento County Superior Court. The membership also includes Rabbi Abraham Cooper of the Simon Wiesenthal Center, Dafer Dakhil of the Omar Ibn Al Khattab Foundation, prominent members of the Sikh community, the California Broadcasters Association, and representative from various public safety organizations.

Over the past year, we have formalized the existence of the STTAAG through the adoption of a charter. This charter reflects the two primary objectives of the group—providing independent advice on privacy, civil rights and civil liberties issues; and, on how our organization can engage the people we serve is a constructive dialog on who we are and what we are doing to enhance their collective security in a manner which respects their individual liberties.

Along these lines, we co-hosted an outreach event with the Simon Wiesenthal Center last November. A substantial number of my senior staff, along with our Federal and local partners in Los Angeles, spent several hours with Southern California business, community and religious leaders. We provided them with information on the terrorist threat, the measures that we are taking to mitigate that threat and the role of the citizen in planning for and preventing terrorist attacks against our homeland. It was an incredibly positive session and we hope to host similar events on annual basis around the State.

BUILDING A MORE ROBUST AND SUSTAINABLE NETWORK OF FUSION CENTERS

In previous hearings this subcommittee reviewed the findings of the February 20, 2008 fusion center report issued by CENTRA Technology, Inc. The report focused on three areas in need of improvement: (1) identifying the priority information needs for both the Department and for State and local fusion centers; (2) streamlining the process for responding to requests for information; and (3) enhancing the open source analytical capabilities of analysts in State and local fusion centers. In general, the Department has acknowledged that these are indeed areas that should be acted upon.

I look forward to working with the Department to assist them in their effort to offer additional open source training opportunities for our first preventers. We are also committed to ensuring timely and accurate responses to requests for information. The Department should be certain that requests initiated, and responsed to, by regional fusion centers are carbon copied to State fusion centers. This will ensure States have optimal situational awareness and enhance their ability to identify emerging trends. Additionally, the Department should be clear in issuing their priority information needs and provide routine feed back to State and locals that contribute information to the Intelligence Community.

To be effective, fusion centers must be staffed with well trained and properly cleared personnel. The National Strategy for Information Sharing acknowledges the importance of personnel and states, "the Federal Government will support the establishment of these centers and help sustain them through grant funding, technical assistance, and training."[3] Congress also recognized the value of staffing fusion centers in passing H.R. 1, the Implementing Recommendations of the 9/11 Commission Act (9/11 Act), which explicitly allows States and locals to utilize homeland security grants to hire personnel to staff fusion centers.

Notwithstanding the urgent operational need and unequivocal legislative intent, the Department has continued to issue guidance (Information Bulletins 235 and 281) regarding the use of Federal funds under the State Homeland Security and Urban Area Security Initiative Grant programs which has been extremely counterproductive and detrimental to State and local efforts to build and sustain a network of fusion centers and contravenes the clear intent of Congress. I urge the committee to eliminate the unduly burdensome and detrimental guidance.

State and locals have invested a lot of time, money and personnel in terrorism prevention and have absorbed the vast majority of the costs for prevention, protection and infrastructure preparedness with State and local funds. Creating, establishing and sustaining fusion centers has been a success story. Staffing them with qualified, cleared analysts has been and remains a challenge. These analysts and fusion centers also clearly work to the benefit of the Federal Government by allowing for better information sharing and real time communication during a crisis.

[3] National Strategy for Information Sharing, October 2007.

Putting unnecessary restrictions on funding while we are still in the developmental stage of the fusion centers and information sharing is unwise. The lack of analysts will have adverse consequences on our infrastructure protection efforts, including their review of classified information and providing information back to DHS's Infrastructure Protection Directorate. California is conducting a number of comprehensive reviews with the Department, and fusion center analysts are assisting in these efforts. We have also developed and invested significant resources in the identification and training of several thousand TLOs at government and private agencies throughout the State. Without a functioning fusion center system, the information gathered by these TLOs will be at risk of not being collected, as the system needs constant attention and skills refreshment.

As I mentioned earlier, embedding DHS personnel in regional and State fusion centers is a positive development. DHS should take every opportunity to replicate the success of this initiative by detailing analysts from other components of the Department. Fusion centers and should be the logical base of operations for DHS's Protective Security Advisors, rather than being assigned to Secret Service field officers. Additionally, Congress has provided additional resources to the Department to deploy Mass/Surface Transit Security and Aviation Security analysts. These personnel would also be good candidates to embed in regional and State fusion centers. Indeed, all agencies and Departments with either law enforcement or emergency response capabilities should have a significant presence at regional fusion centers. Currently the United States Coast Guard, Federal Bureau of Investigation, and the Drug Enforcement Agency participate in California's regional fusion centers. Our prevention, analytical and information sharing capabilities could only be enhanced by a sustained commitment from the Immigration and Customs Enforcement Agency, the Alcohol, Tobacco, and Firearms and Explosives Agency, and Transit Security Administration.

As we build this nationwide matrix of connected State and local fusion centers staffed by a multi-disciplined analysts from the public safety field, it remains important to ensure that barriers to information sharing from traditional Federal, State and local law enforcement agencies are appreciated and reduced consistent with the necessary protection of privileged information. We are building a new capability across the country, focused on prevention, and the key to its success must be the widest possible exchange and access to analysts and information. Great progress has been made, but work remains on demonstrating that Homeland Security professionals and first responders in the fusion centers are equal and relevant partners.

DHS should also expedite the fielding of the Homeland Security Data Network (HSDN) system to the State fusion center. This long awaited project is a needed improvement to California's information sharing and analytical capabilities, as the HSDN system will allow the STTAC and OHS analysts access to some levels of classified information and connectivity with the RTTACs and DHS at the classified level.

Finally, security clearances—both in terms of availability and proper level—remain an issue for State and locals. Perhaps the most recent and best example I can provide you with is the classification of the new Presidential Homeland Security Directive regarding cyber security at the Top Secret level. Unfortunately, the Department has not recognized the need to issue Top Secret clearances to State and local public safety officers—even when those individuals bear the responsibility of implementing national security directives.

Again, thank you for this opportunity to be here today. I will be happy to take your questions.

ATTACHMENT

THE CRITICAL INFRASTRUCTURE AND KEY RESOURCE FUNCTION IN STATE FUSION CENTERS

BACKGROUND

The State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) serves as a forum to ensure State, local, tribal, and territorial homeland security officials, or their designated representatives, are integrated fully as active participants in national critical infrastructure and key resource (CIKR) protection efforts. Additionally, the SLTTGCC provides an organizational structure to coordinate across jurisdictions on State-and local-level CIKR protection guidance, strategies and programs. This paper provides a summary of the SLTTGCC's recent study on the necessity of a critical infrastructure protection functionality located within state and local fusion centers.

OVERVIEW

As part of the National Strategy for Information Sharing, the Federal Government is promoting that State and major urban area fusion centers achieve a baseline level of capability and become interconnected with the Federal Government, each other, and the private sector.

State and Local Fusion Centers (SLFC) represent an increasingly important aspect of the national effort to protect CIKR. SLFCs coordinate the gathering, analysis, and dissemination of law enforcement, homeland security, public safety and terrorism information. They serve as an important resource to exchange information between state and local governments and to communicate with CIKR owners and operators from a regional platform. As a key contributor to critical infrastructure protection programs and activities, it is important to have an operational functionality within Fusion Centers that focuses on securing the Nation's CIKR.

CHARACTERISTICS OF THE CIKR FUNCTION IN FUSION CENTERS

The key function of the CIKR Desk in fusion centers should be the integration of threat, vulnerability, and consequence data to develop information products that enable and support State, local, and private sector decision-making and actions to protect CIKR. Specifically, fusion centers should create a permanent CIKR capability focusing principally on supporting risk-reduction and response needs of State and local CIKR communities. CIKR capability should:

- Have strong relationships with local CIKR owners and operators, both public and private;
- Be analytical in nature;
- Be embedded in the fusion center; and
- Be staffed by subject matter experts in critical infrastructure protection programs.

The CIKR Desk should have the ability to meet the objectives for sharing terrorism information with State and local government and the private sector that are identified in the *Information Sharing Environment Implementation Plan*.

Through the efforts required to complete this study, the SLTTGCC has identified two basic tasks for the CIKR function in a fusion center as follows:[1]

- ***Analysis***. Activities include: selecting analytical techniques and data and carrying out analysis; integrating analyses with pre-existing and new intelligence from various sources; correlating CIKR information against known threats; evaluating and transforming raw data into description, explanations, or conclusions, such as forecasts and interpretations; and developing and disseminating timely CIKR information products.
- ***Dissemination***. Activities include: providing recommendations to appropriate Federal, State, and local authorities and private sector partners to reduce CIKR risk or mitigate the consequences of deliberate attacks or natural disasters; communicating credible and non-credible threats to CIKR stakeholders; disseminating alerts, advisories, and other CIKR informational products; and ensuring communication of relevant information to CIKR personnel on the ground, and participating in national and regional readiness exercises.

CIKR Operations

Key CIKR Desk functions include:

- ***Inputs***: planning, sources of information, and methods of data collection
- ***Conversion***: process information undergoes to make it actionable, timely, and accurate
- ***Output***: mechanisms for disseminating products to users, and the specific decisions that are made based on these products.

CIKR Inputs

CIKR inputs are built on planning, direction, and collection. Planning and direction activities include assessing and specifying the information requirements, requisite analysis, collection methods, and desired timeframe for the information products. Continuous feedback will provide enhancement to the overall process, products, and CIKR protection outcomes. Inputs for CIKR information should, where possible, include all relevant threat, vulnerability and consequence information.[2] Data collection is critical and may come from many sources, including:

- Existing fusion center records and databases;
- Open-source information, e.g., documents, reference books, journals, and newspapers;
- State and local government agency sources; and
- Federal sources, including the Threat Information and Infrastructure Protection Program (TIIPP), DHS Office of Infrastructure Protection (IP), and the Office of Information and Analysis' joint Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).[3]

The CIKR Desk should also collect information by requesting inputs from CIKR security partners.[4] These inputs include: site-specific risk information, interdependency information,

---

[1] SLTTGCC Information Sharing Working Group, Fusion Center Survey Responses, p. 1.

[2] In the context of the NIPP, threat is the intention and capability of an adversary to undertake actions that would be detrimental to CIKR; vulnerability is a weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by a natural hazard or technological failure, and consequence is the effect of an attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident.

[3] SLTTGCC Information Sharing Working Group, Fusion Center Survey Responses, p. 3.

[4] SLTTGCC Information Sharing Working Group, Fusion Center Survey Responses, pp. 3-4.

suspicious activity reports, communications capability information, standard operating procedures for incident response, and emergency contact /alert information.

CIKR Information Conversion

Conversion covers elements of processing and exploitation, and analysis and production. The CIKR Desk track, monitors, integrates, analyzes, and fuses all law enforcement, intelligence, and homeland security information related to CIKR. This information is then processed and disseminated to the appropriate Federal, State, local, and private sector officials. Processing and exploitation includes tasks such as:

- Evaluations to determine the relevance, credibility/reliability, and accuracy of data; and
- Processing and collating information by domain-trained analyst/subject-matter experts.

Analysis and production includes tasks such as:

- Evaluation and transformation of raw data into products, such as forecasts and interpretations;
- Integration of analysis with pre-existing intelligence and new intelligence from other sources; and
- Recommendation to appropriate officials in order to prevent or mitigate attacks.

Outputs for CIKR Desk Operations

SLFC information associated with CIKR is generally related to specific, credible threats, or particular vulnerabilities identified through analysis. The information is generally shared with key stakeholders, including the State's Homeland Security Advisor; the State Police; emergency administrators; the law enforcement agencies with jurisdiction over the affected CIKR; the local FBI; DHS; other state agencies with authorities associated with the particular CIKR; and the owners and operators of the critical infrastructure affected by the information. When distributing the information, the manner of distribution is determined by considering the need for timeliness, as well as information security requirements.

The products that the CIKR Desk produces are disseminated to the users through personal contact, electronic mails, secure portals such as SIPRNet, telephone and multimedia training programs. Other information systems could include the RISSNET, RISS ATIX, FBI LEO, and HSIN and HSDN.

PROTECTING SENSITIVE INFORMATION

Information protection is vital to the success of the critical infrastructure protections mission. In addition to the requirements of handling sensitive intelligence and law enforcement information, there are important sensitivities associated some CIKR information therefore fusion center staff handling this information must be cleared and trained in all relevant information protection regulations, procedures and considerations.

THE PATH FORWARD

Ultimately, protection and preparedness will only be as good as the CIKR information and intelligence that informs it. The approach outlined here aligns successful processes to synthesize large volumes of CIKR threat, vulnerability and consequence information into useful, actionable products developed with the ultimate end user in mind.

Protecting critical infrastructure is a shared responsibility by all levels of government and the owners and operators of the nation's critical infrastructure. While the operational focus of individual fusion centers may vary, the need for CIKR protection is a constant across the Nation. The functions of the CIKR Desk are at the core of the fusion center value proposition articulated to Congress last year:

Ms. Harman. I think we may frame your oral testimony. It is the core mission of subcommittee. I would just add that your example of Torrance, California is one we all know. We had a hearing in Torrance, which is in my congressional district, about how successful that was.

Ms. Kayyem, please summarize your testimony in 5 minutes.

STATEMENT OF JULIETTE N. KAYYEM, UNDER SECRETARY FOR HOMELAND SECURITY, EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY, COMMONWEALTH OF MASSACHUSETTS

Ms. KAYYEM. Thank you very much, Chairwoman Harman and Ranking Member Reichert. I am also pleased to be here. I will take Matt's compliments of the subcommittee and continue.

I think it is great this subcommittee is thinking about the future and also thinking about how to make what is already there better, rather than shifting around again, because from the State perspective, enough shifting so to speak. We need to sort of make a plan and stick with it.

In my written testimony, I discuss our Fusion Center. What it is, what it is doing, how it conceptualizes itself. It will be very different from California's many Fusion Centers in other States. I think that is good and right.

I think given the threats and the particular concerns of any given State and any given governor considering crime or whatever else that we don't want one size doesn't fit all. We don't want to think of Fusion Centers as these sort of new intelligence beasts not linked to the public safety entities that they have to contribute to.

I actually compliment the law enforcement intelligence relationship that exists in most Fusion Centers. I think when the media says those Fusion Centers are just doing criminal analysis, that is actually right. We need to make it all hazards, all threats and make it integrated into the public safety community.

So with my time, let me talk about quickly what works and what is not working on a very specific level and then how we might think about it in the future. I&A and DHS, in its intelligence functions, has to think in the world that exists now where is their value added, because we have so many players in this realm. We have the JTTF in our State, which is excellent. We have any other number of counterterrorism, antiterrorism units. So what is their value added? Basically their value added is with the States and locals and their consumers.

What has worked in that regard is we actually have an I&A specialist. She had been a member of the Fusion Center in our Fusion Center. It is great. I have one person to go to. The quagmire that is DHS for a lot of us, it is answered by one person. She may not have all the answers, she knows how to get them to me. Requests for information come back quickly. We have particular threats in our State. We have high profile people coming to the universities. We need to know stuff fast. I can go to one person. I don't have to come down here, and figure out who to talk to. I think that is great. The CENTRA report promoted that. To the extent, you can get more of them into Fusion Centers, it makes a lot of sense.

What ought to be fixed? The truth is that as a consumer of the intelligence at I&A is pushing out. That is our Fusion Center in many respects. There are three main problems right now. One is and I say it in my written testimony, that the intelligence apparatus here in the District of Columbia sometimes, I think, lives by the motto "publish or perish", the academic model.

There is just too much, it is not helpful to me from the prospective of a State Homeland Security advisor. Great examples of relatively public example. This year alone we have seen an increase in the Osama bin Laden tapes. The content is not that interesting. It is the same tape over and over. But as we reach this transition and certainly a Presidential transition over the course of this year, what I want it know as a consumer of the intelligence, because I can hear about the tapes on CNN, is how is DHS thinking about this? How is I&A thinking about what this means for transition? Are we worried? Should I be worried? Are these more or less? It is the kind of intelligence themes rather than the fact of it that matters more to me. Because based on the Osama bin Laden tape, we are not going to recommend from an operational level to ramp up the State Police or to get MEMA active, Massachusetts Emergency Management Agency activated. That is what I think thematically. We have the JTTF for specific investigations.

Secondly, grants. You know, I won't talk about grants except for one thing, I can not wake up rationally one day and be told by DHS that 25 percent of my Homeland Security funds have to be spent on IED prevention and response planning. When I haven't been told that the year before, but more importantly, I&A has never told me that. The grants are not matching the intelligence. So I wake up thinking how am I going to tell this to the people who want the money. That is a huge problem.

Third, treating us maturely, just picking up on what Matt said. The spy satellite falling from earth was not a movie for many of us, it was real. What we were getting was just not helpful from an operational perspective. That is how we are view ourselves. We are just making operational recommendations. I don't have fire trucks. We are just saying react.

It was not helpful, let's just say. Whether the Department of Defense, or Department of Homeland Security or, as I say in my written testimony, the Secretary of Agriculture is in charge, I could care less. What I wanted to know and what wasn't provided to me is how operationally should we be thinking about this? We were treated like kids, I mean immaturely.

Boston Globe has a banner headline about it and I don't have any good advice to give to either the governor or down to the operational entities except for cross your fingers and let's hope DOD shoots it down. That is not helpful. So in terms of the maturity factor, I would really push that. So that is how those changes would make a lot of sense for the next administration in terms of what I need as a consumer of intelligence. My written testimony gets into some other aspects of the Fusion Center. Thank you very much.

Ms. HARMAN. Thank you very much.

[The statement of Ms. Kayyem follows:]

PREPARED STATEMENT OF JULIETTE N. KAYYEM

APRIL 24, 2008

It is an honor to testify in this important matter, "Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs." It is especially an honor to be here in front of Chairwoman Harman, who has not only been an exceptional leader in this field, but a friend and mentor to me as well.

I hope my testimony today will highlight some of the exceptional work performed by our Commonwealth Fusion Center, provide guidance for how this committee might think about the relationship between the States and the Department of Homeland Security (DHS) regarding intelligence efforts, and provide some thoughts on what does and does not work in the structure that now exists. Since this committee is already familiar with many of the challenges facing fusion centers, including continuing funding by homeland security grants, I will focus my discussion instead on themes and priorities. Of course, like every other homeland security advisor, I worry about sustainability and continued funding of the State's many efforts, but enough said in that regard.

The last time I testified before this committee, I was a lecturer at the Kennedy School of Government, and my focus then was on how the Federal Government could better collect and analyze intelligence. For the last year, I have served as the Under Secretary of Homeland Security for the Commonwealth of Massachusetts. In this position, I report to Secretary of Public Safety Kevin Burke. In addition, I am Governor Deval Patrick's federally designated homeland security advisor. In many respects, the status of my position reflects the trends and changes within homeland security on both the Federal and State level. Just as Hurricane Katrina painfully taught us that a Department solely focused on terrorism may be at risk of undervaluing threats brought by mother nature, a State homeland security apparatus not aligned with the daily needs of public safety entities or first responders could not survive or remain relevant.

In this capacity, then, Governor Patrick and Secretary Burke charged me and our public safety agencies with evaluating the status of homeland security in the State to promote successful integration of our public safety and emergency management operations. Our legacy is in ensuring that policies and practices better protect our citizens from harm, wherever it may arise. So, first and foremost, this meant requiring that the State had plans and policies in place to guide the significant homeland security funds coming to the State, whether they be for interoperability, evacuation planning, resource management, recovery efforts or, as I will highlight here, intelligence efforts.

The Commonwealth Fusion Center, the CFC, is, by Executive Order, the State's designated fusion center and was established in October, 2004. The Boston Regional Intelligence Center, the BRIC, serves as the UASI's primary fusion entity, and we continue to ensure that both of their efforts are cooperative and, to the extent practicable, not duplicative. DHS needs to ensure that limited resources, capabilities and information do not unnecessarily create competition, but ensure cooperation. We have a very good working relationship with the BRIC, and the Boston police for that matter. DHS can play a very useful role in ensuring that resources are shared to create a unified system.

The CFC is, like most fusion centers, part of our State police, reporting through the chain of command to the Colonel of the Massachusetts State Police (MSP). While in the past newspaper articles and commentators have decried the fact that many fusion centers are joint tasked—intelligence and law enforcement based—I think those concerns are ill-founded. Indeed, I can't imagine a structure in which a fusion center was not, in major respects, focused on traditional crime analysis, providing information to localities and receiving important criminal trends from them in return. A fusion center that was solely terrorism focused could not sustain itself, not given the intelligence that is out there nor the competing needs of Governors and Mayors who are, as we are, concerned about crime. Because traditional crime often serves as a means for more nefarious or dangerous activities, we have to focus our efforts holistically. The true power that resides at the State and local level of law enforcement vis-à-vis terrorism prevention is not some grand new intelligence mission, but rather a culture of sharing the product of the good work that has been going on for years. The information that police officers routinely collect in the course of their normal duties is the same information that may identify terrorist financing or a pre-operational cell. It is also, it should be noted, the same information that a local chief can use to identify criminal hotspots or emerging trends.

To that end, we are working to put information and tools in the hands of State and local law enforcement that will enable them to detect and track precursor crimes as well as other trends. The Statewide Information Sharing System, or SWISS, has been funded by our homeland security dollars and while available and utile to all contributing departments, it will drastically enhance the CFC's homeland security and traditional crime missions. The dual-use concept is thoroughly ingrained in our homeland security strategy so that we might both meet head-on and mitigate the challenge of sustainability. Indeed, our fusion center is so integrated into the workings of the MSP that it is financially sustained wholly as part of the current operational costs of the MSP. While homeland security funds focus the CFC's efforts and training, we are not presently facing a wholesale crisis or the potential loss of analysts as is occurring in other fusion centers.

What is interesting here, however, is that not until recently has there been a discussion by DHS with States and localities on how the Federal Government could access that information in a strategic manner. A recent article in the Los Angeles Times highlights the LAPD's efforts to utilize some standardized form that would serve as a trigger for suspicious reporting to DHS. That was a local effort, and to our knowledge the most proactive attempt to treat what the fusion centers are doing as relevant to Federal threat gathering. We do not need a State-by-State capacity to access information about specific investigations or persons; indeed, once an individual jurisdiction sends information to the FBI under Guardian, we no longer have "peeking" ability. What we need is a system in which the trends or activities that are reported to the DHS Office of Intelligence and Analysis (I&A) are done so in a systematic way, and made transparent to those who would need to know the information. Without that capability, the efforts on the State level will be of little value to DHS.

The CFC has, like most fusion centers, been an evolving entity. I sometimes imagine it like Goldilocks, searching for the "just right" fit. Ours began, like many of the post-9/11 entities, as an answer to the call from the Federal Government to help prevent the "next 9/11." The changes that have occurred in the CFC, and that will continue to occur, happen because of the unique needs of our State and the changing nature of the intelligence we receive.

So, what I want to lay out here are my thoughts at this moment in time, with an eye to guiding this committee, as well as DHS, on bettering our collective efforts in the future. The CFC was one of the pilot fusion centers in the recent CENTRA report, and we learned a lot in that process. Where I critique, it is only to urge a more thoughtful assessment for the future; where I compliment, it is to provide, however anecdotally, some evidence where efforts ought to be sustained.

To begin, it might be helpful to simply lay out who is, and isn't, at the fusion center now and what they do. The core of the CFC is staffed with MSP personnel, who first and foremost are responsible to their chain of command. Representatives from other agencies include one Federal Bureau of Investigation (FBI) analyst, one agent and one analyst from the Bureau of Alcohol, Tobacco, Firearms and Explosives, one counter-drug analyst from the Massachusetts National Guard, one analyst from the Department of Correction (currently deployed to Iraq), one representative from DHS I&A, one police officer from CSX railroad, and a Geographic Information Systems specialist from the U.S. Army Civil Support Team. In addition, several MSP troopers under the direct command of the CFC, and therefore the Executive Office of Public Safety and Security, are assigned to the FBI Joint Terrorism Task Force (JTTF) for specific investigation support.

The primary focus for today's hearing is on the Office of Intelligence and Analysis, and how it works with State fusion centers. We are fortunate to be a State with a designated I&A analyst. She had previously worked at the fusion center, and so her knowledge of it, and the State itself, has been a tremendous asset.

She is, for the fusion center, and for me specifically, our one stop shopping. While she may not have every answer at hand, she knows how to get it for us. We should not underestimate how important that is. DHS, for any State, can be both amorphous and large. In Massachusetts alone, the DHS entities—from ICE, to Coast Guard, to FEMA, to a critical infrastructure analyst, to chemical industry regulators, to TSA—are all professional, but from the perspective of a State, are also too numerous to count. While FEMA has taken the lead on trying to integrate these entities, the truth is that their mission and chains of command so vary that it can be difficult. For us to have one liaison that can tap into, at the very least, intelligence efforts at DHS, and across the Federal Government, has proven exceptionally helpful. There are, after all, 16 Federal agencies that make up the Intelligence Community, all attempting to assess the persistent and evolving threats this Nation faces. It may be, one wonders, too many for the Federal Government; it is certainly too many for a single State. As one of our fusion center analysts noted, our I&A

analyst provides a mechanism to reach into the "quagmire" and get the information and resources needed by the State.

This is particularly true in one aspect of our needs: Requests for Information (RFI). Working with the CFC and the BRIC, and due to the CENTRA assessments, I&A submitted recommendations for creating a process which would efficiently serve the State's needs. This process was concluded before the CENTRA report findings, but is supported by that report. While I cannot disclose the details of the requests we have made, they have revolved around unique aspects and threats to our State and to Boston, whether they be related to critical infrastructure or visits by foreign dignitaries. I&A provides connectivity and rapid response for us; some requests are returned with information within hours of being relayed. This information can then be utilized to guide operational planning by the State police or local law enforcement.

There are other benefits, including access to secure cell phones for State designees and getting through the red tape that often is involved in security clearances. Indeed, in a recent trip I took to Paraguay, a Nation that has a relationship with the State's National Guard, our I&A analyst was able to successfully transition our security clearances to the State Department with 1 day's notice.

Thus, the physical presence of a single person who can tap into DHS, who knows why we are asking and what it means for the State, has gone exceptionally far in our relationship with DHS regarding intelligence efforts.

However, it is in the CFC's role as a consumer of intelligence that many of the more persistent difficulties arise. First, the CENTRA report, which I have studied, places tremendous emphasis on making intelligence more accessible to States and localities. That is an important effort. But, while DHS focuses these efforts on ensuring that the quantity of information getting to us continues to flow, we are likely similar to many other States in wondering whether we aren't at risk of threat assessment fatigue.

Let me put this another way. We have placed so much focus on ensuring that intelligence flows horizontally and vertically from and to State and Federal Governments that we may be at risk of the intelligence version of the often quoted academic trajectory: publish or perish. The quantity of information coming to us, often without much reference to either its strategic or tactical relevance, is overwhelming. As a State, we are left in a bit of a dilemma: distribute the information and risk triggering responses that are not justified by the validity of the intelligence or simply close-hold the information and be at risk of recreating the very stovepipes this whole effort was meant to destroy. Thus, while DHS assesses its own intelligence capabilities in the years to come, and under a new president from either party, the quality of the intelligence being shared has got to be an essential aspect of that conversation.

A relatively public example may be helpful. In 2008, there have been a number of Osama bin Laden audiotapes. We received notification of each of them by DHS (as well as by the FBI) but also, I must admit, by CNN. Their substance, for those of us who follow these things, was nothing novel: the literal rantings of the terrorist against everything associated or affiliated with the United States. But, as we all know, we need to remain exceptionally vigilant during times of democratic transition; both Spain and the United Kingdom were victims of terrorist attacks immediately before or immediately after a change in government. So while the fact of the tapes didn't seem to raise anything new in our mind, and the literal statements didn't seem particularly worrisome, as more and more audiotapes came out (and may continue to be released), we would want to be in a position to know how the Federal Government is assessing this, how are they thinking through this summer and fall of transition, and whether we shouldn't be doing the same. It is that kind of strategic guidance that would be helpful.

I am relatively confident that any information that is worthy of a preliminary or criminal investigation will be properly vetted and analyzed by our JTTF, where many of our CFC troopers work. But, for the majority of information, call it white noise or background atmospherics, we are simply consumers, not quite able to decipher whether there is any strategic relevance to so much information, but pretty confident that our operational assessments will not change.

Second, and this is not something we can fix on the State level, DHS needs to ensure that the kinds of guidance we are receiving from other DHS entities or other Federal entities is aligned with the very intelligence we are receiving from I&A. Most recently, the States received guidance and priorities for the major State homeland security grant cycle, which concludes in May. This is the major grant that States and the UASIs receive to support first responder capabilities. While we know that IEDs continue to be a threat in Iraq and against our soldiers abroad, no intelligence we had received from DHS or any Federal entity prepared us for the explicit

focus that the grant now has on IED prevention, protection, and response planning. To be clear, this is an important effort, one that needs attention and one that we have and will continue to address, in particular with our critical infrastructure program, which I will discuss further in a moment. But, by explicitly focusing on IEDs, we were left wondering whether we proverbially didn't know what we didn't know. Or, for another example, the Buffer Zone Protection grants are annually distributed to critical infrastructure sites to buttress prevention and law enforcement efforts. At the same time, some specific industries—say telecommunications or water purifying sites—will be chosen for site visits. From what we know, on the State level, these industries are chosen without us knowing why, and certainly without the industry knowing why. It may be, as I believe now, that DHS is doing due diligence and ensuring that States focus on many different sectors. But, since there is no intelligence to decipher why a specific industry is chosen, or in one case in our State, a specific site, we are left explaining to our private sector partners to simply accept the designation, trying to assure them that they are not at increased risk.

This gets me to the final comment on the challenges of our "consumer" role. Intelligence can be inherently vague and hard to define; with it, comes a tremendous amount of responsibility. While we continue to live with threats, from terrorists or bad actors or even from mother nature, the knowledge of those threats demands that those of us who work and respond to them act professionally and in a reasoned fashion. When intelligence goes from atmospherics, to potentially a real threat, we need to ensure that the very processes we have put into place are utilized and reinforced. This was made entirely clear from our recent responses to the potential consequences of an NRO spy satellite falling to earth. From my perspective, I don't really care if the Secretary of Defense, the Secretary of Homeland Security or even the Secretary of Agriculture, if he is so inclined, is designated the principal Federal officer for an event. The concern is that, as the other homeland security advisors shared information they were receiving in that 2-week period leading up to the successful Defense Department downing of the satellite, it was clear that we simply didn't have a unified notion of how we ought to prepare our public safety agencies, let alone the public. There was also a lack of a reality check in all the chaos that could answer whether the real issue at hand was one of a danger to the public for emergency management planning purposes, or a danger to our national security in that secret information might be disclosed if pieces of the satellite fell in adversary hands. It was in that vacuum that, I believe, each State likely planned differently, based on information that we all believed was probably not forthcoming. Perhaps it was because there was confidence that the Defense Department would successfully shoot down the satellite, or perhaps because the trajectory couldn't actually be determined, or maybe we knew less because the trajectory never made its way to New England, but it was in that vacuum that both paranoia and gossip gets started, and when confidence in the entire process gets undermined. The States must be treated as mature partners in these intelligence efforts.

As we look forward as well, I want to add two important efforts into the mix of how we should be thinking of DHS and I&A intelligence functions in the future. We need to continue, as we do in all homeland security efforts, to provide policies and practices that will be dual-use and respond to many hazards. Thus, as we think about the legacy of fusion centers and their continuing viability, one of the major arenas where they will and can provide unique value is in critical infrastructure assessments. In the past, our State's critical infrastructure assessments were locally based, providing the State with hundreds of potential and vulnerable sites, ranging from nuclear facilities to local high schools. Both are, of course, important, but we had no mechanism to focus these efforts on risk reduction and, from the perspective of the State, response needs.

Specific intelligence against a particular site, and our response to that information, is different than the kind of analysis we are now supporting through the fusion center in Massachusetts. Indeed, many of the homeland security dollars going to the CFC are now supporting training and efforts related to creating a unified critical infrastructure assessment tool, known as ACAMS, which is supported by DHS. We know, and explicitly express in the Commonwealth's State Homeland Security Strategy,[1] that in order to effectively carry out their missions, public safety officials and policymakers need a comprehensive understanding of the vulnerabilities of assets, systems, networks, and functions that provide critical services to the people of the Commonwealth. This knowledge will drive public safety and public policy decisions regarding preventative and protective measures, as well as response activities to

[1] *http://www.mass.gov/?pageID=eopssubtopic&L=3&L0=Home&L1=Homeland+Security+-%26+Emergency+Response&L2=State+Homeland+Security+Strategy&sid=Eeops.*

natural and man-made incidents. We are committed to understanding and assessing risk in the Commonwealth by ranking what assets are in the State based upon their vulnerabilities, whether they are likely to be under threat, and how their destruction, through any means, would impact the State. ACAMS and the CFC provide a State-wide, coordinated approach to the identification, prioritization, and protection of critical infrastructure and key resources that can be shared with important stakeholders and emergency response personnel. For this to be a successful effort, we must also partner with I&A to ensure that their strategic knowledge is shared and disseminated.

Another such critical infrastructure initiative that has recently begun to take shape at the CFC in regard to critical infrastructure is a relationship between the CFC and the Nuclear Regulatory Commission (NRC). At the recent fusion center conference in San Francisco, it was brought to our attention that there exists an NRC database cataloging suspicious activities reported by utility companies throughout the country. Being a State with one active nuclear power plant and two others in bordering States that affect Massachusetts' communities within the 10-mile emergency planning zone, we were intrigued by this information and the opportunity to further our critical infrastructure protection efforts utilizing the NRC database. We have reached out to the NRC and are beginning a process in which the NRC, the CFC, and our emergency management agency will communicate on issues of suspicious activity involving radiological threats.

I believe that these efforts, in conjunction with DHS and I&A, are really the foundation of a legacy for fusion centers nationwide. Not simply because we can better prevent and respond to terrorist threats against our critical infrastructure, but also because we can know, beforehand, how we might prioritize any number of important public safety and public policy needs.

Finally, and this is something that I know Chairwoman Harman promotes, we need to continue to demand that fusion centers are as transparent as possible, ensuring that they serve our important public safety needs in a democratic society. There will always be a tension between liberty and security, but the tension need not impede honest discussion and even evaluation. I believe, as someone who began her career in the Justice Department's Civil Rights Division, and someone who has written extensively in this regard, that we may never permanently settle this issue, but we must always be prepared to have the discussion. Before I came to work for the Commonwealth, my notion of what was going on in the intelligence world was not always a benign one.

The balance at the CFC and in the State we are trying to achieve now has made us reexamine our efforts, our policies, and our transparency. In response to the most recent ACLU examination of fusion centers, we vowed to provide a reply with an honest assessment of where we were and where we hoped to be in the future. That letter is attached for your review. We are, in addition, promoting a privacy council to ensure that we have the benefit of outside council not on specific investigations, but on how the State's public safety agencies might better balance their important public safety mission with the rights of our citizens. I am confident that we are closer now, but I am also confident that the world is changing so quickly and access to information, databases, and technology is so rapidly evolving, that we can not simply rest on such assurances. Such advice need not just apply to the fusion centers, but perhaps to any entity that utilizes intelligence and information sharing as a prevention, protection, and mitigation tool. As information becomes more readily available, and the risks (as well as the benefits) are more easily multiplied, we must formalize structures and policies that embrace the debate, rather than deny or ignore it. We are not alone in our State, and to the extent that DHS can serve as a model or provide the very practices we all are seeking to achieve, we will ensure that we will take the proper steps to protect privacy and civil liberties, while continuing to utilize the mechanisms of intelligence and analysis that help protect our citizens from critical incidents.

I hope I have provided you with useful information to assess and enhance DHS I&A. I have discussed the issues that are at the forefront of the CFC's concerns; which we know also hit home with many other fusion centers. Efforts on the part of DHS and the Federal Government to address the issues that were raised today offer a solid basis for making improvements and continuing useful efforts by I&A.

ATTACHMENT

The Commonwealth of Massachusetts
Executive Office of Public Safety

One Ashburton Place
Boston, Massachusetts 02108
Tel: (617) 727-7775
TTY Tel: (617) 727-6618
Fax: (617) 727-4764
www.mass.gov/eops

Deval L. Patrick
Governor

Timothy P. Murray
Lieutenant Governor

Kevin M. Burke
Secretary

March 10, 2008

Dear Ms. Rose and Mr. Reinstein,

In response to your letter of December 12, 2007, regarding the Commonwealth Fusion Center (CFC), as well as a subsequent conversation we had, the Executive Office of Public Safety and Security (EOPSS) has worked with the CFC to provide you with an honest, comprehensive response to the issues and concerns you have raised.

We would like to take this opportunity to address your more general claims about fusion centers – and why they do not apply to the CFC – as well as your specific claims that the CFC has not been transparent in terms of what it does, what information it collects, and how this information is being shared and used.

In response to your assertion that most fusion centers have ambiguous lines of authority, this is not the case with the CFC. While the CFC has partners from appropriate state and federal agencies and takes strategic guidance from the Department of Homeland Security (DHS), the CFC's chain of command ends with the Colonel of the State Police, who is under the authority of the Secretary of Public Safety and Security and ultimately the Governor. The core of the CFC is staffed with Massachusetts State Police (MSP) personnel, who first and foremost are responsible up their chain of command. Representatives from other agencies include one Federal Bureau of Investigation (FBI) analyst, one agent and one analyst from the Bureau of Alcohol, Tobacco, Firearms and Explosives, one counter-drug analyst from the Massachusetts National Guard (MANG), one analyst from the Department of Correction (currently deployed to Iraq), one representative from the DHS Office of Intelligence and Analysis (I&A), one police officer from CSX railroad, and a Geographic Information Systems (GIS) specialist from the U.S. Army Civil Support Team. In addition, several MSP troopers under the direct command of the CFC, and therefore EOPSS, are assigned to the FBI Joint Terrorism Task Force (JTTF) for specific investigation support.

The CFC actually has several core functions. These include its role as the repository of traditional criminal law enforcement information so that localities and regions can work together to share criminal information about specific investigations, arrests, warrants, and trends. It also includes issues involving critical infrastructure assessments (i.e. managing a statewide database, known as ACAMS, which assesses vulnerabilities), serves as a missing children information clearinghouse, and promotes uniform crime reporting and gun tracing. All of these different roles are subject to strict standards. This letter specifically addresses your concerns with the CFC's role as an intelligence repository or intelligence gathering entity and the standards that govern this role.

Printed on Recycled Paper

As an initial matter, because of the necessity for joint federal/state interaction, an MOU has been implemented between the FBI's JTTF and the MSP, in order to clarify and delineate roles and responsibilities. The JTTF's core function is to investigate terrorism related crimes. The representative from the DHS I&A is present at the CFC to facilitate the coordination and flow of information, provide expertise in intelligence analysis and reporting, coordinate with local DHS and FBI components, and provide DHS with local situational awareness and access to appropriate CFC information. The DHS representative is not involved in intelligence collection in any way. These limited roles and responsibilities will be codified in an MOU between DHS and the CFC soon.

Regarding the CFC's authority over data collection and retention, and their policies for privacy and civil rights, the CFC's National Standards for Intelligence Sharing policy (CFC-07, enclosed) follows national best practices. The policy voluntarily adopts the National Criminal and Intelligence Sharing Plan, the Global Justice Information Sharing Initiative, and the Criminal Intelligence Systems standards under Title 28, part 23 of the Code of Federal Regulations (28 CFR 23). The latter provides criteria for the submission of criminal intelligence, requiring reasonable suspicion of a criminal act before data on individuals or groups can be collected. The mandates of the 28 CFR 23 also require controlled dissemination of that information, information review, and a five year purge of unused information. The DHS representative at the CFC is also bound by 28 CFR 23, any internal regulations set forth by the CFC, and Executive Orders 12333 and 13355 (governing United States intelligence activities), which specifically address retention of personal identifying information on DHS computers or I&A databases.

You have also raised concerns regarding private-sector and military involvement, date mining, and excessive secrecy. With respect to private-sector participation, the sole quasi-private representative is the officer from CSX railroad who serves to ensure that rail-related intelligence is disseminated widely to our rail transportation assets and to work on critical infrastructure analysis. The CFC does communicate when appropriate with the private sector (particularly critical infrastructure). For example, members of the private sector are educated on indicators of terrorism and are encouraged to report suspicious activity gathered in their normal course of business that fits the indicators. Law enforcement sensitive information (covering CORI, among other things) is withheld from the private sector.

In terms of military participation, the CFC has one MANG counter-drug analyst.[1] His duties are solely to provide analytic support for narcotics investigations, as well as to support other counter-drug operations as requested. In addition, the MANG Civil Support Team (which supports emergency response, not intelligence) collaborates with the CFC GIS analyst on a monthly basis.

No "wholesale data collection" goes on at the CFC. Data is collected and maintained in accordance with 28 CFR 23, based on suspected criminal activity.

As to claims of excessive secrecy, the CFC has presented to various audiences on fusion center functions. The CFC will gladly meet with you to discuss their operations and tour their facility. The CFC will continue to respond to all appropriate inquires with transparency and honesty.

Your letter states that the CFC has no civil rights protection policy. In fact, there are two policies governing this issue. The CFC recently revisited and revised its standard operating procedures,

[1] Under United States Code Title 32, this MANG analyst is serving under state duty/authority.

including its Guidelines for Investigations Involving First Amendment Activity (CFC-04, enclosed). This document details the general principles and applicability of the CFC's policy:

> It is the policy of the Commonwealth Fusion Center (CFC) that its members will not initiate or participate in investigations into groups or individuals based solely upon their lawful exercise of First Amendment rights. Where the CFC must initiate or participate in investigations involving First Amendment activity, its policy requires that those investigations conform to the guarantees of the Massachusetts Constitution, the United States Constitution, state law, and federal law. It also requires that those investigations be supported by a legitimate law enforcement or public safety purpose.

An additional CFC privacy policy, previously released to you (CFC-05), embraces privacy design principles developed to ensure that safeguards and sanctions are in place to protect personal information. The policy addresses issues ranging from clearly articulating mission-specific reasons for using information to ensuring data quality and maintaining effective security over personal information. In addition, it is clearly stated in the CFC privacy policy that "all agencies participating in the CFC will make this privacy policy available for public review."

The ACLU also claims that the CFC has wide-ranging data on individuals with no oversight to govern its use and protect against violations of privacy and civil liberties. In addition to the privacy and First Amendment policy standards adopted by the CFC, EOPSS is working with the CFC to develop and establish an advisory group, as suggested by the U.S. Department of Justice and DHS in their "Fusion Center Guidelines" publication. The general function of the CFC advisory group will be to provide oversight and regular review of the policies, procedures, guidelines, organizational structure, and resources of the CFC as they relate to homeland security issues. The advisory group will serve to guarantee that the CFC functions with maximum effectiveness, while continuing to protect the rights and liberties of citizens, through continuous review and updating of policies and procedures. The Governor's clear intent is to maintain a center that maximizes our capabilities to enhance public safety while steadfastly maintaining the privacy, rights and trust of the Commonwealth's citizens.

We recognize and hope we have addressed your concerns with the CFC. Our goal, like yours, is to continue to support our criminal and counter-terrorism needs with as much transparency as possible.

Sincerely,

Juliette N. Kayyem
Undersecretary for Homeland Security

CC: Secretary Kevin Burke, Executive Office of Public Safety and Security
Mr. Ben Clements, Chief Legal Counsel, Office of the Governor
Attorney General Martha Coakley

Ms. HARMAN. Mr. Cilluffo.

STATEMENT OF FRANK J. CILLUFFO, DIRECTOR AND ASSOCIATE VICE PRESIDENT, HOMELAND SECURITY POLICY INSTITUTE, GEORGE WASHINGTON UNIVERSITY

Mr. CILLUFFO. Chairwoman Harman, Ranking Member Reichert, distinguished members of the committee, thank you for the opportunity to testify before you today. I will be very brief, not my strong suit. As you know, I have never had an unspoken thought. I want to pick up on a couple of themes we have heard here and expand on two or three that I think are significant.

Firstly, that the title of the hearing is spot on. That should be the priority of I&A at the Department of Homeland Security. I am not sure they have seen it that way thus far.

While it has become a cliche, timely, accurate and well informed intelligence and information products shared both vertically and horizontally, at all levels of government are more important than ever to inform us about threats, solutions and responses.

Collectively these capabilities build our understanding of the adversary. We tend to focus so much on the indication and warning. The reality is we need to know the context by which this fits in and it is sort of looking for the needle in the haystack. So I think there has been too much emphasis on the warning side and not enough on the broader strategic function. Not only at the State and local level, but at the Federal level as well.

Collection is sexy. We all like to steal secrets and we all like to have secrets. The reality is what does it mean? How can you use it? Is it usable and how do we operationalize it—I think is the real issue we need to be working toward.

While I agree with Matt and Juliette there has been some progress, and I think the national strategy is a good case in point of that, at least in theory if not fully in practice. At least people are now at a point where they understand. I think everyone is getting to the recognition of the need to share vis-à-vis the old need-to-know model.

When I sit down with my State and local authorities, whether they are in the intelligence shops at NYPD or LAPD or any city throughout the United States, two common themes keep coming back to me. One, without a seat at the table in Washington, they cannot, as much as we talk about it, be true partners in the intelligence and information-sharing process. At the same time, the maximum of think globally, act locally should apply to all of our efforts here.

Much of the information that is collected from State and local authorities don't find its way into any national pictures or frameworks or assessments. Many of the products that the national community is providing don't meet the very specific needs that their State and local authorities have. So I sort of see three approaches that DHS I&A can take to try to remedy this approach.

Firstly champion, champion, champion. Serve as the champion for State and local in Washington and within the Beltway, setting standards, designing customer driven intelligence products and processes. In essence, readjusting the entire requirement setting process to meet their needs. This includes I&A inserting itself into the national intelligence priority framework, a very elite table, but I think they should have a voice in that.

I personally believe that I&A has spent too much time proving that they deserve to be a member of the IC and not enough on some of the customers, which is their true, real differentiator at State and local. Secondly, it should enable its State and local partners. To me, the big gap is not the bricks and mortars, it is analytical capacity.

We need to ensure that an analytical capacity, people. Ultimately this is all about people. We need to start investing in people and

make those capabilities and capacities available to our State and local partners.

We love Fusion Centers, they are positive, and they are good and there have been very positive developments there, some better than others. What we really are missing is what comes out of that. That is more of a data collection focus. I would like to see greater analysis. I would like see how that can be strung up together. This is where I&A play a very important role to take regional approaches. What are we seeing in one area, what are we seeing in another and how do we can put those pieces together.

I listed a bunch in my prepared remarks of new products that I think would be helpful. Much of them focused on understanding the adversary, because quite honestly, there is still a dearth of that. I think that some of these deliverables can and should be done instantaneously. It is not in the United States, it is really what are we seeing overseas? What trends are important? What indicators are important? How can that be factored into suspicious activity reporting at the local level? What are we seeing in terms of modus operandi in combat situations? What are we seeing outside of combat situations? What are the trends? I am not sure that that has been done effectively.

Secondly, I think CBP is a unique aspect of DHS and that should be better integrated into our information sharing efforts with State and local.

I think that as Juliette mentioned, some of the videos quite honestly, I think we do need more of that. We need to understand the terrorist narrative, not just what the actions are, but what is making them tick. How can we get to a lexicon where we can communicate with our communities? Ultimately, the solutions are going to be community policing, hopefully intelligence-led, and that to me should be a major, major priority.

One pagers: I would like one pagers of every terrorist incident we have seen overseas. Simple. I would like to see one page about not only incidents but what about thwarted incidents and how are they thwarted and why were they thwarted? This is something that I think could be very valuable. If DHS I&A doesn't provide it, Madam Chairman, and I realize this may be outside of the jurisdiction of this subcommittee, perhaps others, such as FBI and NCTC should be given the authority and responsibility to do so.

On the enabling side my colleagues said it much better than I ever could, but let me recognize the importance of privacy. This shouldn't be an afterthought, it shouldn't be a perfunctory last paragraph in every document. It needs to be part and parcel. It is not just the civil liberties and civil rights communities inside government, but the broader civil rights communities should have a voice. Even if we all can come to some conclusion, it won't work if it doesn't have the trust of the community. Trust and confidence is at the bottom of all of this. That includes the communities that ultimately we all serve. So I would just highlight that, accentuate that and I will stop at that. Thank you.

Ms. HARMAN. Thank you very much.

[The statement of Mr. Cilluffo follows:]

PREPARED STATEMENT OF FRANK J. CILLUFFO

APRIL 24, 2008

Chairwoman Harman, Ranking Member Reichert, and distinguished Members of the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee, thank you for the opportunity to testify before you today. The role of intelligence is the lifeblood in the campaign against terrorism and other threats. Your leadership in examining intelligence issues as they relate to the Department of Homeland Security better serving State, local, tribal and other stakeholders is to be commended. This should be the primary mission of the Office of Intelligence and Analysis.

Officials at the State, local, and tribal levels and their counterparts in the private sector are often the first preventers and responders to terrorism and other security threats. Timely, accurate and well-informed intelligence and information products, shared vertically and horizontally with all responders at all levels of government, are more important than ever in order to inform them about threats, solutions and responses. Collectively, these capabilities build our understanding of the adversary. Already, we have made some headway toward this end in theory, if not entirely in practice. A National Strategy for Information Sharing exists.[1] We are moving toward creating an effective Information Sharing Environment—one supported by a culture based on a "need to share" rather than merely a "need to know." Notably, the National Strategy references the crucial role of State, local and tribal partners in an effective counterterrorism effort. However capable our intelligence apparatus' may be, this is ultimately an exercise in risk management; intelligence simply has limitations. Intelligence estimates, for example, are just that: analysts are not and cannot be expected to be clairvoyant.

In the course of my work as the Director of The George Washington University Homeland Security Policy Institute, I have worked with a range of State and local intelligence and law enforcement officials. Two common themes have emerged among my discussions with them: without a seat at the table in Washington, they cannot be true partners in the intelligence and information sharing process; and at the same time, the maxim of "think globally, act locally" should apply.

Information collected by State and local partners does not always make it into national intelligence assessments, while the products they receive often do not meet their unique needs. The Department of Homeland Security's Office of Intelligence and Analysis has the potential to remedy this through three steps. First, the Office should champion State, local, and tribal stakeholders within the Beltway, setting standards and designing customer-driven intelligence products and processes, such as the National Intelligence Priority Framework. Second, it should enable its State and local partners by investing in analytical capabilities in existing information sharing venues like Fusion Centers and operationalizing that intelligence. Finally, it can work to integrate fully intelligence collection and analysis at all levels of government, producing the first truly all-source, all crimes and all-hazards domestic threat assessment. Respecting and preserving civil rights and civil liberties is crucial in all of this, and the Department's Office of Civil Rights and Civil Liberties should be at the forefront of these efforts, consulting and incorporating to the fullest extent possible the views of the broader civil rights and civil liberties community.

CHAMPIONING STATE, LOCAL AND TRIBAL STAKEHOLDERS AT THE NATIONAL LEVEL

Just as many law enforcement duties and policies are the purview of State and local governments, so too should many corresponding intelligence functions. While Federal agencies rightly should be concerned with transnational threats against our homeland, allies and interests abroad, relying solely on Washington, DC-based agencies for State and community-based intelligence needs ensures local requirements and concerns do not receive the priority they deserve. No one has a better grasp of communities and their particulars than local officials and partners. Thus, while products such as National Intelligence Estimates and programs such as personnel rotations to different intelligence details are important at the national level, the Office of Intelligence and Analysis should ensure State and local partners receive the priority they deserve by representing them at the national and homeland security planning tables, setting priorities and requirements and designing products that meet the unique needs of these partners.

That said, intelligence and analysis on terrorist tradecraft including weapons, financing and modus operandi currently used in combat environments and other tar-

[1] National Strategy for Information Sharing, The White House, October 2007, *http://www.whitehouse.gov/nsc/infosharing/*.

gets of terrorism far from our own municipalities can be useful for domestic purposes. Knowing what and who we face abroad can serve as a positive tool for creating policies, fine tuning tactics, and collaborating on threat indicators among other responses at the local level. As past events have indicated, our geographic isolation from regions frequently affected by terrorism is but a small impediment to those seeking harm against our homeland. The need to think globally and act locally necessitates creating a mechanism whereby State and local partners are kept in the loop regarding national intelligence assessments of international terrorism and transnational crime. The Office of Intelligence and Analysis should ensure partner agencies and officials receive current national intelligence assessments that can be integrated into State and local law enforcement practices.

The Office of Intelligence and Analysis should also take the lead in designing new intelligence products such as the following:

- Regional Threat Assessments, produced by Fusion Centers incorporating intelligence gathered at the State and local levels across a geographic region, would focus on trends in suspicious activity, radicalization, threats to critical infrastructure and other local concerns.[2] Such assessments would, for the first time in many cases, not only make State and local authorities aware of threats and key vulnerabilities in neighboring jurisdictions, but also in those across the country. Besides raising awareness of terrorist and criminal indicators throughout different jurisdictions, Regional Threat Assessments would indicate similarities and differences in how State and local authorities collect intelligence, as well as in what they are collecting. Similarly, these assessments would allow State and local officials to compare threats at a broader level, thereby enabling them to more easily spot trends between different jurisdictions. The Office of Intelligence and Analysis would prove vital to ensuring that information collected at the local level is fed into relevant analysis and that the analytical capacity is in place to turn the intelligence into products to be shared among disparate jurisdictions.
- Along with Regional Threat Assessments, other threat assessments incorporating intelligence gathered overseas that is directly relevant to State and local responders would be produced. These products would include information on threats to the homeland arising overseas, trends in radicalization and counter-radicalization abroad and intelligence collected at U.S. borders by Federal agencies. U.S. Customs and Border Protection, for example, is a unique Department of Homeland Security asset and information collector that should be better incorporated into the intelligence capacities of local and State partners with points of entry within their jurisdiction. The Office of Intelligence and Analysis should act as that enabler. Another example of a best practice that should be further disseminated and replicated is the Integrated Border Enforcement Teams (IBETs) which bring together Canadian and U.S. border security agencies at 23 locations. Intelligence gathered abroad is already available; what is needed is for the Office of Intelligence and Analysis to ensure national collection assets collect the information needed by all levels of government, and that products provided to State and local responders meet their unique needs.
- A virtual library of key documents, statements, video propaganda, and other materials produced by our adversaries would be established and maintained by the Office of Intelligence and Analysis for its State and local partners. This would provide State and local responders with a better understanding of our adversaries' intentions, capabilities, and tactics, but also the narratives they use to spread their appeal—information needed to identify and counter radicalization and emerging threats in their own communities. It could also help State and local responders develop a lexicon for effectively discussing issues of terrorism and radicalization with their communities. In particular, they need more and better analysis, providing a multidisciplinary understanding of our adversaries' motivations, thoughts, and plans. While indications and warnings of possible attacks are vital, better understanding of our adversaries will allow our first responders to move toward preempting and disrupting terrorist activities before they take shape.
- Incident reports providing background on and summaries of international and domestic terrorist actions (including actual incidents and those that were thwarted) would be produced and collected by the Office of Intelligence and Analysis and placed into a virtual data base that would supplement the virtual

[2] The regional approach has merits beyond the intelligence context. See, for example, *Regionalizing Homeland Security: Unifying National Preparedness and Response,* The George Washington University Homeland Security Policy Institute, June 30, 2006, *http://www.gwumc.edu/hspi/pubs/hspiregion.pdf.*

library. These incident reports would inform State and local partners of terrorist activity and trends outside their jurisdictions. Two examples of open source terrorism incident data bases are the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland and the Memorial Institute for the Prevention of Terrorism's Terrorism Knowledge Base.

- Information gathering and reporting processes would be standardized by the Office of Intelligence and Analysis through requirements setting. The Los Angeles Police Department, for example, recently introduced Suspicious Activity Reports (SARs) for its officers to report in detail any kind of potential terrorist-related activity, which fits seamlessly into their daily operations. Department officers have been receiving training in what kinds of suspicious activities to look for based on a 65-item checklist which includes indications that someone conducted surveillance on a government building, tried to acquire explosives, openly espoused extremist views or abandoned a suspicious package, for example. SARs represent a best-practice that could be used at the State and local levels across the country to feed information into customer-driven products like the Regional Threat Assessments. These best-practices are already being implemented by State and local responders; what is needed now is for the Office of Intelligence and Analysis to act as a champion of the SARs in order to implement the program with other partners in a manner that promotes information sharing as broadly as possible. Analysts from the Office of Intelligence and Analysis could take a SAR, for example, and fuse it with other intelligence including that from Fusion Centers, and create a product that is broad but recognizes both a community's unique aspects as well as incorporating regional and national trends.

This is not meant to be a comprehensive list, but to illustrate some of the information products and resources that State and local responders need—and are not necessarily receiving—in order to secure their communities. By championing its State and local partners at the national level, the Office of Intelligence and Analysis can set new priorities and requirements at all levels of government in order to produce these vital and currently overlooked products. While this may be beyond the jurisdiction of this subcommittee, it is important to note that if the Office of Intelligence and Analysis does not take on this role, then others such as the Federal Bureau of Investigation or the National Counter Terrorism Center should be given the authority and responsibility to do so.

ENABLING STATE, LOCAL AND TRIBAL FIRST PREVENTERS & RESPONDERS

Ultimately, the solutions to terrorism and related threats will be local in nature—through localized analysis, community policing, and counter-radicalization that starts from the ground up. More than just setting requirements and providing products needed by State and local entities, the Office of Intelligence and Analysis must enable and empower State and local responders to be true partners in information analysis and sharing—that is, in fighting terrorism.

This means, first and foremost, investing in analytical capacity. Throughout our country's intelligence community, there is an emphasis on collection over analysis. This is especially true with regard to the State and local levels, where many responders lack the resources or capacity to conduct analysis on their own. The New York Police Department and the Los Angeles Police Department offer two exceptions to the rule: both departments have developed effective intelligence collection and analytical capabilities, to their great credit. While there may be a few other exceptions, most municipalities and States do not have the resources to develop similar capabilities on their own, nor necessarily should they. This is not to say that stop-gap measures do not exist. For example, a wealth of open source information concerning our adversaries worldwide is available to State and local officials by the Department of Homeland Security through the Universal Adversary internet portal, a tool that is not yet well known. Training and educating State and local consumers of intelligence analysis on how best to make use of tools such as this is also important.

State and local responders often do not have much luck when turning to avenues of information sharing with the Federal Government. Facing a virtual alphabet soup of State and Federal offices and agencies to contact, it is often difficult to even know where to turn. Even when it is clear, analytical capacity is usually given second billing after collection. Principal Deputy Under Secretary for Intelligence and Analysis Tomarchio, for example, noted in recent testimony that the Office of Intelligence and Analysis now has 23 officers deployed and serving in Fusion Centers around the

country.[3] While this is a positive step, it should be noted that this amounts to a little more than a third of an analyst per Fusion Center, excluding municipal police departments. To remedy this, the Office of Intelligence and Analysis should continue to deploy its own analysts to Fusion Centers and other points of cooperation, working to build out the analytical capabilities of these organizations. The burden of championing, enabling, and integrating the capabilities and goals of State and local partners should not fall to the Department of Homeland Security alone. Rather, sustained, long-term investment of both capital and personnel resources by the White House, various cabinet and sub-cabinet agencies, along with this and other Congressional bodies is necessary to increase the analytical capacities of and access for State and local partners. Unfunded mandates are not the answer, and it is important that Congress remain cognizant of the need for sustained investment in this area over the long run.

The key goal of the Office of Intelligence and Analysis, however, should not be to continue the trend of top-down driven analysis. Instead, it should work to develop the analytical capacity from the bottom-up, by providing the required resources and training, disseminating lessons learned and best practices at home and abroad, and by identifying and filling gaps in capabilities for its State and local partners. For example, the Office of Intelligence and Analysis could enable State and local officials to gain hands-on experience through international partnerships and exchanges, most of which are outside the financial reach of State and local responders. Working with their counterparts overseas, State and local officials can gain greater understanding of how terrorists operate internationally, what counterterrorism approaches are being implemented abroad, what radicalization and counter-radicalization look like on the ground, and on-the-scene situational awareness.[4]

While some information such as a better understanding of our adversaries will likely come from the national intelligence community, intimate knowledge of local communities will not be found in Washington, DC. State and local law enforcement, fire fighters, emergency medical services and others are truly on the front line against terrorism; they are not only the first to respond to an attack but, knowing their communities best, are the best-placed to identify and thwart radicalization and emerging plots before they become critical threats. Though terrorist threats are often transnational in nature, the solutions are primarily local. While the brick-and-mortar infrastructure of Fusion Centers and related entities are important, it is people who are critical—individuals trained and prepared to conduct intelligence analysis and intelligence-led community policing.

These last two are essential. I have often said that in the struggle against terrorism, we cannot simply kill or capture our way to victory, but instead must utilize all instruments of statecraft to undermine the appeal of our adversaries' narrative.[5] This is as true abroad as it is at home. Here, we cannot rely on the hard edge of policing by arresting our way to security. Instead, through community policing and engagement—earning the trust of communities, informing the public, identifying suspicious activities and signs of incipient radicalization, and discerning and diminishing grievances—we can undermine the appeal of our adversaries' narrative at home as well as abroad. The Office of Intelligence and Analysis can play a role not just by enabling and empowering State and local responders to develop their own analytical capabilities, but also by disseminating good work being done in the field of community engagement at the Federal level.

BRINGING STATE, LOCAL, AND FEDERAL TOGETHER

Like much of the Department of Homeland Security since its inception, the role and structure of the Office of Intelligence and Analysis has evolved over time. The Office's integration within the Federal intelligence community as well as with local and State partners is both necessary and challenging. It is important to remember that this integration is a process, the end of which we have not yet reached. As we look to ways to better integrate all levels of government, to enable and empower

---

[3] *Focus on Fusion Centers: A Progress Report.* Testimony of Principal Deputy Under Secretary for Intelligence and Analysis Jack Tomarchio Before the Senate Committee on Homeland Security and Governmental Affairs Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration, 17 April 2008.

[4] *LEAP: A Law Enforcement Assistance and Partnership Strategy: Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement.* Prepared at the request of Congressman Bennie G. Thompson, House Committee on Homeland Security, pp. 10–12.

[5] See for example, *NETworked Radicalization: A Counter-Strategy,* The George Washington University Homeland Security Policy Institute and The University of Virginia Critical Incident Analysis Group, *http://www.gwumc.edu/hspi/reports/NETworked%20Radicalization__A%20Counter%20Strategy.pdf.*

State and local responders, and create a customer-driven intelligence environment, the Office of Intelligence and Analysis will develop the capability to produce a truly powerful intelligence product: a comprehensive National Intelligence Estimate (NIE) addressing threats to the homeland, both foreign and domestic.

Currently, the National Intelligence Council (NIC) provides, among other products, high-level estimates of global trends.[6] Within the NIC, however, there is no National Intelligence Officer (NIO) or deputy NIO from the Department of Homeland Security. This means that a domestic threats security perspective, including systematic input from State and local officials, is not fully provided. The quick fix of a deputy NIO from the FBI did contribute to the July 2007 NIE on threats to the homeland. Looking to the future, however, the responsibility for domestic threat assessments ought to reside outside of the Intelligence Community.

Within the larger discussion of the evolving role of the Office of Intelligence and Analysis, privacy protections must play a central role. Protecting civil rights and civil liberties must not be an afterthought to the discussion of how to effectively collect, share and disseminate intelligence. Rather, ensuring the privacy of Americans should be part-and-parcel with the intelligence and analytical objectives and goals of the Office of Intelligence and Analysis. As more agencies at all levels collect and share information on more facets of our lives at the community level, the opportunity for even the well-intended to cause privacy violations increases. This is problematic not only from the standpoint of an ordinary citizen concerned with their privacy, but also from an operational perspective. If communities view first responders, for example, as intelligence collectors with too broad a mandate, a lack of trust will develop, making it impossible for first responders to fulfill their primary roles and closing off an important avenue of information sharing with their communities. As Benjamin Franklin noted well before intelligence became a specialized discipline, "Anyone who trades liberty for security deserves neither liberty nor security."[7]

By establishing clear and transparent guidelines on the protection of civil rights and liberties, and by designing and providing appropriate training to State and local partners, community-based intelligence programs will not be marred and undermined by concerns of the potential for privacy violations.

For any new intelligence or information sharing program, or collaborative effort through the Department of Homeland Security to be successful, it is critical for the Office of Intelligence and Analysis to build trust and confidence with public and private partners across all governmental levels to better serve its customers. That credibility will allow the Office of Intelligence and Analysis to serve three key functions for its State and local partners: serve their intelligence needs; enhance their creativity, resources and potential; and advocate within the Beltway for enhanced cooperation, funding and other critical resources to help State and local partners better serve their communities. Enhanced intelligence capabilities across local, State, regional and national levels will lead to better community security and ultimately our Nation's security.

It is important not to get lost in the bureaucratic weeds. What we're talking about here today is simple: finding ways to making the good work being done by responders at all levels of government easier and better by connecting all of their efforts together. Since it takes a network to defeat a network, it is essential that we enhance our Nation's responders' interconnectivity and information-sharing capacity. This is one of the most powerful force multipliers for homeland security.

With that in mind, there is a need to de-mystify intelligence and its role in policymaking. As we all know, a little black box with unearthed secrets that is accessible to only those with a sufficient security clearance simply does not exist. Intelligence should play a supporting function—a means to an end rather than an end in and of itself. But those intelligence means are critical to providing national and community-based officials alike with the necessary tools to enable closer cooperation, more informed decisionmaking and more nuanced policymaking. It is the people, not the programs, that are doing the work—and it is in people that the Office of Intelligence and Analysis should be investing.

I wish to thank the committee and its staff for the opportunity to testify before you today, and I would now be pleased to try to answer any questions that you may have.

---

[6] See for example the July 2007 National Intelligence Estimate: *The Terrorist Threat to the U.S. Homeland, http://www.dni.gov/press_releases/20070717_release.pdf.*

[7] An Historical Review of the Constitution and Government of Pennsylvania (1759).

Ms. HARMAN. Each of you anticipated most of my questions. I thought your testimony was excellent and now we will go to the questioning round and I am yielding myself 5 minutes.

Mr. Bettenhausen, enlist, entrust and empower, I think, will become the new committee mantra. Any objections? When we print our coin, if we ever print such a thing, that is what it is going to say, so thank you for that.

Mr. BETTENHAUSEN. Hopefully I will get that first challenge coin.

Mr. PERLMUTTER. Coordination, collaboration, cooperation.

Ms. HARMAN. There we go. We will have a committee meeting on that later. We will put that on the back, then.

More seriously, we have been fighting here, I don't think that is an incorrect word to get the ITACG, and you all are familiar with it. It was set up as a creation in order to accommodate State and local participation, because the NCTC did not want that participation directly as part of it, you can correct me, but at any rate, my view was set up to accommodate State and local participation. We have had this long fight about how many people to include, whether they need clearances, whether they gets desks and pencils, what role they play, whether the products they work on should show the fact that they are part of the NCTC, et cetera. It has been difficult and it required a legislative fix. Language was added to the 9/11 Act last year to compel their inclusion. It took a long time, things are getting better. We are moving in a proper direction. I would argue that it could only go up. Nonetheless in talking with Mike Leiter, the new head of the NCTC, he has told us on the record and in meetings of the value added by this participation. Example, when there was a ricin incident in Las Vegas, he pointed out it was the State and local participants who said that the product describing that should describe what ricin looks like, and how much of it is harmful, and what you do about that. It seems obvious to me, but apparently the intelligence product that had been written at 30,000 feet didn't include that. So it didn't give direct guidance to State and local and tribal partners about what to do.

I appreciated your comments, Juliette, about being treated like children. State and local partners are the people who are going to uncover the next terror attack. It is not going to be me, and it probably isn't going to be you—although it might be—but those are the folks, like Sheriff Reichert who need to have the actionable information. So we have to get this right.

I just want to give each of you an opportunity for more comment on this. I appreciated, Frank, your addition of privacy concerns. It is certainly my view and certainly the committee shares it that those have to be built in on the front end. It is not something you add later. The way I put it, is that privacy and security are not a zero sum game. You either get more of both or less of both. Ben Franklin actually said that a long time ago, even before you skip. It wasn't an idea that you generated. So could you each respond to this notion of full inclusion, what it really means, at least in terms of the Federal agencies that we directly regulate and what about privacy.

Mr. BETTENHAUSEN. Thank you. I share your concern and I also share frustration. That should not have been an 18-month battle. It was appalling the amount of time wasted by leadership at the

State, local and Federal level to get State and locals a seat at that table. It was common sense. That is time we are not going to get back. It should not have been that way. Most of the Federal agencies supported it. Some did not. But that battle is now over, thanks to your intervention on the grant funding. We have to get the Department to fix this.

We are going into an election period, a transition period. These Fusion Centers are new, there is a shortage of analytical capability in Federal agencies and there is also at the State and local. At the same time, we have DHS telling us either come up with your own State funds or lay off those analysts, and push them out the door in the midst of this high-risk environment. The need to develop these capacities and capabilities is appalling and more time wasted.

Since information bulletin 235, I am appalled when I think about how much time we have wasted arguing over an information bulletin when our time could be spent on improving actual products, preparedness an protection activities.

Ms. HARMAN. Thank you. Ms. Kayyem.

Ms. KAYYEM. Thank you.

Ms. HARMAN. Is your microphone on?

Ms. KAYYEM. Excuse me, let me go back. On this sort of why do States need this information as sort of key players, and that is what I think is often forgotten. Your ricin incident is perfect. What does it look like? It is because we have the capacity to get out to the people who are going to actually walk in the front door and say something. We can distribute that information and we have databases. It is bringing the Intelligence Community down a notch from wars and the stuff over there and the threats and IEDs.

There is local and State emergency management, public safety people who are going to walk in the front door and what do you want them to know? On my publisher scenario it really puts the States in a dilemma. The lack of tactical or strategic advice given by DHS on the information coming out. I say I, it is not me, the Fusion Center, whoever is in the dilemma of either distributing intelligence that might trigger operational reactions that are not validated by the intelligence itself.

If I send out a Hamas leader was killed, let's all be worried. I don't know how that will be interpreted by a local police chief. So I have either that dilemma or we hold onto it and then we are creating the very stovepipes that this whole venture meant to destroy. So it is a dilemma for us. If we could bring the Intelligence Community—I say down, but that may not be right. Why do we want to know this? It is not just because we just want to be in the know. There is actually operational needs that we have.

On the civil liberties—I am embarrassed that I talk too fast, your timer went off when you spoke, I wonder if you have an in.

Ms. HARMAN. Mine is off now.

Ms. KAYYEM. No, but on the privacy issue it is something I have been focused on in my previous capacity. We are embarking on a privacy council, and it is not just intelligence. The way the technology is changing means that people have to have assurances that we are looking at this, that this is at the front end, because if something goes wrong and it inevitably will, we don't want to be

following the last crisis. We want to be in a position where we can regroup, say it was either a mistake or consistent with our guidelines, but have the policies and practices in place now so they can guide people who are not lawyers, who do not think about this every day as they shouldn't. We guide them in how they deal with these issues in the future.

Ms. HARMAN. Thank you very much. Mr. Cilluffo. I apologize to my colleagues, I'll let you go over your time also if the answer does that.

Mr. CILLUFFO. I'll try to be brief. I don't think it is a very sexy issue. It is requirement setting. It is customer service. That requires, as Juliette was saying, bringing the intelligence down. But I think we have a lot to learn from the military environment where you are, the J2 and J3, the intelligence and operations in separation. Finally there was some recognition, and this is important to understand what intelligence is, it is a means to an end. It is not the end in and of itself.

We tend to talk about it that it is, itself, the end. It supports something, whether it is policy or budget priorities or operations or diplomacy. It is a support function. I think it really comes down to requirements setting.

I do feel that there are some elite tables that State and locals should have a voice at. I am not sure they should be directly representative of, say, the national intelligence priority framework, but someone needs to be their advocate, someone needs to be their champion, someone needs to speak for them, and someone who speaks for them has to understand them. What makes them tick everyday?

We don't want to create little black boxes that are specifically for terrorism. It better work in a day-to-day function environment, not something totally unique and different.

One other thing that I think is important here, there still is this belief and I think we have to demystify to some extent what intelligence is. There still is this belief, if I only had my TSCI clearances, I would have all the answers. I don't want to compromise a secret there, because it is not. It ain't there.

The reality is we need to recognize the limitations of intelligence on collection and analysis. These are estimators, they are not clairvoyants we don't have all the answers. So to me it is requirement setting, it is getting the customer to drive that. That is not easy either. Once the customer has to actually start and think about its specific needs, they are going to find it is not an easy business, but it has to happen that way.

Ms. HARMAN. Thank you, Mr. Reichert.

Mr. REICHERT. Thank you, Madam Chair. I want to go out to a little bit bigger picture. I think we are all in agreement that we don't want to see any major reorganization occur. We are all nodding our heads on that one.

I will share a little story with you. Back when I was the sheriff, I made some trips here to Washington, DC and worked with Vice President Al Gore and his group on a project called Safe Cities. We were one of the ten in the Nation named a Safe City although we were a county. We were the only county in the country a member of this group and it had to do with gun safety.

Well, as the administration changed then, not too long after that there was discussion about ending safe cities which was a very, very successful program. So what we had to do to fight to keep this program in place under a different administration, the name had to be changed. That is the only way that we were able to keep it. People might recognize this, it changed to Project Safe Neighborhoods. So that came from Safe City.

So what my concern is, and what we are all worried about is reorganization. How do we, and maybe you already have begun discussions with DHS leadership and others that you know, how do we minimize any efforts or attempts to reorganization? Or what have you done or what should we be doing to prevent major reorganization? I think this will be—all of the things that you all have talked about so far this morning will be the death knell for all of us and the progress that we have made.

Mr. BETTENHAUSEN. Let me address a couple of those. We, as the National Governance Association of the Homeland Security Advisory Council, meet regularly with the Department. We as a full group met last April with the Department of Homeland Security last April, we will be back here in May. Over a year ago we had already started those discussions about transition.

Again, it is really more of an afterthought that is still happening about what about your most important customers the State and locals? How can you serve us better? The central report that Charlie Allen had done is a good look at how these things need to be done. We are almost getting in too late in the transition process with this particular administration in terms of what they are doing and how they are going to move it forward.

There is a national Homeland Security consortium, we have put together a white paper which will share with the committee that addresses some of the key transition issues. The congressional research service and our friend John Rollins came out with an excellent report on transition as well. This is going to require it, because Homeland Security is bipartisan. Actually, I would say it is a nonpartisan issue. So whoever the nominees are going to be, we want to start working early on with their potential leadership to talk about these potential transition issues, because we do not want to be caught in a transition exposure by being disorganized.

September 11 itself was a transition attack. The 1993 World Trade Center attack was a transition attack with the second month of the Clinton presidency. The transfer of power from Blair to Brown in the United Kingdom saw an attack. We saw the attack in Spain. This is going to require early on and particularly after the election results are known, immediately working with them. Emphasizing again, let's not reorganize this thing to death, let's work on making sure what is working right, continues to work right, and how do we improve what is broken?

Ms. KAYYEM. I would just add simply a new leadership at the Department of Homeland Security to ask a question of each of these entities, but in particular I&A. What do you do that no one else does? We don't have to reorg for that question. What is your value? I mean, it is a simple Kennedy School question, but it actually helps. We think about that all the time because with crime,

and everything else going on, and no money and schools, what are we doing that is something that no one else is doing?

I think I&A is forced to answer that question, we are the answer. That is it. Then you figure out what their priorities are going to do, how they treat us maturely or your three things. Then also, how they get into resiliency, what I call resiliency intelligence. What are the things that are long term that we should be thinking about in terms of critical infrastructure, aging infrastructure and other issues like that? I think if the entity rather than being told to change, move or whatever else, that is simple. What is your mission statement and then I think we go from there, that no one else could have.

Mr. CILLUFFO. To build on some of Juliette's points, I think the value added was more Harvard Business School than The Kennedy School.

First, I think it is very helpful to look at it. Form should always follow function. The reality is what are the mission areas? What needs to be met? What are the customers defining as the mission areas and what needs to be met. From there we can play with the boxes and the org charts, whether it needs to be reorg'd or not. I am not sure it does. What I would suggest is to look at what the mission is, and if it is not being met, give someone the wherewithal to meet that mission.

I would also argue that it shouldn't be an inside-the-beltway process. This has to be organic and some point there has to be with the top down bottom and the bottom up come together. We haven't even discussed the integrate side. At some point, that is where we need to get.

On the actual transition planning, they actually have, I think, based on briefings I have received, done some interesting work. I have got a pretty radical view in terms of some of how this can be improved in the future. I feel that all deputy secretaries should be career civil servants.

The one thing that the United Kingdom handled quite well, the Home Secretary just got her first JTAC briefing, the first intelligence briefing, literally 3 hours before the prevented incident. The reality is home office and the agencies that are running that, the ops guys are much more like the military. You can be promoted but you are a civil servant, so no gaps in terms of what it is doing. So those are my quick thoughts.

Mr. REICHERT. If I could make one quick comment. I want to encourage you to continue with your efforts. The only reason that this project that I talked about changed from Safe Cities to Project Safe Neighborhoods and continued on was pressure by the local sheriffs, police chiefs, mayors and city councils. Keep up the good work. Thank you.

Ms. HARMAN. Thank you, Mr. Reichert. I have to say I totally agree with your thrust here. Mr. Carney.

Mr. CARNEY. Thank you, Madam Chair. Thank you all for showing up today. This is pretty remarkable to have your experience and insight here. My question actually gets more to the heart of how the relationships work between the Federal Government and the State agency. Do you find it evolving, improving, devolving, not getting any better?

Mr. BETTENHAUSEN. You know sometimes you feel like you have made three steps forward and then you wonder whether you have made two steps or four steps back. It is evolving, but it is getting better. There is an emphasis here on DHS today, but this is beyond DHS. The Federal Bureau of Investigation also has a responsibility to be better sharing the information and looking after the customer focus, because as Director Molar has said, it is not just about prosecution. This is about preemption and prevention. That is what we must be doing and that requires a different mindset.

Mr. CARNEY. Right.

Mr. BETTENHAUSEN. I spent most of my career as a Federal prosecutor and I understand this is a sea change in the way that they are doing business. There are cultural and bureaucratic roadblocks that are still there. This requires an attitude that we are going to have these partnerships, and it will be full and equal, and we want to share. Sometimes that is personality driven. You can have a special agent in charge where things are going swimmingly with all of your partners and that can change overnight with somebody else who comes in.

If we establish the precedent, the requirements, the need for these partnerships and that is expected, that is the gold standard, and nothing less will be allowed or you will be removed from that office or be downgraded with your rating. If we don't have that attitude, you are going to have problems. We have it easier outside the beltway. Where the rubber meets the road, we can often get together and resolve some of these bureaucratic issues and work to have a clear sight of our mission of the realities of what must be doing and how we can do in a common sense way. That also requires changes from on top.

Mr. CARNEY. I agree. Something of the pavement and the Beltway that prevents common sense from interfering with what we are doing here.

Frankly you are right, I think if the folks working the problem would check the egos at the door we would get more done.

Ms. KAYYEM. When I took this job, I don't think I had any idea if I just thought about DHS. I agree with you, FBI is there. We have a very excellent SAC and the JTTF that works. So from the DHS entities alone and I think I listed them, we have ICE, Coast Guard, FEMA, a critical infrastructure analyst, chemical industry regulators, TSA and my I&A person and Coast Guard who report up a totally different structure. We are trying to manage it.

Now rightfully, I think DHS is around more of the emergency management side, on the FEMA side more regionally focused. But Coast Guard is its own beast and it always will be I think. But from the management perspective of the State, it can get very difficult. So I sort of applaud efforts to have DHS figure out what their family looks like so when they react to a State it is helpful. I will tell you I have DHS people in the State that other DHS people don't know about. That is how it works. These chemical industry guys come in and it can he be amorphous and unmanageable. It is through personality and phone calls that you are able to do it.

Mr. CILLUFFO. Very, very briefly. I think it clearly has improved since 9/11. The problem is everyone is in the business now, every-

one is a producer or a customer, that it gets confusing. There is a pandemic of plans. There is a lot of tactics and a lot of strategy, but a lot of doctrine that is missing, that is the big gap. I would also argue that it needs to come from the bottom up. That is where we have to invest in capacity for State and local, largely analytical.

There has been some emphasis on the hard edge, meaning law enforcement. There are other customers who need to be part of at least the information loop and informed. EMS, hospitals, firefighters, where do they fit in this process in a way that is cognizant with constitutionality but also privacy issues.

The real point that Juliette hit on, we wrote a very long report that I think about three people read, although Senators Collins and Lieberman, I think, did move it into legislation. We have to go regions on the intelligence side, we have regions. We need a regional footprint that can coordinate the full panoply in assets that the Department of Homeland Security has in support of State and local. I am not suggesting that they assume that role, but I really do feel if they were one big fix it is in the field. All the big fixes are always in the field and opportunities are in the field. I would regionalize DHS.

Mr. CARNEY. Thank you. I will probably have questions later.

Ms. HARMAN. We will have a second round of questions. This is fascinating.

Mr. Perlmutter, you were here before I gavelled the hearing. I just explained that to Mr. Dent.

Mr. PERLMUTTER. Sorry, Charlie.

A couple questions. As I am listening to the testimony, it kind of reminds me of an old science class I had, with the beaker. It, kind of, comes down, and there is a narrow neck, and then it goes out like that.

Just listening to the conversation, I am trying to figure out, assuming we have intelligence-gathering capacity up here, we have all these law enforcement and first preventers, first responders down here, who is in that narrow—I mean, there has to be some channel of communication. Who is in that narrow neck?

Are you, Mr. Bettenhausen?

Are you, Ms. Kayyem? Are you the narrow neck?

I am trying to figure out how, in a sensible way, do we channel up the information from local law enforcement agencies and channel through down to the local law enforcement agencies the intelligence-gathering capacity of the Federal Government.

Mr. BETTENHAUSEN. It is an apt picture. Sometimes, though, I will turn that upside down, too, because, again, this is a bottom-up. They really need to be at the top of the chart, though, at the same time.

But I think what you are looking at and where that focal point needs to be is the State and regional fusion centers. What you heard from all of us saying here, too, is all of the agencies need to be represented there. It is an investment that they need to make in it, because we can overcome a lot of the stovepiping of information, because, look, we are not going to come up with a be-all, end-all one system that is going to fit everybody's needs. It is probably better if we actually have people who are controlling that. Because then, again, that gets to the privacy, civil liberties. Everybody

doesn't have access to that information, but somebody who is trained and responsible for that and from that agencies will have it.

So, but if you have all of them sitting next to each other, sharing information from both top-down and bottom-up, those fusion centers are the ideal place to do that. Juliette—we have better information-sharing with components of DHS in the field and in these fusion centers than the directions that they are getting from headquarters. Sometimes we get the information before them. So that is where—it shouldn't be individuals.

The beauty of most of these fusion centers, too, is it is not owned by a particular State, Federal or local. It is a shared entity. It is about that cooperation and collaboration. That is why it is the perfect vehicle to have people there.

The other thing is, when you have them sitting and working together, there are things that get resolved and also solved just by, you know, the happenstance of, "Oh, by the way, you know, we have this going on"; "Huh, funny, I have seen the same thing in another part of the State." So having them there and integrating across Federal agencies, across State agencies and local agencies, that is how you ensure those globs of information get shared.

But you also have to—it is not just about collecting all these dots. You have to have the analysts and the personnel, as all three of us have talked about, and the Chairs of your Homeland Security Committee, in riding DHS to allow us to prioritize the use of grant funds to have that analytical capability.

Because the ricin example is a perfect example of how State and local perspective can help. The Virginia Tech shooting was another example, where the Virginia State Fusion Center immediately was able to get information out from the bottom-up that this is not a terrorism-related-in-a-broader-sense incident, this is not something requiring every university to start being worried about multiple attacks.

That is the value. We can get this information all the way up to the President and the White House with truly accurate information and not having to get phone calls from five different Federal agencies about what is going on with something.

Ms. KAYYEM. Sir, when you ask about intelligence, there are two types, in my mind.

One would be the actionable intelligence or investigation intelligence. What we have done, which I think works, is the members of the Commonwealth Fusion Center who serve on the JTTF—actually, in, you know, the org chart, but this matters—are members of the Commonwealth Fusion Center and not of the State Police generally. So we view it as there are Fusion Center folks as part of the JTTF.

So that information flow, whether it is specific investigations or whatever else, the principals get briefed quarterly on—we will get the phone call, basically, because of the relationship with the SAC if something imminent is happening.

You know, there is a lot of hoax stuff out there right now. The SAC will call and say, you know, we are sort of looking into this, we think it is a hoax because the FBI in Detroit had something like

this too, where some guy is just trying to get money from us, but we just wanted to let you know.

On the intelligence theme, the transition stuff that we are all coming back to and whatever else, that is the kind of information that, you know, more analysts and the quality of the intelligence is going to matter a lot to make the fusion centers and DHS relevant in this world. Because the truth is, once it is actionable or once it is a specific investigation, it really is—and rightfully so for privacy reasons, for investigation reasons because it is going to go before a court at some stage—a JTTF or FBI matter. DHS recognizes that and needs to, sort of, understand why I keep going back to what is their value added.

Mr. CILLUFFO. I mean, they covered it beautifully. The only thing is I, kind of, do like the beaker analogy. It needs to change, though. DHS I&A should be, at this point, in the interim, that point where it is the—they need to be the champion, the enabler and, ultimately, the integrator in terms of adding value until we actually get the bottom-up that we are all looking for.

But personalities matter; they really matter. This is a people business, and much more so. Trust and confidence can't be written into legislation. It can't be put on a document. That is something where you are in a foxhole, you have scar tissue, you have been through experiences, you have been through good, bad, ugly and everything else. This business, in particular, is run on trust and confidence more than any other.

So how do we get to the point where people aren't exchanging business cards, as we all know, when the balloon goes up, but rather get to know one another as individuals, translate from individuals to institutions, and personalities into processes, realizing that that will change. But don't underestimate the people factor.

Mr. PERLMUTTER. Thank you.

Ms. HARMAN. Mr. Cilluffo, I can't help but observe that trust and confidence would help Congress, too. We would get a lot more done.

Mr. Dent.

Mr. DENT. Thank you, Madam Chairman.

Thank you all for being here this morning.

Mr. Cilluffo, on page 2 of your testimony you stated that DHS should send out, "current National Intelligence Estimates that can be integrated into State and local law enforcement practices." You also ask that DHS make available for its partners a virtual library of key documents, statements, video propaganda and other material produced by our adversaries.

I think one of the complaints we have been hearing from local law enforcement is that DHS is putting out a lot of products, as you know, that don't reflect current intelligence or law enforcement imperatives. I think Ms. Kayyem may have alluded to that a little bit. So there is a little bit of conflict between what I thought the two of you had said.

In light of that, don't you think that supplying the data that you describe could create a, kind of, information overload for first responders? I would like to hear from both you two, because there seemed to be a little bit of conflict in your testimony on that particular point.

Mr. CILLUFFO. There may be some disagreement, but I am trying to focus what I think is the "so what", the "what matters." I mean, when we look at metrics in this environment, I like Juliette's example, publish or perish, but there is also pay for the pound. I mean, we literally—it is not more product, it is better product, it is different product. We need the analytical capacity to be able to absorb that to meet operational needs.

I still go around, and the reason, I guess, I am invited by all the major city entities to talk about national security issues, is very few people really understand the adversary. They understand their communities, but until you understand the adversary, you have two separate worlds, one that is over there, one that is over here, and what are we protecting against?

Mr. DENT. I guess the question is, what would you suggest, then, to better tailor the resources of these needs to reflect the priorities of local law enforcement I guess is the issue?

Mr. CILLUFFO. Yeah, let them set the requirements. That is the idea, that State and local authorities and tribal leaders would actually set the intelligence requirements and the cycle, so it is meeting their specific needs.

Mr. BETTENHAUSEN. Let me just add one point with this that I think directly meshes what Frank is talking about and what we are talking about.

We need the access to this information. It doesn't mean that I need to overload the cop on the beat in his morning call with all this information. But, you know, the things that we are recovering overseas, are they pictures of infrastructure in our State? What are their tactics? Those kind of things our analytical people need to be able to reach back and look into. We have seen the returns on targets. We have received the return of the planning and things. So our ability to have access in the knowledge base, it needs to be there.

Then what we have to do is be smarter about it to make sure that we are not overloading both the individual at the street operational level and their policymakers and the policymakers above us with too much information.

But I am the last one here to encourage and say that we are getting too much, because we will sort through that. We are not getting enough, or at least the right kind of things. But if we have the access to it completely, it also helps us.

Ms. KAYYEM. I am not sure if there is disagreement or not, but let me just get back to where—from the perspective of, sort of, the State consumer, which I have been focusing on in particular, is the quality of what we are getting—maybe it is Frank's point—the quantity is overwhelming. It has become sometimes white noise to us. Really, I would actually say, if less and better, I am happier.

Because the truth is—and we may disagree on this. Because there is so much going on in the world, and I think the bin Laden tapes is a good example. I mean, I got the bin Laden tapes. Right? I can watch CNN and get the bin Laden tapes. Right? From our perspective, it is, how is DHS actually thinking about what is going on as we enter this summer? It is transparent to me, because I talk to Frank and hear from Tom and others and get the reports from Congressional Research Service and elsewhere. But why is that not

coming from the very entity that ought to be thinking about this, in terms of the quality of the intelligence?

I would hope—and I don't know on the example about whether something that is captured or some intelligence that we get, sort of, focused on, you know, a critical infrastructure facility in Massachusetts, that we would be notified of it. Maybe I am, you know—I actually think I have been in situations in which we are.

I think when it gets to the point of, okay, this is Massachusetts-specific or someone is visiting our State and there is some concern about them, at least so far, and as far as I know, of course, whenever we talk about this, that is the part that is working, when it has "Massachusetts" written on it. It is the other stuff that is going on that I am less confident of, because, you know, we don't know.

Mr. CILLUFFO. Can I just build on two quick points? Because I think it is relevant.

I mean, if you take the military example, what is provided to the very pointy end of the spear, the men and women who are really in harm's way, they are provided information in a certain format that literally means life or death in that particular situation. But there is other information that is provided to so many others along the way that need to be taken into consideration. I don't want the soldier necessarily worrying about that. He has enough to worry about, and he has a job to do. So that, I think, is maybe one way to think about it.

Secondly, metrics, metrics, metrics. What gets measured gets done, but are we measuring what matters? Here I think it gets back to the same issue. To put it into a law enforcement context, as Mr. Reichert would know much better than me, do you want more informants or sources, or do you want an informant or source who actually knows something? We often get more, but I want the one who is inside the decision-making chain or the loop of an organization or an enterprise, so we can bring it down. So that is maybe the differential there.

Mr. DENT. Can I ask just one quick yes-or-no question?

Ms. HARMAN. Yes.

Mr. DENT. Thank you. Thank you, Madam Chair.

On page 5 of your testimony, you discussed LAPD and NYPD developing their own intelligence collection, and we have heard from NYPD over the years here.

Do you think that local law enforcement officials should detail officers overseas to engage in intelligence collection in foreign environments?

Mr. CILLUFFO. I fully endorse the component of the LEAP report that this committee put out that, yes, we should have foreign liaison officers overseas, not for intelligence collection per se. Now, NYPD, LAPD, maybe they are tripping up sources vis-à-vis where they fit in with the other alphabet soup of agencies overseas. But clearly, from learning and being embedded with local law enforcement, you would benefit greatly.

Ms. KAYYEM. I am afraid I don't have a yes-no answer to that. We don't have it. I think there are real problems to it in terms of, sort of, everyone bumping into each other, and don't have intentions of doing it. But I don't know enough about New York and LA's programs to say whether generically we should do it.

Mr. BETTENHAUSEN. Yes. But it should not just be about intelligence collections. It is that relationship and partnerships and fellowships of learning what they are seeing and risks and threats. Because we are in a very small world, and what you are seeing overseas isn't far from our shores, as we saw on 9/11.

Ms. HARMAN. Thank you.

Thank you all. I thought the testimony was superb, and the answers to questions is superb.

That is why, if members want to ask another round of questions, we will stay here to do that. I promise that my questions will not exceed, including your answers, 5 minutes.

Let me first say I had an epiphany when—I think it was Matt who said that everyone is a producer and everyone is a customer. Did you say that?

Mr. BETTENHAUSEN. I think that it was Frank.

Ms. HARMAN. Ah, it was Frank. Matt coined all our new terms. Juliette had the other piece of what is special here, which is where is the value added.

I just want to observe—and when you respond to the one question I am going to ask you, please comment on this too—that I think that I&A may be trying to play too many roles here. It had a core mission ripped out, which was the Federal Fusion Center function, which I mentioned in my opening remarks, and it has been trying since then to find many places that can fit in, when, in fact, if it would focus on value added, it might be a much more effective part of DHS. That is my thought, from what you all said.

My question is about the private sector. No one really mentioned that. I think it was Frank who talked about EMS and hospitals. But I want to observe that in Minneapolis, the other day, we went to the Mall of America. We saw there a very impressive director of security, who has an office of 100 people, who is running an operation in the largest, or one of the largest—in area, it is the largest mall in North America. I don't know that it has the most retail stores. Only my daughter, the shopper, would know that.

But at any rate, his operation, which is tied into the Fusion Center and other law enforcement agencies in Minnesota, seems very effective. He showed us a tape that they made—they have many surveillance cameras there—of an individual who clearly, from this tape, was casing this mall. Turned out to be of foreign origin, and it is a longer story.

But, at any rate, I was impressed. None of you has really addressed how you integrate or how one should integrate private-sector efforts with what you do. So that is my question.

Mr. BETTENHAUSEN. Unfortunately, I didn't have Frank's clock that stopped when summarizing my testimony. But one of the things that I did want to emphasize—because that is critical.

Our critical infrastructure, most of it, is in the private sector's hands. In my written testimony, one of the things that we are advocating for and what the National Governors Association and State and Local Working Group on Infrastructure Protection has advocated is there needs to be a critical infrastructure/key resources desk in every Fusion Center, so that, one, you know what critical infrastructure do you have, what are the potential cascading effects, as well as meshing together threat information so

that it matches the vulnerability and potential consequences that you could have to an attack on critical infrastructure.

One of the things that Governor Schwarzenegger also did in California was our licensed security professionals and security guards in California are required to have 8 hours of training. The Governor, showing his vision and leadership on this, said, look, we ought to change that so that they get at least 4 hours of those 8 hours as terrorism awareness. One, so that they can recognize operational surveillance. Because we know that they have to do target selection, they have to do this, there is that operational cycle. If we can catch on early, we can preempt and prevent.

That is putting—you know, in looking at scale and scope for California, there are 400,000 just-licensed security professionals out there. Linking them in not only with their eyes and ears so they know what to look for, more importantly how to report it back into the Fusion Center process so that we can understand and say, hey, we may have something going on based upon a series of incidents at chemical plants, shopping malls, whatever.

Ms. HARMAN. Thank you.

Other comments.

Ms. KAYYEM. Yes.

Ms. HARMAN. In 1 minute, between you.

Ms. KAYYEM. The critical infrastructure/key resources desk is key. It is, I think, a really legacy function of the fusion centers, whether you have nuclear facilities or LNG terminals, which we have. That is going to be, I think, one of the core future functions of the Fusion Center-Homeland Security relationship.

What we are trying to do, and what I think DHS has been actually very helpful on, is this ACAM system, which is an automated critical infrastructure system. It had a different name in California. But by having one tool that we are all, sort of, monitoring critical infrastructure off of, we are putting all the data in, we are working with our private-sector partners, we then have a basis to determine whether we should be nervous or not, from the State perspective.

Because if I look at my critical infrastructure list, it is over 300. It is every high school. I love high schools; I care about high schools. But from the perspective of, is the Governor going to be terribly worried that there is going to be no energy in New England if something happened in the port, they are different. They are different kinds of worries. So that is a program that has helped very well.

Ms. HARMAN. Thank you.

My time has expired. So hopefully, Mr. Cilluffo, you have nothing to add?

Mr. CILLUFFO. Yes.

Ms. HARMAN. Yes.

Mr. Reichert.

Mr. REICHERT. Thank you, Madam Chair.

One quick question. I know it was really a struggle for me, as a sheriff, to participate in all the Federal task force entities that exist. You are always being asked to be a part of this FBI task force or HIDTA task force or you name it. You want to provide a body to that effort. The same goes with the fusion centers and

JTTF, et cetera. So the funding issue has really always been a sensitive one and one that we have all struggled with.

What is your opinion on the Federal Government's responsibility and role as it relates to assisting local and State agencies in providing funding for fusion centers and task forces?

Mr. BETTENHAUSEN. Very much appreciate that question.

There is a significant role that the Federal Government needs to be making. There is a misperception here in Washington, DC, that somehow $5 billion in Federal grant funding made available to State and locals on an annual basis somehow is supporting all of the State and local public safety efforts. It is almost too much to say it is a drop in the bucket.

You know, you are not recognizing the fact that, you know, what changed after 9/11 is that terrorism prevention and protection is everybody's business. There is a lot of personnel and resources that we, as State and locals, are pouring into this particular effort. The Federal Government needs to support us with that.

That is why it is important, with the grants for the analytical components of our fusion centers, for them to support it. Because there is also a misunderstanding. There is this belief that somehow these fusion centers are only for the benefit of State and locals. It, again, ignores that philosophical that you don't understand what we do as State and locals and what your sheriff's office can help provide them. These are there to support the national terrorism prevention mission. It is also all crimes, all hazards, to make our communities, our States, our Nation safer and better-prepared.

That is why the Federal Government has an obligation to help support these, because it is to their benefit as well. It is not just for the benefit of State and local. It is ignoring all of the other things we are paying, whether it is corrections and prisons and the officers on patrol and all the TLOs, terrorism liaison officers, we trained and who fulfill this and support that national mission. That is why we need that Federal funding.

The best example is, you know, does the Federal Government have urban search and rescue teams? Do they have hazardous material teams? No, they don't. They are in our communities at the State and local level. They become national assets in a time of emergency.

That is why that grant funding we use to buy the equipment and do the training. But we pay for the personnel. If the Federal Government had to then create their own USAR teams to sit around like the Maytag repairman waiting for a national emergency, it would cost you a lot more than the $5 billion a year. Plus, you are losing the benefit of them saving lives and property day-in and day-out, 24/7/365.

Ms. KAYYEM. I actually have nothing to add to that, because that was great.

Mr. REICHERT. I almost felt like I should ask the question, run over there real quick and answer myself.

But thank you for that. I wanted that on the record.

Mr. BETTENHAUSEN. Did I miss anything you would say as a sheriff?

Mr. REICHERT. You hit it right spot on. Thank you.

Ms. HARMAN. See, we do this vertical integration right here. Here he is.

Ms. KAYYEM. I will add one other quick thing on the grants, because the IED thing is not helpful to us, from a State perspective, 25 percent. I mean, we have people so nervous right now for reasons that aren't supported by the intelligence, as I related in the oral testimony.

I actually thought what is going on in the port grants—I know it is not in this jurisdiction, but just something to think about—what is going on in the port grants and obviously in SAFECOM were really helpful exercises for the State. Because, as you know, we have to distribute our money 80/20. But to be told by the Feds that the State has to come up with a plan, and it is your plan because I am a Commonwealth and I have crazy radio systems all over the place, and come up with a plan about how you are going to fix it, tell us how you are going to fix it, have an integrated plan, we will approve the plan and then release the money, and then you spend the money according to the plan, great, great process. I love it, because the complaining fire chief in a small jurisdiction who doesn't get what he wants, I say, not part of the plan.

The port folks are doing the same thing with the trade resiliency. You have to come up with the plan first for your port money—we have $4 million this year—about how you will resume trade, how you will be resilient. Then all the jurisdictions mad at us, mad at the State, because they are not going to get everything they want, they can apply for grants according to the plan. It works great from a management perspective and a security perspective.

Mr. BETTENHAUSEN. I also caution, because I see a trend toward trying to require matches, whether it is soft or hard, and that is a mistake. There is not enough money there, based on what we are already contributing as State and locals, and to throw that match requirement on in these budget times, these economic circumstances—and, more importantly and fundamentally, it ignores that this is a Federal responsibility. If they want those assets to become national assets in times of disaster and catastrophe, you have to help us support it, support and build them.

Mr. REICHERT. Thank you.

Ms. HARMAN. Mr. Perlmutter.

Mr. PERLMUTTER. Thanks.

Just, No. 1, I want to thank the panelists. It has been an excellent discussion, and just appreciate, you know, the knowledge and the fact that you have lived this subject. You can tell from your testimony.

Switch gears a little bit and talk about open source opportunities or reports and just whether you think that is something that the Intelligence Community, DHS should be focusing on, whether we should be providing any legislation concerning open source reports. Then, you know, if you have a privacy aspect to it, I would like to hear that too.

Mr. CILLUFFO. Well, in my prepared remarks I did highlight the importance and significance of open source. I think a vast majority of this information is. Its collation that gets a little complex, but in terms of the information itself, is publicly available if you know where to look for it.

The adversary relies entirely, if we are talking about al Qaeda or terrorism, on the Internet. So they need that to sustain their own operations. So they are tipping off many of their intentions, capabilities, plans and the like.

If you look back during the Cold War, the amount of resources we have devoted—war colleges popped up, defense universities popped up—to understand the Soviet Union, we haven't even come close to understanding this adversary. We do so at our own peril. They are not madmen. They are not crazy. We have to actually understand. To me, open source can play a huge role in that.

I think some of the better products are actually open source. One of the better DHS products is called The Universal Adversary, and I am not sure you guys have even seen it. It is not a very well-known product, because it is open source.

That is something we also have to change. If it has that marking with a code word on it, we think it is better. That doesn't mean it is better. The reality is just because—it is how it was collected. I don't want to get into the whole process of what collection, what markings are and classification.

But the vast majority of this stuff is available and should be. We need to devote the education, the resources and time to do it.

Mr. BETTENHAUSEN. Open source is very important because you can pull a lot of this together. Sometimes we get more timely information from reading the news reports than we do in getting the products. I mean, you know, the National Intelligence Estimate, we were reading about what was in there in the paper for a week before we ever even got a briefing from DHS on it. That is frustrating, and that has to change.

But open source is critical. The CENTRA report—I don't think it requires legislation, in direct answer to your question. But the CENTRA report that Charlie Allen and DHS I&A commissioned talks about the importance of open source. In fact, they have started a couple pilot training programs. We were pleased to have one of them in California in our Sacramento Regional Threat Assessment Center. It was very useful. It was well-received.

So it is the kind of customer service that the customers are saying, hey, we want more of this. So it needs to be at the top of their priority, and they should be funding—you know, now they are struggling, well, how do we continue this pilot and move this on? Well, you know, when it is meeting that need and it is being greeted warmly and with success, well, then we need to prioritize and do it. Because it is a critical part of the operations.

It was followed up by the ODNI's conference, open source conference here in Washington, DC, that we attended and I spoke at. Because that is very important, to be able to access and use that information and get a better understanding of our adversaries.

The importance, again, of that counter-narrative that Frank is talking about, in terms of making sure that we don't have radicalization occurring in our own communities, what are the issues to prevent that from having traction and preventing true assimilation and integration of our very diverse populations in the United States.

Ms. KAYYEM. Then, finally, just consistent with this, I think that the push I think a lot of States are making now to put the privacy

and first amendment and retention-of-information rules at the front end will not impede the open source, I am pretty confident of that, but will provide assurances to a public that doesn't often know what we are doing. I mean, you know, it is just fusion centers are—if you even know what it is, what is it doing and stuff.

So, you know, maybe I am in the publish or perish mode, but I am, like, overwhelming people with, like, here is our privacy guidelines, here is—just because I want people to know that we have them, that we are not not thinking about this. If you can get that out there at the front end, then the other stuff sort of flows from it, and then they are consistent.

You know, the ACLU remarks about fusion centers, you can't hide from them, they are out there. They represent, whether it is the ACLU or people's feeling about intelligence, which I often can have sometimes too, they represent a core feeling by many Americans. We can't pretend like the debate is going to go away. We have to, sort of, take it on front end and say, we are also rational people who recognize the importance of this.

Mr. PERLMUTTER. Okay. Thank you very much.

Ms. HARMAN. Thank you.

Thank you to the colleagues on this subcommittee and to our witnesses. I thought the testimony and the Q&A were excellent.

We feel good about the direction we are taking. Glad the message is being received out and about in the country. We want to continue to work with the three of you, specifically, on ways to satisfy the customer better and get I&A and DHS to fulfill its core mission better.

Hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 11:34 a.m., the subcommittee was adjourned.]

○