AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HOMELAND SECURITY INTELLIGENCE: ITS RELEVANCE AND LIMITATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MARCH 18, 2009

Serial No. 111–9

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

49–943 PDF WASHINGTON : 2010

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

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

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

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

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

JANE HARMAN, California, *Chair*

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

MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
PAUL C. BROUN, Georgia
MARK E. SOUDER, Indiana
PETER T. KING, New York *(Ex Officio)*

THOMAS M. FINAN, *Staff Director*
BRANDON DECLET, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
DERON MCELROY, *Minority Subcommittee Lead*

CONTENTS

HOMELAND SECURITY INTELLIGENCE: ITS RELEVANCE AND LIMITATIONS

Wednesday, March 18, 2009

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 [Chair of the subcommittee] presiding.

Present: Representatives Harman, Carney, Clarke, Green, Thompson (ex-officio), McCaul, Dent, Broun, and Souder.

Ms. HARMAN. The subcommittee will come to order.

Good morning, everyone. We are meeting today to receive testimony on homeland security intelligence, its relevance, and its limitations.

Last summer, Shirwa Ahmed, a U.S. citizen, traveled from his home in Minneapolis, Minnesota, to Somalia. In October, he got into a truck filled with explosives, drove to the north of that country, and blew himself up, killing as many as 30 other people. According to the FBI, Mr. Ahmed is the first known U.S. citizen to conduct a suicide bombing overseas. Several of his friends from Minneapolis also left the country for Somalia last summer. They are presently unaccounted for.

Last month, Ahmadullah Sais Niazi, a Tustin, California, man of Afghani origin, appeared in Federal court to answer charges that could send him to prison for decades. He failed to mention when he applied for U.S. citizenship several years ago that his brother-in-law, Amin al-Haq, is an al Qaeda terrorist, Osama bin Ladin's bodyguard to be exact. The United Nation's Security Council identified Mr. Niazi's brother-in-law as an al Qaeda operative in March, 2001; and the U.S. Government designated him as a specially designated global terrorist shortly after 9/11.

At Mr. Niazi's bail hearing several weeks ago, an FBI agent testified that the Bureau had recent recordings of Mr. Niazi referring to funding Afghan Mujihadin and blowing up vacant buildings. On those tapes, Mr. Niazi also reportedly describes Osama bin Ladin as "an angel".

In December of last year, Fahim Ahmid was named as a co-conspirator in a terrorism case in Atlanta that included plans to attack military bases, oil storage facilities, and refineries in the United States. Mr. Fahim is an alleged ringleader of the Toronto 18, a group of Canadian youth that in 2005 had planned to attack

Parliament buildings, detonate truck bombs, and behead the Canadian Prime Minister.

According to the indictment, Mr. Fahim met in early 2005 with two American citizens who came to visit him to discuss traveling to Pakistan to receive paramilitary training with Lashkar-e-Taiba. We all remember that they were associated with the recent Mumbai incidents. Among Lashkar-e-Taiba's exploits was the massacre in Mumbai.

Imagine a Mumbai in Minneapolis or Tustin or Atlanta. In each of these American hometowns, local law enforcement officers are first preventers, who are sitting in front of us, walk the beat every day as part of their traditional work of preventing, investigating, and prosecuting crime, which brings me to a simple question: While we want police and sheriffs' officers Nation-wide to keep their community safe from traditional bad guys, don't we want them also to know about potential terrorists in their midst who mean us harm?

That is what homeland security intelligence is all about: getting accurate, actionable, and timely information to the officers in our hometowns so they know who and what to look for in order to prevent the next 9/11.

If homeland security intelligence is done the right way—let me stress this again, because we have a second panel that is going to address what the "right way" is—if homeland security intelligence is done the right way, countless lives can be saved. If patrol officers know what everyday materials terrorists might purchase to build IED, law enforcement can meet with store owners and share this information and invite tips that might warrant further information.

As we are going to hear in a moment from one of our witnesses, if they know what ricin looks like—ricin, a very deadly agent, as we all know, which was discovered recently in Las Vegas—they can prevent a ricin attack.

If those same officers know what crimes terrorists are committing to finance their activities, they can dig deeper into otherwise routine investigations to see if they can come across terrorism dots that need connecting.

If our first preventers know what kinds of homeland attacks are most likely to occur in the next 2, 4, 5, 6 years, moreover, they can train appropriately, deploy efficiently, and prepare more thoroughly to meet anticipated threats.

But let us not fool ourselves. If homeland security intelligence is done the wrong way, then what we will have is what some who will testify on the second panel have called the "thought police"; and we will be the worse for it.

The National Applications Office is a glaring example, in my view, of a homeland security intelligence program gone wrong. Before Congress fenced its funding, the NAO would have tasked military satellites with providing imagery for homeland security and law enforcement purposes. Although the NAO may have been created with good intentions, the Department of Homeland Security did not create a clear legal framework outlining the office's power. Instead, it created what lawyers like me call a slippery slope for potential abuses, and U.S. law enforcement officials haven't requested this additional ability. So I hope that Secretary Napolitano

follows my advice and the advice of some other Members here and closes that office permanently.

My goal in this Congress is to get DHS, the FBI, and other Homeland Security officers where they need to be to disrupt terror plots and protect American lives. I am not new to the arguments about homeland security intelligence, but I want this hearing to focus attention on the debate. This is something I think is very important. I wish we had done it in the last Congress, but we are doing it as our first hearing now.

As the second panel will recognize in testimony today, we need clear definitions about what we are doing, we need transparency and a process to hold people accountable, and we need to shut down what doesn't work and what we know can't work. The rule of law must always apply.

So this hearing is a starting point for talking with some of those who fight this fight every day—thank you for your service—and are trying to do homeland intelligence right. It is also our starting point for those who are concerned that we are not doing things right enough and who have good ideas about how to get on a better track.

I welcome all of our witnesses and look forward to our testimony; and I now yield to the Ranking Member, Mr. McCaul, for his opening statement.

Mr. MCCAUL. Thank you, Madam Chair, and let me say how much I look forward to working with you on this subcommittee.

I remember meeting with the Minister of Security in Israel who said, we defeat the terrorists through intelligence. Good intelligence, that is probably the most important weapon we have on this war on terror.

Let me also thank the witnesses for being here today. I know you have busy schedules. Your work is essential to our frontline homeland security efforts, and we welcome you to this committee.

When I worked on the Joint Terrorism Task Force in my home State of Texas, I saw first-hand how important information sharing and collaboration is between all levels of government. An effective homeland security intelligence capability requires that key State, local, and tribal law enforcement at least be integrated into the homeland security enterprise. They are our Nation's first preventers, as the Chair already said. You are the eyes and the ears, and your participation in the intelligence process is critical to preventing further attacks.

To illustrate this point, shortly before 9/11, three of the highjackers were separately intercepted for traffic offenses by local law enforcement. In fact, Mohammad Atta, the leader of the 9/11 operation who piloted one of the planes that crashed into the Twin Towers, was stopped and fined in Florida for driving without a valid driver's license. Atta did not pay the fine, and a warrant was issued for his arrest. However, he was let go several weeks later when he was once again stopped for speeding, as the officer who stopped him was not aware of this warrant.

Had an integrated intelligence enterprise with State and local law enforcement participation existed prior to 9/11, we may have had a chance at intercepting and detaining him before the dreaded 9/11 attacks.

While this State and local picture is essential, homeland security intelligence is incomplete without a robust Federal picture as well. A large part of that picture is provided by DHS. In fact, according to DHS, in fiscal year 2008, the Office of Intelligence and Analysis responded to over 1,200 Federal requests for information. This is compared to approximately 1,700 from State, local, and tribal sources. This illustrates that, while I&A is a key resource for locals, it is also relied upon by many Federal agencies as well.

A comprehensive intelligence picture, including border data, immigration information, and transportation security information, is essential to defending our homeland. By properly adding the State, local, and tribal perspectives, DHS can provide or help provide a truly comprehensive picture of the threats that we face as a Nation.

I look forward to the testimony and the critical work of this subcommittee. I look forward to building a stronger, more robust Office of Intelligence and Analysis that serves all of its partners that is consistent with our constitutional rights.

I thank you, Madam Chair.

Ms. HARMAN. Now I will recognize the Chairman of the full committee and welcome him to our subcommittee hearing; Mr. Thompson, for opening remarks.

Mr. THOMPSON. Thank you very much, Madam Chair; and let me also welcome our witnesses in the first panel here today.

Also, Madam Chair, I am pleased that we are getting back to basics by addressing what homeland security intelligence is and what DHS's mission in developing it should be.

In many ways, DHS's Office of Intelligence and Analysis is at a crossroads. That is a good thing, because a crossroads is a place where new directions can be taken, and that is exactly what is needed at I&A. Secretary Napolitano has promised that DHS going forward would partner better with State, local, tribal, and private sector stakeholders. For its part, I&A, therefore, should stop with its typical top-down approach to intelligence and start putting State, local, tribal, and private sector needs first. Refocusing I&A as a national fusion center with strict privacy and civil liberties protections in place would be a step in the right direction.

Put simply, Madam Chair, I&A must make it a priority to analyze relevant State, local, tribal, and private sector information and compare it with national intelligence. In doing so, it would be uniquely able to connect the dots and create situational awareness of both near-term and long-term threats to the homeland.

Constitutional safeguards, in turn, must be the starting, middle, and end points of this effort. Without them, it would be a worrisome and wasted one.

I look forward to the witnesses' testimony, Madam Chair, on all of these points; and welcome, again, to all of the witnesses.

Ms. HARMAN. I thank the Chairman of the full committee and fully endorse his comments about a new role and new focus for I&A.

I just want our witnesses to know that some of us on this committee have pushed as hard as we can to get Secretary Napolitano to name someone from State or local law enforcement as the head of I&A. The Chairman just said "absolutely." I believe she is going

to name a deputy from State or local law enforcement, but I want to say, on the record, that I am disappointed. I think it is a huge missed opportunity to send a new signal about the function of intelligence at the Department of Homeland Security.

Our Members are reminded that, under the committee rules, opening statements may be submitted for the record; and I now welcome our witnesses this morning.

Our first witness, from my hometown, is Commander Joan McNamara, a 27-year veteran of the LAPD, where she presently serves as Assistant Commanding Officer of the Counter Terrorism and Criminal Intelligence Bureau. Commander McNamara developed both the threat stat analytical model and the system of suspicious activity reporting that I believe holds tremendous promise, if implemented correctly, for homeland security intelligence. Her SAR initiative is being adopted Nation-wide to identify and share counterterrorism information related with State, local, and tribal Federal partners.

Commander McNamara has had numerous other accomplishments with the LAPD as commanding officer of the Los Angeles harbor area. She spearheaded unique efforts to combat crime in the Wilmington Ghost Town area, a neighborhood that has been plagued with violent crime, gang, and narcotics activity for 30 years. During her leadership of the Newton Patrol Division, she likewise oversaw an unprecedented reduction in crime.

Commander McNamara has also initiated several highly-successful community-based youth programs in Los Angeles.

Our second witness, Sheriff Doug Gillespie, is a 28-year veteran of the Las Vegas Metropolitan Police Department. He serves as the chairman of the Major Cities Chiefs Association's Homeland Security Committee and as vice president of the Major County Sheriffs Association. During his tenure, Sheriff Gillespie has placed considerable emphasis on addressing the terrorist threat at the local level.

His department includes a Homeland Security Division that includes a newly-created Homeland Security Bureau, along with an existing Vice and Narcotics Bureau.

Sheriff Gillespie has likewise committed additional personnel to the Southern Nevada Task Force. He has also advanced a newly-created counterterroism section within his department in coordination with his existing criminal intelligence technical and surveillance and special investigations sections. Sheriff Gillespie has also developed an all-hazard ARMOR response unit and emergency management section to more accurately identify, prevent, and respond to terror and other threats.

Our third witness, Gary Edwards, is the Chief Executive Officer of the National Native American Law Enforcement Association, a nonprofit public service association which advocates for Native American law enforcement professionals Nation-wide. Mr. Edwards serves on a number of national Federal advisory committees and task forces, including the Interagency Threat Assessment Coordination Group, the ITACG, Advisory Council; and the National Center for State and local Law Enforcement Training Advisory Committee, SALTAC; and the regional Four Corners Homeland Security Commission.

Mr. Edwards is currently a recently retired deputy assistant director of the United States Secret Service, where he served for 28 years. During his tenure with the Secret Service, Mr. Edwards worked in the Office of Human Resources and Training, the Office of Inspection, and the Office of Government and Public Affairs. His career was replete with service and merit awards and honors.

Our next witness, John Gaissert, is Chief of Police for the city of Commerce, Georgia.

Mr. Broun, I will let you do the honors to introduce him.

Mr. BROUN. Thank you, Chair Harman; and thank you, Ranking Member McCaul.

Today, I have the honor of introducing my friend, the Chief of Police in Commerce, Georgia, Chief Gaissert. Chief Gaissert has a 35-year career in the military, law enforcement, as well as corporate experience. During his career, he has served with distinction in uniform patrol, special operations, and criminal investigation units. During the 1996 Centennial Olympic Games in Georgia, Chief Gaissert performed the demanding task of operations' officer for the Athens Clark County Police Department and offered the operational plan supporting the events.

Chief Gaissert obtained level 5 certification in homeland security from the American College of Forensic Examiners. He serves as Department of Homeland Security liaison for the Sheriff of Jackson County, Georgia, and chairs the County Threats Assessment Committee.

Chief Gaissert completed a law enforcement exchange program in counterterrorism with Israeli National Police and was awarded executive certification in counterterrorism from ICT, the Lauder School of Government in Israel.

Chief Gaissert was recalled to active duty during the Persian Gulf War and retired from the U.S. Navy at the rank of commander.

I have the pleasure of introducing my good friend, Chief Gaissert.

Ms. HARMAN. Without objection, the witnesses' full statements will be inserted in the record.

I now ask Commander McNamara to summarize her statement in 5 minutes, and we will try to be quite vigilant about the clock—I assume you can see it—because that will give us more time for interaction with Members.

As you know, we have a second panel. Let me urge that you, in particular, stick around for the second panel, because a number of our witnesses want to address your initiatives.

STATEMENT OF COMMANDER JOAN T. McNAMARA, LOS ANGELES POLICE DEPARTMENT

Ms. MCNAMARA. Madam Chair, Ranking Member McCaul, Members of the subcommittee, thank you for this opportunity to appear before you today.

I have been asked to discuss efforts by the LAPD to gather, document, review, analyze, and share terrorism-related Suspicious Activity Reports, or SARs, and to describe to you how these efforts relate to the national SAR Initiative.

In my written testimony, I have provided the subcommittee background on both the Nation-wide SAR Initiative and the LAPD SAR program. Instead of restating that today, I respectfully request that my prepared statement be accepted into the record.

Ms. HARMAN. Without objection, all of your prepared statements are accepted into the record.

Ms. MCNAMARA. Thank you, Madam Chair.

In my limited time this morning, I would like to address two questions that I believe are fundamental to today's hearing: First, does SAR's process directly enhance the ability of local police to protect our communities from violent crime, including terrorism? Second, can the SAR process be carried out in a manner that protects privacy, civil liberties, and the civil rights of all Americans?

I believe the answer to both of these questions are a resounding yes.

Protecting our communities. While our program is relatively new, we are already seeing results. The LAPD SARs statistics are as follows: We have 1,374 SARs in process. Of those, we have made four arrests. Fifty-one of those have been sent over to the Joint Terrorism Task Force for follow-up; and, in my opinion, while the number of investigation and arrests are important, they are almost secondary to a newfound ability to connect events that in the past would have appeared unrelated.

For example, prior to SAR, when a suspicious package call was received by the LAPD, our bomb squad would respond. If the package was determined to be nonexplosive device, the bomb squad would then call clear, and then no further analysis was done. Today, the bomb squad also completes a Suspicious Activity Report, and through the process we are now able to map all bomb calls in the city of Los Angeles. This paints an amazing picture in real time and over time.

Other cities are implementing the SAR process and are seeing similar results.

Let me address the second part, the privacy and civil rights.

The second question I would like to address is whether the SAR process can be carried out in a manner that protects privacy, civil liberties, and civil rights. As I have stated previously, I believe the answer to this question is "yes" as well. In almost 8 years following the 9/11 attacks, we have sought to engage frontline law enforcement officers in the event to prevent future terrorist attacks. Until now, information and training provided to these frontline officers was superficial and was not tailored in advance to the changing roles from first responders to first preventers. Nor was there a reporting mechanism in place.

The SAR Initiative is important because now, for the first time, we are able to train our frontline personnel regarding behaviors associated with terrorism-related crime and providing them the information they need to distinguish between behaviors that are reasonably associated with criminal activity and those that are not.

Let me be very clear today: Not every person wearing a trench coat is a robber, not every person loitering on a corner is a drug dealer, and not every person taking a picture of a monument today is a terrorist.

As a law enforcement executive, I do not want my officers involved with confrontational interactions with innocent people engaged in innocent activities. I do not want to fill them or fill my systems with information regarding innocent people involved in innocent activities. I do not want my officers making stops based on race, their ethnicity, or religious beliefs.

My officers, investigators, and analysts have been trained on behaviors and indicators associated with criminal activity. I have put into place clear policies regarding interactions and how they are to be handled and how information about those contacts and calls for service should be handled.

It means putting in place privacy and civil liberty protections. It means reminding our officers that it is inappropriate to collect information regarding people engaged in constitutionally protected activities when there is no nexus to criminal activity. Finally, it means holding people accountable when they violate these rights and policies.

This is what LAPD SAR process is all about. This is what the Nation-wide SAR process initiative seeks to place across the Nation. This is what we need to do if we are going to reduce the number of inappropriate police-citizen contacts.

There are some who will tell you today that we don't need a SAR process. I will tell you they are missing the point. The SAR process isn't about asking officers to collect a new type of information. It is about information that they have already gathered in the course of their day-to-day business. But the process ensures that we carry out their first preventers' response and abilities in a manner that protects privacy, civil liberties, and rights.

Ms. HARMAN. Could you summarize at this point?

Ms. MCNAMARA. In closing, the Nation-wide SARS initiative has brought together Federal, State, local, and tribal officials as well as representatives from the privacy and civil liberties communities in a way that I have not seen in my 27 years. While the effort is still young, those of us involved are convinced, through it we will be better able to protect our communities from crime, including terrorism, and safeguard the privacy, civil liberty, civil rights of people we are sworn to protect and serve.

[The statement of Ms. McNamara follows:]

PREPARED STATEMENT OF JOAN T. MCNAMARA

MARCH 18, 2009

Madam Chair and Members of the committee. Thank you for the opportunity to be here with you, to describe the tremendous progress achieved by local law enforcement toward the integration of counter-terrorism efforts into the day-to-day work by local law enforcement to protect our communities from crime and violence.

The role of local police in counter-terrorism efforts has become more clearly defined over the past 8 years. Front-line officers, with their intimate knowledge of their communities and their keen observational skills, have traditionally been thought of as first responders.

That perception changed with the 9/11 terrorist attacks. Policymakers, law enforcement executives and others increasingly called for police to be redefined as "first preventers" of terrorism and the emphasis at the local level shifted from response to prevention. Local police were now considered an integral part of efforts to protect the Nation from a variety of threats—including that posed by domestic and international terrorist. Local law enforcement are now considered an integral part of our "national security" effort. In the years following the 9/11 attacks, enhanced collaboration and revolutionary new sharing protocols had been forged with

Federal partners to increase knowledge, awareness, and information flow. Still, a critical gap existed in the information-sharing cycle.

Tasking local law enforcement with the policing of traditional crime and the prevention of terror attacks in their local jurisdictions constituted a dramatic paradigm shift, both for the Federal Government and for the local and State agencies themselves. If this shift in established thought and practice were to be successful, it would require law enforcement agencies Nation-wide to adopt universal guidelines for effective communication with Federal partners and information-sharing. This was far easier said than done. There was no system in place at any level to facilitate this crucial and necessary exchange.

The Suspicious Activity Reporting (SAR) program was the Los Angeles Police Department's answer to this problem and now serves as a national model for the American law enforcement community as it is being institutionalized through the Nation-wide SAR Initiative (NSI). The underlying premise of SARs is very simple: A police officer's observation and reporting of just one of these events could be the vital "nugget" of information needed to focus attention in the right place, or to connect seemingly unrelated dots and predict or prevent a terrorist act. The SAR program takes the emphasis off of the racial or ethnic characteristics of individuals and places it on detecting behaviors and activities with potential links to terrorism-related criminal activity. Coupled with extensive training this approach ensures that citizens' civil and privacy rights are protected.

The foundation to the SAR program is built upon behaviors and activities, which have been historically linked to pre-operational planning and preparation for terrorist attacks. They include actions such as: acquiring illicit explosive material; taking measurements or drawing diagrams; abandoning suspicious packages or vehicles; and testing security measures.

This is the first program in the United States to create a national standard for terrorism-related Modus Operandi (MO) codes. By creating and assigning numbers, or codes, to the terrorism-related behaviors, terrorist activities can be tracked by date, time, and location, just as other crimes are currently tracked. With the advent of coding, an agency's records management system has been transformed into a valuable and viable terrorism prevention tool.

When the preliminary information contained on a SAR report is analyzed using these codes, the system can be utilized to map, chart, and graph suspicious behaviors, and allows counter-terrorism personnel to run specific queries based on a particular behavior, location, or time frame in order to identify emerging patterns. The eventuality of a Nation-wide application of this behavioral coding and uniform reporting and tracking method will provide the revolutionary basis for linking behaviors and indicators and revealing emerging patterns for terrorist throughout the United States. These standardized codes also enable local agencies across the country to share information in a systematic and uniform fashion that enables trends, spikes, and patterns to be identified and placed in a national context. The SAR methodology has the potential to revolutionize how American law enforcement reveals the emerging patterns of terrorism-related indicators and behaviors. In addition, these SARs provide police with the capability to search through previously reported suspicious activity and identify important links to behavior that might otherwise be overlooked. This ability to query is crucial to law enforcement's ability to successfully analyze and synthesize information and to produce actionable intelligence toward prevention.

Fusing the SARs-related information with an "all crimes" picture provides decisionmakers with: the statistical support they need to allocate resources and police officers in a more strategic way; closes gaps in training, investigation, enforcement and protection; and reveals potential patterns that extend beyond the region to the rest of the country and, potentially, overseas. Once information is shared vertically and horizontally throughout the region and Nation, activities previously viewed as having happened in isolation can be placed in a national context.

PRIVACY AND CIVIL LIBERTIES

In the process of creating the SARs program, the Los Angeles Police Department has had the privilege of working closely with privacy and civil liberty groups on both the local and the national initiatives. We have collaborated to create a comprehensive and transparent process that strikes an important balance between the safety of our communities and the proper constitutional protections. The concerns that the Nation-wide SAR Initiative will lead to increased police interactions with individuals involved in innocent First Amendment-protected behaviors are diminished with the transparency of the program. Closer evaluation of the SAR process highlights layers of scrutiny which includes vetting, auditing, and the un-founding of SAR re-

ports that do not meet set standards. Training provided to front-line and analytic personnel is designed to enable them to distinguish between behaviors associated with criminal activity and those behaviors that are innocent or constitutionally protected. As the SAR process gains momentum, we remain committed to collaboration with advocacy groups for the accurate development and expansion of the Nationwide SAR Initiative.

ROLE OF THE DEPARTMENT OF HOMELAND SECURITY

As the National SARs Initiative moves forward, it should be noted that the successful institutionalization of the National SAR Initiative has the potential to significantly enhance the Department of Homeland Security's ability to work with State and local partners to identify and mitigate a range of emerging threats to the homeland. But the DHS Office of Intelligence & Analysis, which serves as the analytic hub for all information and intelligence generated by the DHS work force, currently has no mechanism for gathering and analyzing SARs generated by individual DHS components. It also lacks a mechanism to blend those SARs with others generated by Federal, State, and local entities.

SARS AND THE NATIONAL LANDSCAPE

The SARs program is representative of the tremendous strides that local law enforcement has made in the area of counter-terrorism. The SARs program enables police to paint their own rich picture of what is happening "on the ground" in their communities in relation to terrorism, rather than relying solely on their Federal partners for information. This goes a long way toward closing what were previously wide gaps in information sharing. The program also makes local law enforcement agencies stronger partners in the national effort to prevent terrorism and other crimes on U.S. soil. It essentially flips the age-old paradigm in which information is pushed from the Federal to the local level with very little push the other way. Now local police departments are valuable players in the information-sharing process and are increasingly relied upon to provide their Federal partners with an accurate picture of what is happening at the local level.

Fusion centers also stand to benefit from the SARs program. Reports about suspicious activity that contain comprehensive data and are provided by a trained work force will result in more informed analytical products, valued dissemination, and more stringent investigative requirements.

Leveraged properly, the SARs program stands to become one of the essential threads that ensure the seamless information flow that is critical to cooperation on the national and international levels. In order to effectively counter a threat such as terrorism, we must first know where these activities are taking place and with what frequency. Law enforcement must have situational awareness that is enabled by standardized processes with strong civil liberties protections that are shared by most, if not all, across the Nation. The time has come for local police to contribute to this process in a significant way. The SARs program is one of the contributions that stands to make that vision a reality.

Madam Chairwoman and Members of the subcommittee, thank you for inviting me to speak today on this important subject. I am happy to answer any questions you may have.

Ms. HARMAN. The Chair now recognizes Sheriff Gillespie for 5 minutes.

STATEMENT OF SHERIFF DOUGLAS C. GILLESPIE, LAS VEGAS METROPOLITAN POLICE DEPARTMENT

Sheriff GILLESPIE. I hear you, Chair Harman, and sheriffs aren't used to being limited in our time, but I will do my best to stay within it.

Ms. HARMAN. That applies up here, too.

Sheriff GILLESPIE. Good morning, and I want to thank you all for giving me this opportunity, Chair Harman, Ranking Member McCaul, and distinguished Members of the subcommittee. I represent Major City Chiefs as well as Major County Sheriffs this morning in my summary of my comments.

We are committed to intelligence-led policing. The analysis of crime data, coupled with execution of innovative policing tactics, is the cornerstone of our efforts to successfully fight crime. The same thing is true in our efforts to combat terrorism in our homeland. Suspicious activity reporting is long overdue, and I think Commander McNamara gave a very good overview of that.

We must apply all crime policies to our fusion centers. To establish robust information and intelligence sharing capabilities in the Las Vegas area, we established a Southern Nevada Counterterrorism Center, an all-crimes, all-hazards, fusion center.

The committee should mandate all the provisions of LEAP. For the chiefs and sheriffs, we wish to formally commend the committee for your report, LEAP, Law Enforcement Assistance and Partnerships. We endorse all seven of the initiatives articulated in the report published by the House Committee on Homeland Security, and we urge Congress to provide appropriations to carry out those critical law enforcement programs.

ITACG is a critical element in the national framework. We cannot and should not rely on the Federal Government to find and implement the solutions unilaterally. State, local, and tribal government need to help carry this effort forward.

Major City Chiefs' Intelligence Commander Group plays a vital role. The purpose of the Intelligence Commanders Group is to strengthen and coordinate the intelligence capabilities and operations of law enforcement agencies and major metropolitan areas. NCTC must establish a stronger working relationship with law enforcement agencies. Foreign liaison is essential.

When terrorists attacked the city of Mumbai on November 26, 2008, cities across America watched as armed gunmen created chaos and carnage in a metropolitan city of 15 million. Every sheriff and police chief in America asked him or herself, could this be my town? Thankfully, the Indian government was extraordinarily forthcoming with the details, and the U.S. news media was providing near constant coverage, so information was easily and quickly obtained. Had this not been the case, State, local, and tribal law enforcement, exactly those agencies tasks responding to the attacks, would not be able to prepare for them.

We understand that the information will ultimately be provided by the Federal Government. That is not the issue. The problem lies in the timeliness of the distribution and the relevance of the content. Would an FBI agent or DHS analyst know what questions a street cop or a hotel security chief in Las Vegas would ask?

Fighting crime is a priority, and fusion centers help. Sustainment funding is needed for fusion centers. It is in this area that we have seen the greatest improvement. DHS has performed admirably in ensuring that funding was available to train incumbent analysts as well as allocate moneys so that agencies without sufficient analytical capability could contract, especially trained personnel.

Private security personnel are critical. In the Las Vegas area, our highly trained cadre of security professionals more than double the number of sworn police officers employed by my agency. Furthermore, they are in the best position to detect suspicious activity,

identify the behavior consistent with pre-operational activities, and report or interdict the activity.

Security clearances continue to be a problem. DHS must restore a Law Enforcement Terrorism Prevention Program, LETPP. We need consistency in funding. DHS, I&A should establish an advisory board to include Major County Sheriffs and Major City Chiefs.

Madam Chair and Ranking Member McCaul, those of us on the front lines look to you for leadership and support for our mission; and thank you for allowing me to speak this morning.

Ms. HARMAN. Right on the button. Thank you, Sheriff Gillespie. You are a timely man.

I also want to note, consistent with your testimony, that this committee authored and it passed the House on the consent calendar legislation to set up DHS as a petri dish to declassify information that law enforcement needs to know what to look for and what to do that will help with this problem that you have just identified of not enough security clearances.

[The statement of Sheriff Gillespie follows:]

PREPARED STATEMENT OF DOUGLAS C. GILLESPIE

MARCH 18, 2009

Chairwoman Harman, Ranking Member McCaul, and distinguished Members of the subcommittee: Today I speak for both the major cities chiefs of police, representing the 56 largest cities in the Nation, as well as the major county sheriffs, representing the top 100 counties. We protect the majority of the American people and have authority in every major urban area. To exemplify the coordination between chiefs and sheriffs, I serve as both chair of the homeland security committee for major cities, and I am vice president of the major county sheriffs.

I am the sheriff of the largest law enforcement agency in the State of Nevada: the Las Vegas Metropolitan Police Department. Because Las Vegas is home to many of the world's largest hotels, and a major center of international tourism and entertainment, my jurisdiction is continuously mentioned by our enemy as a potential target.

I will begin my remarks by quoting from a report prepared by the committee, *LEAP: A Law Enforcement Assistance and Partnership Strategy.* This document challenged Federal agencies to leverage the vast resources of our Nation's "first preventers" in the Global War on Terrorism—State, local, and Tribal law enforcement. As the authors correctly concluded in 2006, "Unfortunately, 5 years after 9/11, critical failures of imagination continue to leave these 'first preventers' as a largely untapped resource in the war on terror."[1] Speaking for chiefs and sheriffs across the Nation, I can report today that while progress has been realized in the more recent years, we have not reached the goals established by the committee.

This should not be construed as an indictment on the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), or any other agency included in the intelligence community. Indeed, the progress made by the intelligence community with regard to information sharing has been laudable. DHS has led the charge by incorporating State, local, and tribal law enforcement into the national effort to protect our homeland. The Department's success in organizing and funding a robust network of 70 Fusion Centers in 3 short years is nothing short of remarkable. The FBI has achieved dramatic improvement in sharing information by enhancing the Joint Terrorism Task Force (JTTF) program, and by sponsoring security clearances for senior police officials so that they can receive the information from their employees assigned to these JTTF's. The achievements notwithstanding, there is still significant room for improvement as State, local, and tribal law enforcement strives to be full partners with the Federal Government in the fight to keep America safe.

[1] *LEAP—Law Enforcement Assistance and Partnership Strategy: Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement.* (2006) Prepared by the Democratic Staff of the Committee on Homeland Security, U.S. House of Representatives. (p.1)

We are committed to Intelligence-Led Policing.

The Major Cities Chiefs Association endorses, and the Las Vegas Metropolitan Police Department employs, the Intelligence-Led Policing philosophy. The analysis of crime data, coupled with the execution of innovative policing tactics, is the cornerstone of our efforts to successfully fight crime. But before analysis can be effectively accomplished, information and crime data must be collected. The same is true in our efforts to combat terrorism in our homeland. Before analysts from our Fusion Centers and intelligence community can synthesize and analyze data, the data must be collected from the source. The 800,000 State, local, and tribal law enforcement officers are better positioned than the Federal Government to collect this information at the State, local, and tribal level.

Suspicious Activity Reporting (SAR) is long overdue.

Las Vegas has joined with Los Angeles and other agencies across the Nation to establish a process for recording, screening and reporting suspicious activity. We are pleased that the Federal Government came to the Major Cities Chiefs to establish the SAR effort, and today the committee is hearing from Commander Joan McNamara who pioneered SAR for the LAPD and the Major Cities Chiefs. Las Vegas is a partner with LAPD in SAR and we are moving forward with sensitivity to privacy concerns and appropriate safeguards. Las Vegas will be adopting the privacy and civil liberties policies that have been developed by the DOJ in collaboration with the American Civil Liberties Union, to ensure maximum accountability, transparency, protection of civil liberties.

We must apply All-Crimes policy to Fusion Centers.

To establish robust information and intelligence-sharing capabilities in the Las Vegas area, I established the Southern Nevada Counter Terrorism Center (SNCTC) as an all-crimes and all-hazards fusion center. The SNCTC's core mission is to provide tactical and strategic analytic support to regional stakeholders. The tactical analysis section provides timely and actionable information to command staff and field personnel. The strategic analysis section complements tactical operations by developing analytical products. Gang, counter terrorism, narcotics, and criminal analysts produce a variety of issue-specific products on issues facing our region.

The SNCTC has established strong relationships with local industry, the public health community, and emergency management agencies. Awareness training is provided to major employers on how to identify and report suspicious behavior.

Co-located with the analysts, the SNCTC houses a 24/7 watch capability, investigators that handle tips, leads, and suspicious activity reports, critical infrastructure protection group, and the All Hazards Regional Multi Agency Operations and Response (ARMOR) Detail. The team consists of local, county, State, and Federal experts in chemical, biological, radiological, nuclear, and explosive (CBRNE) response, detection, and identification.

At the SNCTC, we have developed a privacy policy that is founded on 28 CFR part 23, and with the guidance provided by the DOJ *Privacy Policy Development Guide,* LEIU *Intelligence File Guidelines,* and the Global Justice Information Sharing Initiative (Global). We are open with our privacy policies, and welcome the review and input from our local civil liberties community.

The Las Vegas ricin case as a case study.

The discovery of ricin in a Las Vegas area hotel last year was a timely demonstration of why local agencies must be able to prepare for, prevent, and respond before any Federal agency publishes a report. An individual was suffering from respiratory distress, and because of evidence at the scene, it was suspected that he had been exposed to ricin. It would later be determined that he had in fact manufactured ricin from castor beans.

Throughout the incident and the subsequent investigation, the SNCTC provided officers on scene with critical information on ricin, background on potential suspects, as well as intelligence on known potential terrorist threats involving ricin. SNCTC provided situational awareness to the hotel and casino industry and area hotels, alerting them on what to do if anyone else displayed signs of ricin poisoning.

The Committee should mandate all the provisions of LEAP.

For the chiefs and sheriffs, we wish to formally commend the committee for your report, *Law Enforcement Assistance and Partnerships (LEAP).* We endorse all seven of the initiatives articulated in the report published by the House Committee on Homeland Security and we urge Congress to provide appropriations to carry out those critical law enforcement programs. Until your report is fully adopted, our intelligence efforts will have limited success.

All too often, the information we have received from Federal agencies is less timely and less helpful than what is available from CNN. For years, we have waited for a system to provide timely threat intelligence, especially classified reports that contain information that might help law enforcement to protect particular targets and sectors. While progress has been made, much more needs to be done. On behalf of the chiefs and sheriffs, I offer these recommendations:

ITACG is a critical element in the national framework.

We are grateful to Chair Jane Harman and those who supported her efforts to establish this ITACG. A key recommendation in the LEAP report is the Vertical Intelligence Terrorism Analysis Link (VITAL). The core mission of VITAL is to improve the information sharing between the intelligence community and the front line "first preventers." We cannot, and should not, rely on the Federal Government to find and implement the solutions unilaterally—State, local, and tribal governments need to help carry this effort forward. All we ask is the opportunity to be full partners in these efforts.

But ITACG has been slow to realize its full potential and carry out the intent of this committee. For example, ITACG is not allowed to share intelligence with the local agencies that it is intended to serve. Rather, ITACG is limited to editing intelligence and returning those products to originating agencies where the information may or may not reach State and local law enforcement agencies. The NCTC must work with DHS and the FBI work to adopt a process that ensures this vital information will get to the front lines. I believe that the creation of the ITACG is a giant step in solving this problem. I believe in the ITACG program so strongly, that I have assigned a Detective Sergeant to the National Counterterrorism Center in Washington, DC for a 1-year tour. This was not an easy decision, as staffing levels in Las Vegas are at a critical level, and we are working hard in these difficult economic times to increase our staffing.

Better intelligence products are needed and direct connectivity with major agencies.

We commend Director Mike Leiter and the staff at NCTC for a new report termed "Roll Call," a new unclassified report for law enforcement agencies. Other excellent classified NCTC resources are available to some fusion centers but not accessible by operating intelligence units. NCTC has pledged to work with major agencies to allow access through DHS and the FBI.

Major Cities Chiefs' Intelligence Commanders Group plays a vital role.

As chairman of the homeland security committee, it has been my pleasure to form an unprecedented alliance of the Nation's most valuable intelligence resources—local police and sheriffs' intelligence enterprise across the Nation. We ask for your support to build an integrated national intelligence capability to counter terrorism and protect our communities from crime. The purpose of the Intelligence Commanders Group is to strengthen and coordinate the intelligence capabilities and operations of law enforcement agencies in major metropolitan areas. To date this vital network of intelligence resources has been ignored and not funded by Federal agencies and we ask the committee to support this effort so that your objectives may be realized.

NCTC must establish a stronger working relationship with law enforcement agencies.

I have been to NCTC and visited with the excellent staff who stand ready to support law enforcement. But there has been no NCTC training and this invaluable resource is not accessible by most local law enforcement agencies. We ask that NCTC expand and empower its outreach components to include training access and use of intelligence systems and databases. Liaison personnel and desk officers are needed to maintain a flow of current intelligence to State and local agencies.

Foreign Liaison is Essential.

I would like to discuss one of the programs recommended in the LEAP document: the Foreign Liaison Officers Against Terrorism (FLOAT) program. There is exceptional value in this program and it warrants further dialog and close consideration. The Major Cities Chiefs Association recognizes the legal authority of the FBI to engage in the investigation of crimes against U.S. citizens abroad. But the needs of State, local, and tribal law enforcement are different than those of the FBI. We have little need to participate in the investigation and ultimate prosecution of acts of terrorism occurring in foreign lands. But, we have a tremendous need to quickly learn about acts of terrorism, so that we can translate those lessons to better prepare our street-level first responders for similar attacks. As my good friend and colleague, Chief Bill Bratton, said, "The aim is not to sever or supplant information from

Homeland Security and the Department of Justice, but to have a multiplicity of channels of information that will allow chiefs of police to make decisions . . . ".[2]

The July 7 London subway attacks and the Madrid train bombing best illustrate the fact that the enemy may already be within our borders, and State, local, and tribal law enforcement stand ready to help in the fight against these terrorists. More recently, when terrorists attacked the city of Mumbai on November 26, 2007, cities across America watched as armed gunman created chaos and carnage in a metropolitan city of 15 million. Every major city police chief in America asked him or herself: "Could this happen in my city?" and "How would we react to a similar attack?" Thankfully, the Indian government was extraordinarily forthcoming with details, and U.S. news media was providing near-constant coverage, so information was easily and quickly obtained. Had this not been the case, State, local, and tribal law enforcement (exactly those agencies tasked with responding to the attacks) would not be able to prepare for them.

We understand that the information will ultimately be provided by the Federal Government. That is not the issue. The problems lie in the timeliness of distribution, and the relevance of the content. Would an FBI agent or DHS analyst know what questions a street cop or hotel security chief in Las Vegas would ask?

We urge the distinguished members of this subcommittee to objectively consider the advantage that State, local, and tribal law enforcement would realize—as well as our private sector partners—by quickly collecting and reporting the facts surrounding an overseas terror attack. The decisions made by public safety executives and their private sector counterparts in response to terror attacks overseas can cost taxpayers and private industry millions of dollars. The Federal Government should not interfere with, indeed they should facilitate, the efforts to collect and transmit the most current and most accurate information on which these leaders will base these decisions.

Violent crime and drug trafficking remain our top priority.

I would like to address the threat of violent crime and our borders—particularly our southern border—and how intelligence can be applied to address violent crime. While Nevada does not have a common border with Mexico, we have seen the well-publicized violence spread to our community. In October of last year, a 3-year-old boy was violently kidnapped from his home in Las Vegas. It was quickly determined by our investigators that he had been taken and was being held hostage by members of a Mexican drug cartel for a drug debt owed by his grandfather.

What we found during the investigation was that if properly applied, the information gathering capability of the Fusion Centers could be a true investigative asset. What we also found was that local law enforcement could work with the FBI, DEA, and other Federal agencies without degenerating into "turf battles" over jurisdiction. This case has a happy ending, the young boy was recovered unharmed in Las Vegas—abandoned on a suburban street by his abductors when media and public attention became too great of a risk for the kidnappers.

We know that hostage taking for revenge, ransom, and profit is widespread in South and Central America, and we can reasonably assume that this crime trend may spread north into the United States as the conditions in Mexico continue to deteriorate. As a crime that directly affects State, local, and tribal law enforcement, yet with a clear Federal nexus, we recommend that discussions begin in earnest to consider the options available to Federal, State, local, and tribal law enforcement.

Sustainment funding is needed for Fusion Centers.

In the LEAP document, it was recommended that State and Local Fusion Centers receive funding for the operational costs, as well as the costs associated with contracting and training intelligence analysts. It is in this area that we have seen the greatest improvement. DHS has performed admirably in ensuring that funding was available to train incumbent analysts, as well as allocate moneys so that agencies without sufficient analytical capability could contract specially trained personnel. Thanks to the efforts of Chair Harman and distinguished Members of this subcommittee, DHS was moved to eliminate all time restrictions related to the funding of analytical personnel assigned to Fusion Centers. As the committee has recommended, Congress should establish a dedicated grant program for this purpose, the Fusion and Law Enforcement Education and Training (FLEET). We further propose an advisory panel for DHS to identify how to further strengthen UASI and LETPP funding for intelligence and fusion centers.

---

[2] Robert Block, "Miffed at Washington, Police Develop Own Terror Plans," *Wall Street Journal* (Oct. 10, 2005) at B1, available at *https://online.wsj.com/article/SB112889637083663974.html?*.

Private security personnel are critical.

Included in the VITAL program was a recommendation to "develop clear policies and procedures for converting highly classified intelligence into an unclassified or 'less classified' law enforcement sensitive format that can be shared rapidly with state, local and tribal law enforcement."[3] Yet, there is an entire population of "First Preventers" employed in the private sector, who still are unable to receive intelligence documents identified as "law enforcement sensitive" (LES) or "For Official Use Only" (FOUO). In Las Vegas, our highly skilled, highly trained cadre of security professionals more than doubles the number of sworn police officers employed by the Las Vegas Metropolitan Police Department, and is larger than all but the very largest police agencies in this country. Furthermore, they are the best positioned to detect suspicious activity, identify the behavior consistent with pre-operational activities, and report or interdict the activity. Yet, because of LES or FOUO handling restrictions, we cannot provide private security with these documents that would allow them to be better informed. Before State, local, and tribal law enforcement can effectively team with our private sector partners, we need to consider the necessity of including LES and FOUO handling requirements. The default should be "unclassified" unless there is a compelling need to include handling restrictions, due to attestable criminal case sensitivity, or National Security reasons.

Security clearances remain a problem.

DHS has been very accommodating for sponsorship of security clearances and the FBI has likewise sponsored clearances for police officials that have membership in the JTTF, and those in the responsible chain of command. Constant promotions, retirements, and transfers of assignment in State, local, and tribal law enforcement can make it very difficult for the FBI to keep up.

While the major cities chiefs and major county sheriffs applaud the FBI and DHS for their willingness to provide clearances, there has been little progress in accomplishing a process for reciprocal acceptance of those clearances to access systems and conduct briefings. Refusal by one Federal agency to routinely accept the clearances issued by another is a disruptive policy that contradicts information sharing and threatens our progress toward realizing the goals of this committee. Chiefs and sheriffs ask for your help to resolve this issue once and for all.

DHS must restore the Law Enforcement Terrorism Prevention Program (LETPP).

Contrary to the intent of Congress, OMB, and DHS eliminated the Law Enforcement Terrorism Prevention Program (LETPP)—the only program dedicated to prevention of a terrorist attack. Although funded, LETPP is merely a quota and no longer a separate program with goals and a required plan. If there is truly a commitment on the part of the Federal Government to the prevention of terrorism on U.S. soil, the appropriation should be maintained at its original level of $500 million. I am submitting for the record a letter we previously sent to the committee and we ask that you call on the administration to correct this condition.

We need consistency in the Urban Areas Security Initiative (UASI).

Repeated changes to the UASI program have caused unnecessary conflict and confusion, a "roller coaster ride" for agencies like my own. It is impossible to plan intelligence programs from year to year when we cannot rely on consistent funding to support those efforts. Passing funds for urban areas through Governors has caused waste and delay. Annual revisions to the list of eligible urban areas preclude effective planning and coordination where it is most needed—in the urban areas most likely to be attacked. Congress should provide more clarity, stability, and consistency to the UASI program. The approved list of high threat urban areas should be finalized and unchanging.

Fellowships are key to strong partnerships.

Major cities chiefs and major county sheriffs are grateful to DHS I&A and NCTC for the recent assignment of local law enforcement officers who serve tours in Washington, DC. It has been my privilege and my pleasure to assign personnel from Las Vegas to serve at DHS in the National Operations Center, our new assignment to ITAGC and I look forward to the future assignment of our personnel to the DHS I&A Directorate.

DHS I&A should establish an advisory panel of Major Cities Chiefs.

To receive guidance and assistance from local law enforcement, we urge DHS I&A to establish an advisory panel from the major cities and counties. This sounding

[3] LEAP, supra note 1, (p. 21).

board would help to guide the new products and services to be provided by DHS, including threat advisories and other intelligence products. The Under Secretary for Intelligence and Analysis would receive support and technical assistance across a wide range of issues, including fusion centers, infrastructure protection and threat assessments.

Madam Chair and Ranking Member McCaul, those of us on the front lines look to you for your leadership and support of our mission. Local law enforcement is charged with the solemn duty to discover, disrupt, and stop plots hatched within the United States. Please know that my colleagues and I are committed to a purpose shared by this committee—the prevention of another attack and the interdiction of those who would bring us harm. We need your continued help to be successful, and I look forward to working with the distinguished Members of this subcommittee in the future.

Thank you.

Ms. HARMAN. Mr. Edwards, you are recognized for 5 minutes.

STATEMENT OF GARY L. EDWARDS, CHIEF EXECUTIVE OFFICER, NATIONAL NATIVE AMERICAN LAW ENFORCEMENT ASSOCIATION (NNALEA)

Mr. EDWARDS. Thank you.

Distinguished Members of the committee and my distinguished panel members, my name is Gary Edwards, the Chief Executive Officer of the National Native American Law Enforcement Association; and it is a privilege and honor to be able to speak with you today regarding tribal inclusion in homeland security and, in particular, intelligence and information sharing.

We, the Native American people, are the most experienced people at protecting homeland since we have been working at that since 1492 and we are still active today. Today, though our reservations are not as large as they used to be, represent over 100 million acres in the Continental United States and Alaskan villages. Also, the Hawaiian natives feel like their homeland is also connected with the Native people as well.

We have in the Continental United States over 55 million acres, over 300 reservations, 562 federally recognized tribes. Our lands are replete with oil. We have the eighth financial power in the world at the producing of natural gas. We have pipelines that run across our lands. We have railways and also interstate systems as critical junctures go right through tribal lands. We have an enormous amount of borderland, and our people sit on the border and straddle the border, which are major issues to our local communities.

With all of these assets—and another thing, just to mention that we also are a major contributor to some of the hydroelectric power grids from hydroelectricity from the power grids in the Western United States. So these critical infrastructures and the law enforcement that protects these infrastructures are still many years and decades behind our non-tribal counterparts. Primarily that is because that we do not have the training, funding, outreach, and connectivity that other law enforcement and emergency and first responders have.

Our communication systems are not quite as good as our smoke signals were when the first European intervention came to the United States. That is, that we can read our smoke signals, but the non-tribal people cannot, and their ability to send smoke signals are almost non-existent, and it is literally that bad.

We have to first become operable before we can become interoperable, and we have to be interoperable before we can really adequately share intelligence and information.

By Constitution, we are considered a little higher than the States. However, we are treated in the situations with regard to funding, information intelligence systems through the States. We have been working to make that work, but the honest answer to that question is that it isn't working. It is not because our colleagues don't want to, and it is not because they don't care about it and realize their importance. But they have their own communities that they are working on and they are responsible to, and we understand that. But it is the Congress' responsibility to find the way to get what is needed to Indian Country to be able to communicate and to be able to participate in homeland security. Because, remember, most of the attacks—even though we have a lot of rural lands—most of the attacks were planned in non-rural lands. Just like the September 11 attacks in the practice flying of the planes.

I mean, the whole thing about it is in intelligence we have to be able to get intelligence from national and international sources. With intelligence, sometimes it takes a while to develop, but we need to have an awareness out in our communities. The big things we need in the communities is the ability to take that information and make it actionable immediately, and that is the key and important part.

When you look right now at tribal land, you have a huge hole in our ability to do that. The fusion centers, we can't praise them enough, and they are a local initiative that would provide the local communities with the ability to more quickly and better share intelligence and communications. We want to be a part of that, but, in reality, they are far away from our homes, and we are really not a part of it. We are on paper, but we are actually ancient people. We are out there somewhere. We need to be an active part.

Our solution to that is to develop regional tribal fusion centers that will connect into the State and local fusion centers. But we are not going to be able to get anywhere unless the Congress watches where the funding is going, making sure that it is actually producing something. The one program that we have from Homeland Security that deals with regionalization and including tribes is due to sunset September 30. That is the only program in Homeland Security for tribes.

So we need your help, our country needs your help, and we will stand shoulder to shoulder with you and other Americans to defend our country against all oppressors as we have done in every war against the United States in history.

Ms. HARMAN. I want you to know your testimony is very important to this committee. We appreciate you coming.

[The statement of Mr. Edwards follows:]

PREPARED STATEMENT OF GARY L. EDWARDS

MARCH 18, 2009

INTRODUCTION

Chair Harman and distinguished Members of the committee, my name is Gary Edwards and I am the Chief Executive Officer of the National Native American Law Enforcement Association ("NNALEA "). I am honored and pleased to appear before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment regarding "Homeland Security Intelligence: Its Relevance and Limitations."

The assessment, judgments, evaluations, and opinions I offer to you today is based upon my service of over 28 years as a Special Agent in the United States Secret Service. During my tenure in the Service the routine use of shared intelligence and information was a part of every workday. My expertise and use of intelligence and information was honed through extensive training and field work as a Special Agent. Secret Service employees are ingrained with the deep-seated awareness that in the Secret Service protective arena there is no room for error, no excuse for not knowing and no reason for not eliminating any threat or possible vulnerability to a protective mission. The success of our protective missions depended greatly upon the help, cooperation, and sharing of intelligence and information by many professionals, organizations and agencies, especially those whose mission required collection of intelligence and information regarding terrorist and criminals.

As the CEO of NNALEA I have focused my attention on Indian countries sharing of intelligence and information and tribal participation in the information sharing environment. Much of my tribal training and experience was gained from tribal professionals who work every day on the streets and in rural communities, risking their lives to secure our homeland.

In addition, I have served on numerous homeland security advisory committees, task forces, and working groups for the Department of Homeland Security, the Interagency Threat Assessment and Coordination Group, the Department of the Interior, and the Department of Justice. I have co-authored two NNLAEA publications: "Tribal Lands Homeland Security Report" and "The Importance of Tribes at the Frontlines of Border and Homeland Security." Also, I co-developed the DHS-certified training course "Regional Collaboration and Tribal Partnerships" which is currently being taught nationally.

BACKGROUND ON NNALEA

As many of you may be aware, NNALEA is a non-profit public service organization founded in 1993, which among other things, provides a media for the exchange of ideas and new techniques, and establishes networks for training, collaboration, technical assistance, information sharing, and investigative assistance between Federal, tribal, State, and local governments and agencies and the private sector. NNALEA has conducted sixteen (16) National Training Conferences across the United States, and is currently preparing for its thirteenth (17th) [sic] National Training Conference to be held on September 08–11, 2009 in Catoosa, Oklahoma. Homeland Security Intelligence and Information Sharing will be hot topics at this upcoming National Training Conference.

A SIGNIFICANT WAR

Our Nation is engaged in a significant war against terrorism, criminal activity, and international threats against our freedom and way of life. It is a guerrilla-type warfare that has already touched our homeland and our hearts. It has violated our feeling of security. This war threatens economic stability which is in the midst of a depression. Those that wish us harm and are trying to make profit from illegal drug dealings, smuggling, acts of terror, and other crimes are waging terrible and violent war against our citizens.

On the international front our enemies threatening world peace and world economic calamity. Our enemy has targeted battlefields in our cities, towns, communities, and backyards. We have risen to the occasion united, resilient, and determined with God's help to be victorious. Our Nation's primary weapon in this fight is the timely sharing of accurate intelligence and information by those who have a responsibility to provide the intelligence necessary to protect lives, property, critical infrastructure, economic stability, and our freedom.

Intelligence and information sharing is a significant tool in this war that has been reinvented, to more seamlessly and speedily flow massive amounts of intelligence and information vertically and horizontally both domestically and internationally.

There are many experts more astute than I in the intelligence and information sharing environment and I am confident they will apprise you of the latest trends and future of intelligence and information sharing. I will share with you NNALEA's assessments, observations, and opinions regarding Indian Country's willingness to participate in the intelligence and information sharing environment, Tribal opportunities to participate in the intelligence community and the critical importance of Tribal participation in the National Strategy for Intelligence and Information Sharing.

THE IMPORTANT OF INDIAN COUNTRY

There are over 100 million acres of Tribal lands in the continental United States and Alaska native villages. Tribal lands in the continental Unites States consist of over 55 million acres and include 300 reservations. The largest reservation is the Navajo Reservation which is larger than the entire State of West Virginia with parts of the reservation in four States. Tribal lands and the Alaskan villages are federally recognized and are referred to as Indian Country. Indian Country is replete with critical infrastructure and key resources, some of which are:

- Dams; Water Impoundments and Reservoirs; Electrical Generation Plants Feeding Major Power Grids; Natural Gas, Oil and Coal Production Facilities; Major Entertainment Facilities; Critical Pipelines, Railway and Vehicular Transcontinental Highway Systems; Airports and Remote Landing Strips.
- 25 Tribal Reservations are located on and/or across the Unites States International Borders with Canada and Mexico; 41 Tribal Reservations are within 100 miles of those International U.S. Borders. Tribal Lands also include Ports and Waterways Open to Navigation from International Waters.
- Farming and Husbandry on an International Scale.
- Timber, Wildlife and Green Eco-System-Friendly Management.
- Bio-diesel-friendly farming lands.
- Major Drinking Water and Waste Systems.

The above-cited Critical Infrastructure and Key Resources on Tribal lands have much primary vulnerability and risk due to:

- The existence of non-integrated Tribal law enforcement and a lack of jurisdictional clarity;
- The minimal emergency response, and medical capacity, planning, and implementation;
- A general lack of operable communications;
- Drug cartels and terrorist organizations targeting Tribal lands and casinos for terrorist acts, illegal operations, and distribution of drugs on a national scale;
- The lack of preparedness planning, partnering and capabilities to protect citizens, property, critical infrastructure and key resources;
- Inadequate funding to develop emergency capabilities;
- Widespread Tribal unemployment;
- Inadequate medical care;
- Non-participation in State and local Fusion Centers;
- Non-Tribal organizations and agencies not willing to share intelligence and information with Tribal authorities;
- Federal Agencies unwillingness to share Tribal information with each other.

The above-listed threats and vulnerabilities in Indian Country can have a negative impact outside the reservations and do not solidify our national efforts to eliminate terrorist acts, violent crime, and international threats to our Nation.

THE RELEVANCE OF HOMELAND SECURITY INTELLIGENCE

"Not having the information you need when you need it leaves you wanting. Not knowing where to look for that information leaves you powerless. In a society where information is king, none of us can afford that."—Lois Horowitz

THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (DNI)

Relevance to Tribes.—The Director of National Intelligence is the "Master Weaver" of national intelligence, validates its collection, accuracy, analysis, objectivity, and timely distribution to appropriate users of the intelligence products produced, which include Tribes.

Limitations to Tribes.—The Office of the Director of National Intelligence has been slow to develop a national action plan for Tribal inclusion in the intelligence community (IC). There has been an effort to produce a program in Indian Country. However, its first attempt met with undesired results.

Solutions for Tribes.—We believe that DNI intelligence projects for Indian Country would be better served and more likely to be accepted by Tribes, if direct funding

for the projects was made directly to Tribes and their partners whose primary focus is a national approach to Indian Country intelligence and information sharing.

THE INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP (ITACG)

Relevance to Tribes.—The IATCG Detail and Advisory Council purpose and vision are consistent with the vision of intelligence sharing in Indian Country. The ITACG's relationship within the information sharing environment (ISE) is of great value to the Tribal and non-Tribal intelligence community (IC). The products development by the ITACG detail are right now actionable to all within the IC and ISE partnerships. The men and women that make up the ITACG are exceptional, dedicated professionals that always give their best efforts to serve their counterparts in the field. The ITACG detail and advisory council have worked hard to ensure Indian Country participation. The ITACG recently completed an ITACG Dissemination Process and Issues Survey in an effort to better serve the users of the ITACG detail products.

Limitations to Tribes.—Although the purpose and vision of the ITACG Detail and Advisory Council are clear, some of the intelligence products they would like to produce have not been forthcoming as quickly as desired due largely to the cumbersome administrative process that is to be expected in the intelligence arena.

The greatest concern for the Tribal Intelligence Community (TIC) and for the ITACG Detail and Advisory Council is the disturbing results of Tribal participation in the ITACG Dissimilation Process and Issues Survey. Of the 480 responses to the survey only 3 were Tribal, two from Tribal Fire Departments in California and one from a Tribal Law Enforcement Department in Alabama. Therefore, the outreach and awareness efforts of the ITACG are not reaching the Tribal intelligence community. There may be too many Federal intelligence and information sharing groups within the Federal Government that appear to duplicate or replicate intelligence dissemination. Many Tribal departments do not have the staff to participate in multiple groups and compare and analyze which one best serves their need for a particular vulnerability or threat. The result is that the good information provided in ITACG intelligence products are not used to their full and desired potential. We feel this is true for many non-Tribal departments as well, not to mention the cost of duplicate programs in Government.

Solutions for Tribes.—We believe the Tribal solution to this intelligence dissemination problem is answered in three actions: (1) The ITACG should partner with a national organization whose primary focus is a national approach to Indian Country for intelligence and information sharing; (2) the ITACG should reach out to Tribes with awareness training, exercises, and surveys through the partnership with the National Indian Country partner cited above; and (3) this congressional committee and the ITACG should advocate for the elimination of costly duplicative Federal intelligence and information sharing programs.

We feel the new leadership of the IATCG will remove road blocks and empower the ITACG detail and advisory council to accurately produce and rapidly disseminate ITACG intelligence products needed by State, Tribal, and local intelligence community professionals in the field.

THE DEPARTMENT OF HOMELAND SECURITY—OFFICE OF INTELLIGENCE AND ANALYSIS (I&A)

Relevance to Tribes.—Indian Country embraces the DHS I&A's commitment to change the national intelligence culture from "a need to know" to "a responsibility to provide" intelligence and information sharing to the Tribal and non-Tribal intelligence sharing environment and culture. The best way to lead change is through example. Indian Country law enforcement and other Tribal first responders desperately need and seeks real-time, accurate intelligence and information from the DHS I&A regarding: (1) Threats related to border security; (2) the threat of radicalization and extremism; (3) threats from particular groups entering the United States; (4) threats to the homeland's critical infrastructure and key resources; and (5) information regarding weapons of mass destruction and health threats. These five areas of intelligence and information sharing for which DHS has analytic thrusts are extremely important to Tribal communities on a daily, even hourly basis to save lives, protect property, prevent destruction of critical infrastructure and key resources, preserve economic systems, and contribute to the defense of the United States of America.

Indian Country is pleased with the appointment of Governor Janet Napolitano as the Secretary of the Department of Homeland Security. In her former position as Governor of Arizona, she has grained extensive knowledge of Indian culture and values. Arizona has the greatest population of Native Americans that any State in the

continental United States. Secretary Napolitano's quick action to bring consultation between Tribe and DHS is historic and long overdue. We commend and join the Secretary in her support for State and local Fusion Centers as the "centerpiece of our mutual intelligence future." Currently, partners in Indian Country are already planning for "Tribal Regional Fusion Centers" (TRFC). We look with anticipation to the TRFC's interaction with State and local Fusion Centers and becoming an integral part of the intelligence community and the information sharing environment.

Limitations to Tribes.—Tribes have many limitations preventing participation with the DHS I&A information sharing environment and intelligence community. Some of the limitations are: (1) A lack of recognition by DHS of Tribal sovereignty; (2) the DHS minimal outreach to Tribal leaders and officials; (3) regularly overlooking Tribes to participate in National, regional and State homeland security exercises and events; (4) on a yearly basis, DHS's provides inadequate funding for Tribal programs regarding homeland security planning, training, equipment, connectivity, partnership building, and inclusion in DHS national programs; and (5) the lack of outreach, awareness, a favorable location, cooperation, funding, training, cultural issues, sharing of intelligence and information, and partnership building on a national basis, limits Indian Country's willingness to daily participate in State and local Fusion Centers.

Solutions for Tribes.—Most of the above cited limitations can be eliminated within a short time cycle with the combined effort of the White House, this Congressional committee, and the Secretary of Homeland Security. The DHS Tribal solutions are:

(1) Secretary Napolitano began removing the first cited limitation when she recently instituted a DHS policy of Tribal consultation between the DHS and Tribal governments. This government-to-government relationship recognizes Tribal sovereignty;

(2) The President, Secretary Napolitano and Congressional Members participation in national Tribal events and meetings with Tribal leaders can remove the 2nd limitation;

(3) A sincere effort by DHS program directors inviting Tribal leaders send Tribal representatives to participate in National, regional, and State exercises and events will yield partnerships and Tribal support for DHS National, regional, State, and Tribal projects and thereby remove another limitation;

(4)(a) NNALEA and the National Congress of American Indians (NCAI) request a minimal increase of the Tribal portion of the SHGP from 0.1 percent to 1.0 percent and to allow Tribes to apply directly to DHS for all grant programs rather than through the States. (b) DHS provided funding and support for Tribal Homeland Security programs and initiatives to national organizations whose primary focus and body of work is a national approach to Indian Country homeland security issues and whose organization houses the expertise necessary to carry out a national program for Indian Country. (c) DHS providing continuation funding for successful Tribal training programs and initiatives that encourage regional Tribal inclusion in programs like intelligence and information sharing (note: the only Tribal DHS certified "Regional Collaboration and Tribal Partnerships" training program that will have reached 60 regional training sites Nation-wide should receive continuation funding to deliver that critical partnership training after October 1, 2009.)

(5)(a) Generally, Indian Country supports the concept of State and local Fusion Centers so much so that plans are underway to develop a Tribal Regional Fusion Center on the Navajo Reservation to connect Tribes in its region directly to State and local Fusion Centers. (b) DHS funding and DHS I&A support are critical for TRFC plans to be successful. (c) The success of Tribal Regional Fusion Centers can eliminate most of the limitations cited above for Tribes and their participation in State and local Fusion Centers. (d) The Bureau of Indian Affairs, Office of Justice Services (BIA–OJS) must be a major component of any intelligence and information sharing initiative for Indian Country like the Tribal Regional Fusion Centers. BIA–OJS is the premier national law enforcement agency for Indian Country whose primary mission is Indian Country law enforcement. (e) The DOI, Office of Indian Affairs should be a partner and leader in Tribal homeland security intelligence and information sharing initiatives by DHS I&A and the DHS intelligence enterprise (IE) internal partners.

CONCLUSION

For the protection of our homeland to be successful, our Nation must have a seamless network of homeland security intelligence and information sharing. To be seamless, this network must include Tribes. Tribes, though, are often left wanting for homeland security information. This, in turn, limits our Country's network of

homeland security intelligence and information sharing. Fortunately, intelligence and information sharing with Tribes can be fixed rather quickly through the actions delineated above by the White House, this Congressional committee and the Department of Homeland Security.

I am happy to answer any questions you may have.

Ms. HARMAN. Chief Gaissert, you are recognized for 5 minutes.

STATEMENT OF CHIEF JOHN W. GAISSERT, COMMERCE, GEORGIA, POLICE DEPARTMENT

Chief GAISSERT. Thank you, Madam Chair, distinguished committee Members, and esteemed panelists.

Terrorism is a phenomenon that perhaps represents the defining issue of our time. It is a challenge that requires an entirely new dimension for operational readiness for law enforcement and all other public agencies.

We have been blessed as a Nation not to have had a major terrorist event on United States soil since 9/11. However, to quote Jefferson in 1801, "Eternal vigilance is the price of liberty." I submit that our resources for intelligence and information sharing must be focused within this context.

I am making some recommendations and conclusions regarding our intelligence efforts.

No. 1, the United States should make good use of the Israeli model for homeland security. There is a reason that their counterterrorism measures stopped more than 90 percent of attacks. Central to this success is intelligence dominance derived from integrated resources and combined with the ability to rapidly conduct surgical interdiction of terrorist operations. The result is to reduce or neutralize threats and minimize collateral damage, including civilian casualties.

I want to add as an addendum here that I am not talking about some KGB-style program to spy on citizens, but the Israelis have the ability, from a grassroots level, to develop information and data that can point to threats early. There are any number of pre-attack indicators which do not include the profiling of individuals. It is a matter, as most street cops would tell you, of being able to determine things that are out of character and out of place. The street cop isn't looking for the normal; he is looking for the abnormal.

No. 2, domestic law enforcement must assess and evolve their training doctrine to address the potential for asymmetrical tactical threats posed by the phenomenon of terrorism. In Israel, an officer responding to a traditional crime reacts traditionally. If he finds something else, if it is terrorist related, he stops thinking like a cop and starts thinking like a soldier. Because his adversary is trained using small unit infantry tactics with assault security and support elements. It requires a different tactical approach; and we need to train for that dimension, including its implication for the rules of engagement.

No. 3, consider designating an intelligence officer in every State or local law enforcement agency, regardless of size, and process that officer for an appropriate level of clearance. I believe unless something is changed, you can obtain a "secret" with a national agency check.

No. 4, expand access to information technology such as the GTIP program in Georgia to facilitate the flow of information between

partners. I applaud Commander McNamara. I think if we could standardize a reporting format, it would be highly advantageous to the national interest.

No. 5, money is policy. Consider additional funding of law enforcement training for counterterrorism, particularly at the local level. There are alternative mediums to facilitate such training.

I also recommend expanding that to civilians, to civic groups, and to educate our populace as to what they might be seeing in terms of pre-attack indicators. This could be facilitated through the United States Attorney, the auspices of State training agencies, and so forth.

No. 6, review the Homeland Security Advisory System as it relates to public release. Consider adding specific public guidance at each level of alert or eliminating the alert status altogether for public notice.

One of the weaknesses that I find in this system is that what we are doing is issuing some vague public alarm which causes potentially a sense of unease, and this could actually support terrorist objectives.

Madam Chairman, in closing, let me say that any measure considered for Homeland Security must be balanced with the expectation of privacy and the inalienable rights of the American people. As Dr. Franklin once observed, "Those who exchange freedom for security end up with neither freedom nor security." If we concede our freedoms, the terrorists win.

I pray that the Lord will have mercy on this Nation and that he will sustain our way of life.

[The statement of Chief Gaissert follows:]

PREPARED STATEMENT OF JOHN W. GAISSERT

MARCH 18, 2009

Terrorism is a phenomenon that perhaps represents the defining issue of our time. It is a challenge that requires an entirely new dimension of operational readiness for law enforcement and all other public safety agencies. We have been blessed as a Nation not to have had a major terrorist event on United States soil since 9/11. However, to quote Jefferson in 1801, "Eternal vigilance is the price of liberty." I submit that our resources for intelligence and information sharing must be focused within this context.

In my professional judgment, failure to know the enemy is the fundamental weakness in both developing homeland security counterterrorism measures and prosecuting the war in general. In the 6th century B.C., General Sun Tzu wrote, "The Art of War". He said that every battle is won before it is ever fought. One of his central propositions is that you must become your enemy in the sense of not only understanding his tactics but his epistemology; that is what he believes about the world, his ideology, religion, and dedication to those belief systems.

In my judgment, the radical Jihadists are committed to bringing the world under submission to Allah. They are religiously motivated and convinced that Allah has commissioned their Jihad to precipitate the end of the world according to their teachings and tradition. Alternatively, they intend to impose obedience by conversion or eliminate infidels. Their endgame strategy is simple:

a. It is a zero-sum game; either win or lose.
b. Destroy the Jewish State of Israel.
c. Establish a global Islamic theocracy under Sharia Law.
d. No time constraint to accomplish both political and religious goals.

Dr. Bruce Hoffman at Georgetown describes the conflict as a ceaseless, generational struggle. This conclusion is arguably correct in view of the last 1,500 years of Islamic fundamentalist history. However, I place the genesis of the conflict in the Book of Genesis. It began 4,000 years ago with a man named Abraham and two boys, Isaac and Ishmael. No one will have a viable paradigm to understand the

current threat without a grasp of the Old Testament Canon, as well as The Koran and the Hadith. The conflict can be viewed as a continued outworking of the enmity set between these ancient protagonists. This same animus can be traced through Biblical times to the sixth century A.D. and the advent of Islamic fundamentalism. The result is for some to view the current dilemma as a clash of cultures and others to view it as a clash of civilizations. However, I submit that ultimately it can be understood best as a clash of religious belief systems; Judeo/Christian and all others versus Islamic. The scope of this testimony precludes specific contrasts in beliefs, but it ultimately begs the question, "How do you apply traditional secular solutions to a conflict which at its nexus is a religious dispute?"

Without a grasp of this history, the United States' strategic decisionmaking processes could result in serious miscalculations vis-à-vis intelligence functions, public safety training and domestic operational response. We are engaged in what could be characterized as 4th generation warfare and face asymmetrical threats. Terrorist combatants are predominantly non-state actors but in many instances act as proxies for nation-states. The transnational nature of terrorist attacks should be examined from the perspective that these are not random acts of violence, but they represent different fronts in a global Jihad.

Since al Qaeda has become as generic to terrorism as Xerox has to photocopies, I shall use that term to describe all affiliates and rogue groups; albeit they largely have common purposes. As Dr. Boaz Ganor, Institute for Counter Terror, Herzliya, Israel notes, "Terrorists have an inter-national network, battlefield experience and learn from their mistakes." He further defines the salient difference between terrorists and other labels such as guerilla or freedom fighter. Terrorists target civilians and non-combatants; they sanctify death. Based on my training and experience, it appears that our domestic counterterrorism doctrine has not fully addressed the evolution of terrorist strategies or their dedication to the endgame. We are not just fighting a war on the battlefields of Iraq and Afghanistan, Central Theatre. The Jihadists or their sympathizers are fighting us in multiple dimensions largely transparent to the American public and using deception as a key strategy. I shall name only a few examples that bear directly on law enforcement responsibility and the need to assist in developing actionable intelligence.

They are fighting us using financial crime to counterfeit clothing, pirate CD's, DVD's, sunglasses, and other articles, perpetrate related fraud and the criminal laundering of money. In the world of information technology, there are over 7,000 Jihadist Web sites. Many of these sites can be used covertly to communicate with potential sleeper cells. They operate domestically using false identification or forged documents. The Israeli concept that terrorists commit small crimes before they commit big ones is particularly useful in domestic deterrence efforts. By example, officers might detect traffic violations, criminal trespass, false identification, or giving false information.

This context and these considerations have profound implications for the modalities ultimately employed to deter and interdict terrorist operational capabilities. Dr. Boaz Ganor asserts that intelligence is the key to successful counterterrorism initiatives. In fact, the Israelis operate on the concept of intelligence dominance. Information and/or data are fluidly moved through varied levels of responsibility with potential corresponding operational responses initiated in a brief period of time. I shall not discuss specific operational capabilities in open source material, but the concept is reasonably clear.

We need to ensure minimum barriers consistent with operational security (OPSEC). This approach should be integrated with State and local law enforcement as well as Federal, regional, and international security partners to achieve required intelligence objectives. While there are obvious reasons to view intelligence strategically, I recommend that greater emphasis be placed on training, funding, and communicating with local resources. One of the best sources of information in this Nation is the old street cop. On the beat or mobile, cops are sensitive to things that do not look right or do not sound right. By extension, involving corporate or private security, educating the public and civic organizations are important tools for developing the type of grassroots information required to enhance deterrence of further terrorist events.

We can most assuredly benefit from Dr. G. Edward Deming's organizational theory that quality of outcome is based on the continuous improvement of processes. Additional emphasis on improving intelligence sharing, particularly at the local level, could produce dramatic results. Remember, it was a rookie cop on a routine check that resulted in the arrest of Eric Robert Rudolph in North Carolina despite the commitment of enormous Federal resources. In my own jurisdiction, Commerce Police Department has been involved in providing many potential leads and infor-

mation of an unusual nature to the Georgia Intelligence Sharing and Analysis Center (GISAC) since 2001.

The city of Commerce is in Jackson County, Georgia. It is located approximately 55 miles northeast of Atlanta. We have a semi-rural environment bisected by Interstate 85 and other major State transportation corridors. Although we have emerging growth, there is still a significant agricultural presence. Smaller towns and communities dot the landscape. However, we are not immune from the potential for atypical events. Two of the 9/11 hijackers did touch-and-go landings at Jackson County Airport while flight training out of Gwinnett County. Local jurisdictions must be cautious to heed the "Terminal Philosophy"; it cannot happen here, and it cannot happen to me. There is no guarantee that attacks or the training for those operations will occur only in large cities.

Since 9/11, another example of concern for some local citizens is the presence of a Muslim of America (MOA) compound less than 10 miles from Commerce called Medina Village. I have been the Chief of Police in Commerce since 2001 and have seen local concern ebb and flow through the ensuing years. The MOA organization is reported to be affiliated or linked to Sheik Mubarak Galani in Pakistan. There have been and are residents of Medina Village who either work or patronize businesses within our jurisdiction. No violent incidents have been associated with the group at this time.

There are numerous examples of information provided by our agency to GISAC. We had a reported theft of 300 gallons of diesel fuel from a local supplier. In another time, we would start looking for farmers or commercial drivers. In today's world, consideration also had to be given to the possibility that the fuel might be used to construct an improvised explosive device. In another instance, a phone call made to a propane gas company resulted in the reporting of unusual questions and interest expressed about tank capacities and operational procedures not relevant to private use.

In my judgment, one of the considerable weaknesses that developed during the decade of the '90s was the degradation of human intelligence (HUMINT) in favor of signal intelligence (SIGINT). I simply do not know how to successfully substitute technology for eyes and ears; boots on the ground. The Israeli Model is well-suited to account for a balanced approach to this issue. We are fortunate that our GISAC fusion center has provided excellent support in the form of law enforcement assistance and regular Law Enforcement Bulletins. However, most of the information condensed and presented in the bulletins could be researched from open-source material with the exception of some additional law enforcement sensitive information.

The unclassified FBI briefs on terrorist attack planning and "dry run" tactics indicate that terrorists use dry runs during the final stages of operational planning to simulate an actual attack, expose strengths and weaknesses in the plan and make adaptations to the operating environment. Terrorist surveillance and reconnaissance of potential targets offer law enforcement and security personnel opportunities to observe their activities and implement investigative, counterterrorism and force protection measures. Indicators include such activities as observing security reaction drills or procedures, monitoring police radio frequencies and response times, or photographing unusual places. The best resource in position to initially assess these types of activities is none other than the street cop, security officer, or an observant citizen in the local jurisdiction. Expanding the community policing programs in our local jurisdictions to accommodate counterterrorism intelligence could complement and leverage the gathering of pertinent information. This is not to recommend a KGB-style program to spy on your neighbor, but we should actively seek to educate the public on being aware of surroundings and reporting events that are out of character or out of place.

One of the striking observations that I made on several training missions to Israel was the level of sensitivity on the part of average citizens to odd occurrences and their willingness to report unusual activity. Of course, a large percentage of Israeli citizens are veterans of the armed forces, police, or other emergency services and by extension have specialized training. I also found that the incident response of street officers was dramatically different than basic police training in Georgia. The Israelis have uniquely integrated both military and civilian police doctrine such that an officer responding to a traditional crime responds in a traditional way. However, should they discover a terrorist-related event, they stop thinking like a cop, start thinking like a soldier, and react accordingly. The reason is that their adversary is trained using small unit infantry tactics incorporating assault, security, and support elements. This is particularly important in a Mumbai-style armed assault. However, it demands crucial training officers regarding the rules of engagement. Since the two most prevalent types of attack are still bombings and armed assault, Israeli po-

lice actively train to tactically address multiple assailants in a dynamic environment.

In Georgia, we have many officers limited to punching holes in two targets when the whistle blows for annual qualification. They receive little in the way of additional training in tactical response. My opinion is that our tactical teams and other specialized police units are very well-trained by comparison. Although it is perfectly fine and desirable to have a state-mandated and standardized course of fire to qualify annually, I am convinced based on professional experience that officers will respond like they train. This is not to be critical but to point out an opportunity to evolve our training doctrine in a positive way. The great obstacle to advanced training today is the same as it has been historically; funding. There is a symbiotic relationship between policy and money. When I was a Navy Lieutenant, I once worked for a Commander who had a big sign on his desk that said, "Money is Policy". It stuck, and I have had that notion reinforced experientially. The Law Enforcement Liaison for the United States Attorney, Northern District of Georgia, advised me that their office received $100,000 post-9/11 for counterterrorism training. They have received no additional funding since that time. When training requirements are triaged, the funding has to be carved out of the operating budget highlighting continued resource limitations. This condition is not limited to tactical training operations but general training as well.

Some sources point to an emerging nexus between organized crime and terrorism with mutually supportive interests. According to Associated Press, about 7,000 people have been killed in the Mexican drug wars since 2007. The violence is spilling into U.S. cities in some parts of the country. There have been reports of drug cartel members settling scores with adversaries in such places as Atlanta, Phoenix, and Birmingham, Alabama. I suggest that the potential for drug violence to spread into smaller communities will grow significantly. This is a wake-up call to either secure or control the border. We probably should know something about the individuals coming into the United States. In any event, this issue places a further burden on State and local law enforcement, and it highlights the escalating importance of the intelligence partnership with Federal authorities. The southern border could be an Achilles heel for the United States and serve al Qaeda as an easy point of entry through which to infiltrate operational teams. By the way, the border is the first line of defense in Israel.

Since al Qaeda is now using what might be characterized as a "Dune Model" of operations, their strategy is disappearance instead of an institutional presence. Command and control are shifting or based on loose cells or lone operators. This approach was religiously validated by Osama bin Laden's spiritual mentor, Abdallah Azzam. Subsequently, Bin Laden issued a fatwa that Muslims have an individual as well as a general duty to Jihad. We also are seeing the Da'awa (call) to recruit and radicalize converts within western industrialized nations. Remember, the attacks against the London subway system were perpetrated by British citizens and not foreign terrorists. This is another issue that ups the ante for State and local law enforcement resources. We must be trained competently in counterterrorism measures supporting intelligence dominance. The potential attackers could submerge anywhere in our society as individuals or sleeper cells.

One bright spot in Georgia's intelligence effort is the development of the GTIP Program by our fusion center. GTIP is a secure Web-based threat/leads tracking system that is law enforcement-sensitive. Complete access to the system is available to GTIP partners and limited access, such as read-only, may be made available on an as-needed basis. GTIP is a Georgia Bureau of Investigation (GBI) program funded by Department of Homeland Security (DHS) grants to enhance the intelligence capabilities of key major law enforcement agencies across Georgia. The E-Team program is the name of the secure Web-based software used by the participants and managed by GISAC fusion center supervisors to process and address tips or leads for appropriate action. This provides an emerging high-tech tool to facilitate information sharing and coordination of counterterrorism activities among partners. By definition, counterterrorism measures are offensive (military) or proactive (law enforcement), whereas anti-terrorism measures are defensive and tend to be self-enforcing such as the wall of separation between parts of Israel and designated Palestinian areas to prevent uncontrolled access to the country.

As a final note, my Israeli contacts do not hold the Homeland Security Advisory System in high esteem. The primary reason is that it conveys a vague sense of alarm to the public without specific guidance for appropriate action. I recommend that this process be reviewed to enhance its effectiveness. There is specific guidance for public safety entities within each level of alert similar to the military defense condition (DEFCON) system. However, vague alarms can arguably precipitate a general unease that actually supports terrorist objectives.

My recommendations and conclusions are summarized as follows:

1. The United States should make good use of the Israeli Model for Homeland Security. There is a reason that their counter measures stop more than 90 percent of attempted attacks. Central to this success is intelligence dominance derived from integrated resources and combined with the ability to rapidly conduct surgical interdiction of terrorist operations. The result is to reduce or neutralize threats and minimize collateral damage including civilian casualties.
2. Domestic law enforcement must assess and evolve their training doctrine to address the potential for asymmetrical tactical threats posed by the phenomenon of terrorism.
3. Consider designating an intelligence officer in every State or local law enforcement agency regardless of size. Process that officer for a security clearance through the FBI Liaison Program in order to enhance processing of sensitive or classified information.
4. Expand access to information technology such as the GTIP Program in Georgia to facilitate the flow of information between partners.
5. Money is policy. Consider additional funding of law enforcement training for counterterrorism particularly the local level. There are alternative mediums through which to facilitate training programs.
6. Review the Homeland Security Advisory System as it relates to public release. Consider adding specific public guidance at each level of alert or eliminating the alert status altogether for public notice.
7. Winning does not necessarily mean annihilating the enemy. Stabilizing areas of conflict and maintaining our way of life may prove to be a better measure of success. Employing the Roosevelt Doctrine of speaking softly but carrying a big stick could prove to be useful while seeking diplomatic accommodation.

Mr. Chairman, thank you for the privilege of testifying before your committee on a topic so vitally important to the security interests of the United States. In closing, may I say that all measures considered for homeland security must be balanced with the expectation of privacy and inalienable rights of the American people. As Dr. Franklin once observed, "Those who exchange freedom for security end up with neither freedom nor security." If we concede our freedoms, the terrorists win. I pray that G-d will have mercy on this Nation and sustain our way of life.

Ms. HARMAN. Thank you all for excellent testimony. All of you not only addressed the need to collect information but the need to protect civil liberties, and I think every member of this panel applauds that.

I often use a precious sound bite, Chief Gaissert, based on what Ben Franklin said. My version is: Security and liberty are not a zero-sum game. You either get more of both or less of both.

Obviously, this committee is determined on a bipartisan basis—I am sure everyone agrees—to get more of both; and that is why we are starting today with this hearing.

Commander McNamara, I read ahead; and you are going to hear some comments from the second panel about SARs and some of the risk of SARs. Would you describe it briefly, what it is? I know it is in your full testimony, but not everyone in the audience has read it, your full testimony, that is. What is it, and what isn't it?

You mentioned that you have gone national with this idea. Who is using it, and is DHS using it or should DHS be using it?

Finally, if we would have had SARs up and running somewhere here in some port city, could it have been useful to guard against a Mumbai-style attack?

Ms. MCNAMARA. Thank you, Madam Chair. All great questions and thank you for that opportunity.

The SAR process, as the Sheriff or the Chief mentioned, is about indicators, identifying the indicators that—all pre-operational in terrorism in domestic and international cases. We found a common thread. So we identified in Los Angeles about 65 indicators. Train-

ing your officers on those indicators so that they are aware of what is happening.

Ms. HARMAN. Could you list a couple so we get a better idea?

Ms. MCNAMARA. Absolutely.

Obtaining illicit explosives is one that is an obvious one. It is one that we never listed before. Putting our officers in contact with that.

Securing security measures or taking security plans. Our officers run across many times that type of thing.

Suspicious photography, but suspicious. I had a recent example of a laundromat who found a disk in the pocket at a local cleaners. They looked at the photographs, and they happened to be of a local airport: the fence line, the TSA, the airplanes on the tarmac. They handed that over. We took that report.

Interesting enough, we did the investigation; and it happened to be an airport personnel taking those photographs. But had we not had that capability, that would have been one of those unknown things.

So SARs gives us the ability not only to investigate and connect dots; it helps us eliminate potential threats as well. So we are training in Los Angeles specifically on the indicators for our officers.

As you can see, it has garnered a lot of success.

Ms. HARMAN. Who makes a decision what becomes a "dot" on your map and what doesn't? Does the individual who has the training? Or is there some kind of supervision and perhaps some punitive action against those who are not careful?

Ms. MCNAMARA. I think that is the greatest thing about it. We took our crime report from Los Angeles, and there is a lot of value on our crime report, and we adjusted the crime report. All cops in Los Angeles are very familiar with the crime report. They just put exactly what happened. Like the case of the laundromat, they write the details.

Those details, that report, is then—a supervisor in Los Angeles then reviews the report, makes sure that it is reported properly. So every supervisor in Los Angeles has been trained on this SAR process. So they understand the difference at the front-line level.

Once a SAR is signed by a supervisor, then it goes to our Criminal Intelligence Bureau where they code it so they put the indicator numbers so we know that that indicator is appropriate.

Ms. HARMAN. So there are really three sets of eyes: the intake, the supervisor, and the dot decisionmaker on each report; and the reports are standardized—I know this is part of the magic of this—so that it is apples-to-apples. Then you put this stuff up on a map and these dots appear, and if a lot of them appear around a particular facility, that is cause for concern; is that right?

Ms. MCNAMARA. That is correct.

I would like to add another layer. Because before managers and executives at my level were not able to see these pictures emerging, it is a management accountability tool as well. I have seen several patterns emerge that I have been able to address——

Ms. HARMAN. In 29 seconds, can you tell us if this device could have helped with the Mumbai-style attack?

Ms. MCNAMARA. Absolutely. Cops ask the right questions. In the report, they are more specific to date, to time, to location.

If the Mumbai attacks had SARs, we would have been able to predict the time of attack. We would have been able to put the proper resources into place to prevent a terror attack.

Ms. HARMAN. I yield 5 minutes of questions to the Ranking Member, Mr. McCaul.

Mr. MCCAUL. Thank you, Madam Chair.

I want to make a few comments and throw out a general question.

Commander McNamara, I commend you for putting out the SAR program. I think it is a real model. It is a great idea coming from a local area, and I look forward to the integration with DHS in terms of trying to develop this model across the Nation.

Sheriff Gillespie, I want to comment on the idea of this foreign liaison that you mentioned and the advisory board. That is something I would like to take a stronger look at. Security clearances are going to continue to be an issue, and I am sure that Madam Chair and I will be working closely on that.

Mr. Edwards, the tribal lands had been ignored in this process; and I think it is time we start looking and paying attention to that. I have several tribes in my State of Texas, many right on the border; and that is an area of tremendous concern. So we look forward to working with you on that important issue.

Finally, Chief Gaissert, I liked your comparison to the Israeli model. As I mentioned in my opening statement, we met over in Israel with the Minister of Security. He told us how it is really intelligence. You win this by good intelligence. They—we have a lot to learn, I think, from Israel; and I was very interested in your comments on that.

Finally, you said in your statements that terrorist commit small crimes before they commit big ones. We refer to the traffic violations of the 9/11 highjackers, Tim McVeigh. It is a good example of how we caught somebody on a traffic violation.

What I am interested in is when I worked in the Justice Department, really the only thing we had to share information or integrate after 9/11 were the Joint Terrorism Task Forces. The idea of these fusion centers was just a sort of a concept. At that time, it was nowhere near a reality. It is still not a reality, I think, to the extent that maybe it should be across the Nation.

So I just wanted to throw that out with the 2½ minutes that I have for anybody who would like to answer that question. Can you tell me the current state of your relationship with these fusion centers and with the Joint Terrorism Task Forces and how we can better improve that coordination?

Sheriff GILLESPIE. You know, from the Las Vegas perspective, Mr. McCaul, I would say we rely heavily on the fusion process in our day-to-day crime fighting as well as the integration of homeland security-type information. I think the ricin incident that was talked about before was a prime example of that.

No. 1, it was a cop on the street that realized that a sick individual, some of the writings in the room, and animals not feeling well—the cop put the dots together on this and immediately contacted our fusion people. With the process of that, from our stand-

point, we started looking at a local. Then when we started to see some of the signs that we did, we were easily integrated into the Federal side of it.

Then our response to it. If we hadn't been proactive in our all-hazards approach to not only the investigation but the mitigation of these types of situations, we wouldn't have had the ability to send a specially trained group, cross-disciplined, cross-organizations. Our two fire departments and our police department participate in our ARMOR program; and, basically, we have a hazardous material, a C-burn, and an explosive response with an investigative component. They responded out there. They were able to determine if there were any ricin levels out there or in another hotel room.

But the other part I will say is we are not there yet. We at the local law enforcement need to be integrated at the national level and developing the policies that are created to expand upon that which we currently have. We can't be the afterthought. We have to be there initially.

Mr. MCCAUL. Commander McNamara, can you tell me about your relationship locally with your fusion center with your SARs programs?

Ms. MCNAMARA. I think as we move forward on the SARs process it is going to add the structure that the fusion centers need right now. I love the concept of the fusion centers. By having the correct mechanisms at the fusion centers, it adds that structure. It gives you that ability to paint that regional picture that you are looking for and connect those dots regionally. Then, of course, to our partners like Sheriff Gillespie, we enjoy a great relationship and they talk over cross-border.

So I really like what the future looks for at the fusion center with the SARs process being interjected.

Ms. HARMAN. Thank you, Mr. McCaul. I just would note that at a hearing in the last Congress, where Mike Leiter, the head of National Counterterrorism Center, testified, he made the point that someone in the ITACG suggested that in an intelligence product prepared by the ITACG, they should describe ricin. Now that you hear what I just said, it seems incredible that a product saying ricin is a threat in local areas wouldn't describe what it looks like. Fortunately in Las Vegas they have very smart cops.

The Chair now yields 5 minutes for questions to Mr. Carney of Pennsylvania.

Mr. CARNEY. Thank you, Madam Chair.

First let me say in listening to your testimony, I am very heartened by the quality of folks we have in the field on the front lines. It makes me feel a little bit better. The task that you have is enormous. But for starting with this quality, there is no task we can't manage.

Let me ask a question to all of you from about the 50,000-foot level. What keeps you up at night in terms of terrorism? Ladies first, I guess.

Ms. MCNAMARA. I think I feel better about sleeping now that we have the ability to connect these dots that we talk about. Prior to this process, prior to being able to paint a picture what is going on in your local communities, being able to protect your communities, knowing that you had this tremendous responsibility once the par-

adigm shift occurred after 9/11, that you did not have the mechanisms and the standardizations in place to see emerging patterns and to redeploy appropriately, that is what kept me up.

What keeps me up now is the excitement of where this process is going and what is going to happen to make this America safer.

Mr. CARNEY. Thank you.

Sheriff.

Sheriff GILLESPIE. Actually I can be very honest in telling you that I sleep well. I won't tell you that there aren't things that bother me, but I know that there are many people in my profession, State, local, and Federal, that are literally working long hours and days to keep not only their communities, but this country safe.

But with that being said, even pre- the Mumbai incident, one of the things in my hometown that we have constantly talked about and constantly worries us is not necessarily the al Qaeda attack, but the individual and/or individuals wishing to make a statement. They may not necessarily be from abroad; they could be very well within. So I can tell you that that is the one aspect of my job that continually raises the hair on the back of my neck.

Mr. CARNEY. Thank you.

Mr. Edwards.

Mr. EDWARDS. There are actually two things that keep me awake at night when I look at tribal issues. One is the tribal families that live on or near the borders and the terror and decisions that they have to go through on a daily basis. Most of them are unemployed, or a lot of them are, very poor incomes. You have a tremendous threat of people trying to pay for their way to get their support. Some of them are family members, you have those terrors, and some of them are just afraid because of violence going on in their neighborhoods. Then I worry about that spreading from Indian Country to the other non-Indian Country outside the reservations.

The second thing that keeps me up is the vastness of Indian lands and the lack of protection and the lack of law enforcement. I worry about some group, whether it is national or international, that plan and plot a terrorist act that takes place in the United States, devastates the reservation, devastates the non-Tribal communities, and the Tribes are looked at as not doing their job and letting the country down, and we are not that way as Indian people.

Thank you.

Mr. CARNEY. Chief.

Chief GAISSERT. Congressman, I am confident in the abilities of American law enforcement. With that said, I have a concern about the potential for sleeper cells. We know that al Qaeda is recruiting and radicalizing within the Western industrialized nations. I would like to point out it was British citizens who attacked the London subway, not foreign insurgents or foreign terrorists.

Also, I want to take a moment to just tell you how critically important I believe it is to educate and train our first-line responders, particularly the street cop, because it is the ability to interdict or to develop that critical data or information at the ground level that may deter the attack. Remember, it was a rookie cop that netted Eric Rudolph, not the vast Federal resources committed in North Carolina. It touches the local level.

We had two of the 9/11 highjackers who did touch-and-go landings at Jackson County Airport in Georgia prior to 9/11. I worked for a commander at one that had a sign on his desk that said, money is policy. It assumes to be a symbiotic relationship between the two. I hope we can at least place greater emphasis on that process.

Thank you.

Mr. CARNEY. Thank you. That sign on the desk is amazingly candid actually.

I have a lot more questions. I will yield back, though.

Ms. HARMAN. Thank you.

The Chair now recognizes Mr. Dent of Pennsylvania for 5 minutes.

Mr. DENT. Thank you, Madam Chair.

I guess I will take a slightly different spin on Congressman Carney's question. As opposed to what keeps you up at night, is there an overarching intelligence need that you all have in common? If there is, do you think the DOJ and Homeland Security Department are doing enough to help you meet those needs?

I guess I will start at the other end. Chief Gaissert.

Chief GAISSERT. Thank you, Congressman.

It has been my personal observation that we have certainly improved the communication between State, local, and Federal agencies since 9/11. But to use Dr. Deming's management concept of trying to approach it from a process of continuous improvement, there is certainly room to grow that relationship.

We receive bulletins both from the Fusion Center, from Joint Terrorism Task Force and various sources, but I think there is a huge opportunity to better improve that process. As I indicated in my earlier testimony, if we had a designated intelligence capability within each agency, that might help facilitate that process.

Mr. DENT. Thank you.

Mr. EDWARDS. I believe that the greatest thing that is needed is getting people on-line and getting the information moved along more quickly. I think we have a lot of duplicative efforts that now in times of troubled economy that we don't need. We have people that don't know the roles in intelligence, and they are not getting the information out in a timely fashion. They don't understand about the collection procedures and how it is distributed even on a national basis. I think a lot of attention should be paid to that quickly, and there should be demands made by Congress that they report back as to progress they have made within a short period of time.

Mr. DENT. Sheriff Gillespie.

Sheriff GILLESPIE. No doubt improvements have been made since 9/11; however, from my perspective, I read a book once, "Five Dysfunctions of a Team", and fear of conflict and lack of trust—I believe those are the stumbling blocks to us in our information-sharing process. I believe we are making inroads, but as I stated before, that aspect of including us in the development of policies and protocols is essential to this information sharing from an intelligence standpoint throughout America.

Mr. DENT. Who don't you trust?

Sheriff GILLESPIE. Well, I don't think it is that I don't trust. I think other agencies don't necessarily trust. I think there is ingrained levels of distrust within law enforcement communities. I use an example, when I was a street cop, I would carry around my notebook, and I still have it today. I used to write a lot of information in it. In the early days in policing, you didn't hand that off to someone, you kept it pretty close to yourself.

Over the years we have learned that that is not the most appropriate way nor the effective way or efficient way to do policing. We are dealing with that at the national level, and I don't think we can turn a blind eye to it. I don't think we can ignore it. You have to deal with the brutal facts, and the brutal facts are we are not necessarily exchanging the information as quickly and as efficiently as we need to.

How do we overcome that? I believe including us in the processes, asking us our thoughts. We made the commitment a few weeks ago to Secretary Napolitano. She took time out of her day to come and meet with myself, Gary and a variety of other law enforcement officials, and we said to her, we are willing to commit our resources to come back here and do that.

Behind me sit two officers from my agency, one of which is assigned to the NCTC, part of the ITACG program. I tell you what, if I will commit someone to that, I commit another person to the NOC, I will definitely commit someone to working on these policies.

Mr. DENT. Commander.

Ms. MCNAMARA. I recently did a loan with Director Leiter at the National Counterterrorism Center. It was very enlightening for us, and it highlighted what we lack. Local law enforcement lacks the timely, consistent flow of information and intelligence that we could put on top of our SAR process for true situational awareness. We also lack the proper receptacles at local law enforcement and the processes. So we need improvement as well. So it is not just the Federal look, but it can be blended to do a better job in the future.

Mr. DENT. Yield back.

Ms. HARMAN. The gentleman yields back.

I would point out to our witnesses something that we say in many hearings. This committee views its role as representing you at the Federal level, not the other way around, representing the Federal level in the communities. We think your perspective that the way information is prepared and the way information moves is—for you is exactly right, and that is why we have made such an effort to include local law enforcement in the ITACG team process, which we insisted on, by the way. That is why we continue to think that the I&A function should be primarily led by people with your perspective.

The Chair now yields 5 minutes to Mr. Green of Texas.

Mr. GREEN. Thank you, Madam Chair. I thank you and the Ranking Member for this outstanding hearing. I am most appreciative that we have these witnesses who have provided us with information that I deem to be critical and exceedingly important.

I believe that our mission is to limit the use of our first responders by making greater use of our first preventers. I think that a number, a good number, of you talked about how first preventers

can prevent the use of first responders. I think it is important what has been said about educating first preventers and understanding who the first preventers are.

Chief, you reference the officer on the street, clearly a first preventer. But I would also add to a certain extent, with your consent and permission, because I would like to hear your response, the security officer who may be a licensed peace officer or who may not be, but who does have a watch, who may be at a hotel or on some apartment complex. I would add that we broaden that concept of first preventers such that we include literally anyone who has a watch, such that the person understands that he or she is a part of a homeland security network, and that intelligence acquisition is in his or her hands while he or she is on watch, and perhaps while you are off watch if something out of the ordinary should come within your purview.

So, Chief, if you would, tell me how broad do you think the definition of first preventers should be?

Chief GAISSERT. Congressman, I appreciate your observations. They are poignant, and I address this to some extent in the full written testimony, but this is one of the salient strengths of the Israeli model of homeland security, because they integrate the ability to obtain information from citizens, from private security companies, from civic groups, from anyone who has eyes and ears on the ground. So first preventers, in my view, would reasonably be the citizen on the street. If we can get them to understand that when they see things, it is like an old street cop: If it don't look right or it don't sound right, and he starts scratching into it or she starts looking into it a little bit, if it don't look right or it don't sound right, somebody needs to notify the appropriate authorities.

That doesn't mean to create some panic situation or to try to foster some sort of mentality of paranoia, but it does mean that we need to educate our first responders and the public in general on preattack indicators.

Mr. GREEN. Thank you, Chief.

Let me make one additional comment—I have about a minute and 10 seconds left—to Mr. Edwards. Sir, you indicated that, and I am paraphrasing, that you perceive yourself to be on paper, but off the radar, and I paraphrased it, but that was the essence of what I heard. I would like to give you an assurance, and I believe that this is what persons of goodwill would say, is that we want to make sure that you are not only on the radar, but you are part of the system that operates the radar, and that we make good use of the intelligence that you may be able to help us and provide to us. But for fear that I may not have heard you entirely correct, would you kindly give additional information as to the extent that you perceive yourself to need greater inclusivity?

Mr. EDWARDS. Your statement was exactly accurate, and I thank you for that, sir. I thank the committee for being concerned here. I think that is exactly right. It is just like everyone here today; whenever you talk about law enforcement or partners or communications, you are talking about State and local. When you talk about the head of DHS or I&A, you are talking about State, local sheriffs, no mention of Tribal. If you look at the legislation, we have done a good job of getting Tribal in there. Everywhere it says

Federal, State, and local, we have got Tribal in there. But it is in there, but it is not really happening out in the field.

To give you a prime example of that, with regard to a survey that was just sent out by the ITACG and we just got back regarding fusion centers and regarding the packages of information that they are sending down, the intelligence down to the field, they contacted 480 outlets. Of that 480 that responded, only 3 were Tribal. Two represented Tribal fire departments from California and one Tribal law enforcement from Alabama. So consequently, that is a prime indicator that we are not included.

Eighty percent of the Navajo reservation, larger than the State of West Virginia and several Northeastern States, has 80 percent inability to communicate via radios or cell phones on that vast reservation. A lot of people out there, their primary first language is not English. Native Americans in dealing with Native American communities are unique, and they must be dealt with uniquely because of the cultural differences and the isolation that has been placed on our people in dealing with things for hundreds of years. But we are open to work and help. We have had one hand tied behind us because we are a small population, and in many places like the Navajo Reservation, we have parts of the reservation in four separate States. It almost makes it impossible to meet the requirements to be able to get Homeland Security funding through the State.

But yet with that arm tied behind our back, we are still fighting, and we are fighting for this country and the citizens of this country, and we need your help to make sure we are included.

Ms. HARMAN. Thank you, Mr. Edwards, and thank you, Mr. Green. I let the time run over because I thought it was very important for that statement to be on the record. I also want to suggest, if it has not happened yet, that a Tribal person be one of the local people included in the ITACG in the near future. I think your perspective is very valuable.

A final set of questions comes from Mr. Broun of Georgia.

Mr. BROUN. Thank you, Chair Harman.

We know that information sharing is a vital part of preventing the next terrorist attack. I, as well as, I am sure, you, have gathered from what Chair Harman has stated and my dear friend Mr. Green has stated that we consider you guys to be right on the front line of that information-gathering process as well as sharing that information.

The Department of Homeland Security has the responsibility to receive the information from and to provide information to the State and local law enforcement. I know that everyone on this subcommittee wants to ensure that the information that you receive from the Department is useful at your level, the local level, as well as the State level.

Chief Gaissert, could you elaborate on the specific challenges that rural law enforcement agencies and officials face with regard to dealing with terroristic threats in more rural areas? Specifically are you getting enough information to deal with the threats in your specific jurisdiction?

Chief GAISSERT. Congressman, we have special challenges in rural and semirural areas of this Nation. Primarily among them

would be manpower and boat, the equipment and type of particularly tactical training that would be necessary to meet that type of threat, certainly if we were engaged in some sort of Mumbai attack.

In my view, training would be one of the most critical components, and it is an area where we do need more support. I think that you would find in most jurisdictions, such as ours in Jackson County, Georgia, that the average police officer does not receive much in the way of counterterrorism training outside of the 4 hours in basic mandate, which is in basic academy training. Once that is completed, unless they seek out on their own or their agency will support that process, there is little in the way of additional training. That is not to say that we don't have very well-trained tactical teams and a specialized or special operations unit. I was a street cop, and my heart is with that street officer, and I think that is probably one of the greatest opportunities we have to deter and to interdict terrorist attacks.

We are facing a very determined enemy. Take a moment in December 1978, the 40th Soviet Army rolled into Afghanistan. By 1985 they had approximately 130,000 troops in theater. They left in 1988 with 26,000 casualties. Now, these were not Boy Scouts; these were combat veterans, and they had reasonably good equipment. Albeit we were providing sport to the mujahideen; however, once that action was over, an American journalist interviewed a Taliban leader and asked him this question. He said, how is it that you were able to fight the Russian Army to a stump on horseback? The response was this, and I quote. He said, "We intended to fight to the last man, and they didn't."

General Sun Tzu said in the 6th century you have to become your enemy. You have to understand him and his epistemology through his eyes. So I think we have a real opportunity and duty to educate particularly down to the street officer level exactly the nature and character of the enemy, as well as to provide him with the tools necessary to meet that challenge should it occur.

Mr. BROUN. Well, thank you. I have got a whole bunch of questions I am sure we are going to submit to you guys.

I as well as, I think, everybody on this committee are very concerned about homegrown terrorists. So I would just like to add that I am going to ask you all a question, each of you, about preventing homegrown terrorism and how to interdict that type of threat in this Nation. So I would like to get your ideas in writing. So I look forward to your answers on that, and, Madam Chair, I yield back.

Ms. HARMAN. Thank you, Mr. Broun. I assume it is fine with the witnesses to respond in writing to that very important question. Great.

This panel has been excellent. All of you have contributed important information to the record of this committee. I would love to go a second round, but we have a second panel. If it is possible for you to remain here, that would be good, because you will hear some thoughtful testimony, I promise you it is very thoughtful, on some issues that are involved in getting homeland security intelligence right. So please stick around if you can. Certainly our committee Members will stick around.

It will take about a minute for the clerk to change the witness table, so we will suspend for a minute or two. Thank you.

Second panel are all set up? Very efficient. I want to commend the clerk and welcome the second panel of witnesses.

Our first witness is not new to this committee and certainly not new to me, Caroline Fredrickson, who is the Director of the Washington Legislative Office of the ACLU. She is that organization's top lobbyist and supervises a nearly 60-person team in promoting ACLU priorities in Congress.

Ms. Fredrickson has years of experience as a senior staffer on Capitol Hill, having previously served as Chief of Staff to Senator Maria Cantwell and as Deputy Chief of Staff to then-Senate Minority Leader Tom Daschle. In 1998 and 1999, she was a Special Assistant to the President for Legislative Affairs, a position that required her to work closely with both parties in the Senate to forge bipartisan agreements on the White House's legislative priorities. She is a Columbia University Law School graduate and was a Harlan Fiske scholar.

Our second witness, Greg Nojeim, again is not new to me and not new to the projects of this committee. He is the Director of the Project on Freedom, Security & Technology at the Center for Democracy & Technology.

Mr. Nojeim has substantial experience on the application of the Foreign Intelligence Surveillance Act and on the civil liberties protection it affords. His expertise also includes governmental data mining, the PATRIOT Act, the state secrets privilege, and the privacy implications of aviation security measures.

Mr. Nojeim previously worked at the Washington Legislative Office at the ACLU, a little incestuous here, for 12 years. He has frequently testified before Congress about antiterrorism and aviation security legislation counterterrorism proposals, the use of secret evidence in immigration proceedings, driver's license privacy, aviation security profiling, and the intrusive body scan technologies, and finally the threat to civil liberties that might be caused by national ID cards.

Our third witness, Kate Martin, is the Director of the Center for National Security Studies, another old buddy. That is a nonprofit human rights and civil liberties organization. She previously served as litigation director for the center when it was a joint project of the ACLU and the Fund for Peace.

From 1993 to 1999, Ms. Martin was also codirector of a project on security services in a constitutional democracy in 12 former Communist countries in Europe. She has taught strategic intelligence and public policy at Georgetown Law School and also served as general counsel to the National Security Archive, a research library located at the George Washington University.

Ms. Martin has litigated causes involving the entire range of national security and civil liberties issues, including serving as lead counsel in a lawsuit brought by more than 20 organizations challenging the secret arrest of 1,200 people in the wake of September 11.

As you all know, your written testimony will be printed in the record in full. I am now asking that each of you summarize your

written testimony in 5 minutes. We will start with Ms. Fredrickson.

STATEMENT OF CAROLINE FREDRICKSON, DIRECTOR, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION

Ms. FREDRICKSON. Good morning, Chair Harman, Ranking Member McCaul, and my dear friends and colleagues on the panel. Thank you very much for the opportunity to testify on behalf of the American Civil Liberties Union.

The ACLU testified before the full Homeland Security Committee in 2007 to express our concerns about the Department's use of spy satellites through its National Applications Office. We would like to thank Chairman Thompson and Chair Harman for their leadership in challenging NA's funding unless and until a proper legal framework can be established to protect the privacy of Americans.

Recent news that DHS is using Predator drones for surveillance on our northern border raises similar concerns, as do warrantless laptop and cell phone searches and other data seizures at the U.S. border, and we look forward to working with you to address these concerns.

My written testimony explores both practical and theoretical problems with the concept of homeland security intelligence, but in my time today I will focus on known abuses.

By their nature, all domestic intelligence operations pose a threat to civil liberties and democratic processes. Whenever the Government is involved in gathering information about Americans, absent a reasonable suspicion of criminal activity, there is a substantial risk of chilling lawful dissent and associations.

As the Supreme Court observed in the Keith case, history abundantly documents the tendency of Government, however benevolent and benign its motives, to view with suspicion those who most fervently dispute its policies.

Let me highlight a few recent incidents that suggest DHS is ignoring this history in its zeal to establish an intelligence role and improperly monitoring peaceful advocacy groups and religious and racial minorities. Last month a Texas fusion center supported by DHS released an intelligence bulletin that described a purported conspiracy between Muslim civil rights organizations' lobbying groups, the antiwar movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip-hop bands to spread sharia law in United States.

The bulletin, which reportedly is sent to over 100 different agencies, would be laughable, except that it comes with the imprimatur of a federally backed intelligence operation, and it directs law enforcement officers to monitor the activities of these groups in their areas.

We don't know whether anyone launched surveillance of hip-hop artists based on this report, but if they did, it would be far from the first such silly and unjustified investigation in our history.

The ACLU of Maryland recently uncovered a Maryland State Police intelligence operation that targeted 53 nonviolent political activists, including peace activists, Quakers, and death penalty opponents, based solely on the exercise of their first amendment rights.

We now know that DHS was involved in collecting and disseminating the e-mails of one of the peace groups subjected to the Maryland spying operation. This is alarming, particularly because DHS representatives had previously denied to Members of Congress that DHS had any information on the matter. A DHS spokesman later told the Washington Post that law enforcement agencies exchange information regarding planned demonstrations, "every day."

A March 2006 protective intelligence bulletin issued by the Federal Protective Service listed several advocacy groups that were targets of the Maryland operation. It contains a, "civil activist and extremist action calendar," that details dozens of demonstrations planned around the country, mostly peace rallies. There is no indication anywhere in the document to suggest that illegal activity might occur at any of these demonstrations. The Federal Protective Service apparently gleans this information from the Internet, but it is not clear under what authority DHS officials are monitoring the Internet to document and report on the activities of, "civil activists."

What is clear is that the Maryland police and DHS spying operations targeting peaceful activists serve no legitimate law enforcement, intelligence, or homeland security purpose. They were a threat to free expression, and they were a waste of time and money.

Another intelligence report produced for DHS by a private contractor smears environmental organizations like the Sierra Club, the Humane Society, the Audubon Society as, "mainstream organizations with known or possible links to ecoterrorism."

Spying on the innocent does not protect security. Domestic intelligence operations are dangerous to our freedom unless they are narrowly focused on real threats, tightly regulated, and closely monitored.

We look forward to working with this subcommittee to examine DHS's involvement in monitoring peaceful advocacy organizations and to construct checks and balances that will prevent abuses.

[The statement of Ms. Fredrickson follows:]

PREPARED STATEMENT OF CAROLINE FREDRICKSON

MARCH 18, 2009

Good morning Chair Harman, Ranking Member McCaul, and Members of the subcommittee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union, its hundreds of thousands of members and 53 affiliates Nationwide, regarding the intelligence activities of the Department of Homeland Security (DHS). As you know, the ACLU testified before the full Homeland Security Committee in 2007 to express our concerns about the Department's domestic use of spy satellites through its National Applications Office (NAO).[1] We know this committee shares our unease with this program and we would like to thank Chairman Thompson and Chair Harman for their leadership in challenging the NAO's funding unless and until a proper legal framework can be established to protect the privacy of ordi-

[1] *Turning Spy Satellites on the Homeland: the Privacy and Civil Liberties Implications of the National Applications Office: Hearing before the H. Comm. on Homeland Security,* 110th Cong. (Sept. 6, 2007) (statement of Barry Steinhardt, Director, Technology and Liberty Program, American Civil Liberties Union), available at *http://www.aclu.org/images/asset_upload_file278_31829.pdf.*

nary Americans.[2] Recent news that DHS is using Predator drones for surveillance on our northern border raises similar concerns,[3] as do warrantless laptop and cell phone searches and other data seizures at the U.S. border. We look forward to working with you to address these matters.

But rather than focus on particular programs I would like to ask more fundamental questions about the role of intelligence in homeland security, and particularly within DHS. As explained below, problems inherent in the way the intelligence community produces "intelligence" limit its reliability, rendering its value in improving security suspect. In addition, "homeland security" is a relatively new and exceptionally broad concept that combines protecting against traditional threats from hostile nations, terrorists, and other criminal groups with preparing to respond to outbreaks of infectious disease, natural disasters, and industrial accidents. While these are all important missions, taking such an unfocused "all crimes, all hazards"[4] approach to intelligence collection poses significant risks to our individual liberties, our democratic principles and, ironically, even our security. Frederick the Great warned that those who seek to defend everything defend nothing. Especially at a point in history when the troubled economy is regarded as the most significant threat to national security, we must ensure that all of our security resources are used wisely and focused on real threats.[5] Unfortunately, U.S. intelligence activities have too often targeted political dissent as a threat to security, which has led to misguided investigations that violated rights, chilled free expression, and wasted the time and resources of our security agencies. Recent events indicate that in its zeal to fulfill its broad mandate and establish an intelligence capability, DHS is repeating these mistakes. If DHS is to have a meaningful intelligence role that actually enhances security, it must assess the information it produces accurately, identify an intelligence need to be served, and evaluate whether it can fill this need without violating the privacy and civil rights of innocent Americans. Congress should evaluate these programs regularly and withhold funding from any activities that are unnecessary, ineffective, or prone to abuse.

I. THE RELEVANCE OF INTELLIGENCE IN HOMELAND SECURITY

The immediate obstacle to determining the relevance of intelligence in homeland security is the lack of a commonly understood definition of "intelligence."[6] People often hear the word and assume that this type of information has some magical quality giving it heightened importance and meaning. But by its very nature, intelligence is often uncorroborated, inadequately vetted, and fragmentary at best, and unreliable, misleading, or just plain wrong at worst. This deficiency is due to the secretive manner in which intelligence agencies gather, analyze, use and report information. By allowing people to report information against their neighbors or colleagues in secret, the social mores and legal consequences that normally restrain people from making false or misleading accusations are removed. By masking the sources and methods used to obtain this information, "intelligence" is stripped of the most essential clues for determining its value. Knowing whether an accusation that a politician is misusing campaign funds is coming from a trusted insider, a political opponent or an unemployed cab driver makes all the difference in determining its credibility. By then compartmentalizing this information and limiting its distribution, outside experts are prevented from effectively evaluating or challenging the finished "intelligence." And finally, by keeping contradictory pieces of intelligence and dissenting opinions secret, policymakers can too easily ignore information or ad-

---

[2] See Letter from Rep. Bennie G. Thompson, Chairman, Committee on Homeland Security, U.S. House of Representatives, Rep. Jane Harman, Chair, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives, and Rep. Christopher P. Carney, Chairman, Subcommittee on Management, Investigations, and Oversight, Committee on Homeland Security, U.S. House of Representatives, to Michael Chertoff, Department of Homeland Security and Charles Allen, Office of Intelligence and Analysis, Department of Homeland Security (Apr. 7, 2008) (on file with authors), available at *http://www.gwu.edu/nsarchiv/NSAEBB/NSAEBB229/44c.pdf.*

[3] *Drone to Patrol Border Between Manitoba and North Dakota,* The Canadian Press, Feb. 16, 2009, *http://cnews.canoe.ca/CNEWS/World/2009/02/16/8412951-cp.html.*

[4] Todd Masse, Siobhan O'Neil & John Rollins, Congressional Research Service, CRS Report for Congress: Fusion Centers: Issues and Options for Congress 22 (July 6, 2007), available at *http://www.fas.org/sgp/crs/intel/RL34070.pdf.*

[5] *Current and Projected National Security Threats to the United States: Hearing before the S. Select Comm. on Intelligence,* 111th Cong. (Feb. 12, 2009) (statement of Admiral Dennis C. Blair, Director of National Intelligence), *http://www.dni.gov/testimonies/20090212_testimony.pdf.*

[6] See, Mark A. Randol, Congressional Research Service, CRS Report for Congress: Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches 2 (Jan. 14, 2009), available at *http://fas.org/sgp/crs/intel/RL33616.pdf* ("At the broadest level, there is a plethora of definitions for intelligence.").

vice that might weigh against the policies or activities they choose to pursue. None of these processes necessarily make the final product false; they simply reduce the probability that it is reliable. If we called this material "unsubstantiated allegations," "rumor," "speculation," or "educated guesses" we would understand its value, but when we call it "intelligence" it takes on a significance it does not necessarily deserve.

Mark Randol of the Congressional Research Service argues that "raw" information does not become intelligence "until its sources have been evaluated, the information is combined or corroborated by other sources, and analytical and due diligence methodologies are applied to ascertain the information's value."[7] But this asks too much of a closed analytical process. Investigations into the intelligence failures regarding the presence of weapons of mass destruction in Iraq prior to the U.S. invasion, for example, find no shortage of attempts to validate the separate pieces of information.[8] This information was subjected to all the processes Randol describes, but in the end the "finished" intelligence was wrong. As the Senate Intelligence Committee Phase II report concluded, "[i]t is entirely possible for an analyst to perform meticulous and skillful analysis and be completely wrong."[9] In the end, the intelligence community chose to rely on an untrustworthy source named "Curveball" despite ample warnings that he was a fabricator,[10] and policymakers failed to heed dissenting opinions about whether aluminum tubes Iraq purchased were designed for use in a nuclear centrifuge.[11] These failures in pre-war intelligence were not because of a lack of process, rather because of what the process lacked.

Our legal system provides a contrasting method for determining the reliability of information. Centuries of jurisprudence have distilled rules of evidence and procedure that are specifically designed to provide the analytical due diligence Randol says is necessary for converting information into intelligence, though in the legal system this information is called "evidence." Evidence is "something (as testimony, writings, or objects) presented at a judicial or administrative proceeding for the purpose of establishing the truth or falsity of an alleged matter of fact" (emphasis added).[12] The rules of evidence are not arbitrary obstacles for lawyers to navigate; they represent time-tested methods for discerning truth. In order to be admitted into evidence documents must be authenticated by the individual or organization that produced them. Witnesses are examined in public and under oath. Information known to be obtained through unreliable means, such as coerced confessions, is not admissible. And once entered, evidence is challenged in an adversarial process, before a neutral arbiter and a jury of ordinary citizens serving as the ultimate fact-finders. Finally, this process is conducted in public, so that the justice system and those who work within it are accountable to the people they serve. A closed intelligence process simply cannot match this rigorous testing, and the reliability of the information it produces suffers as a result.

The one thing that is certain about "intelligence," is that it is only valuable to our security when it is true. Faulty intelligence is worse than no intelligence at all because it compels policymakers to take actions that may not have been necessary or to fail to take actions that were. And errors in intelligence are often compounded because security resources are finite. Increasing the assets directed at one threat invariably means reducing efforts devoted to another. For example, the New York Times reported that FBI officials began noticing a surge of mortgage frauds in 2003 and 2004 but their requests for additional resources to address financial crimes were denied by a Justice Department focused on counterterrorism.[13] Yet Director of National Intelligence Dennis Blair now identifies the global economic crisis as the

---

[7] Mark A. Randol, Congressional Research Service, CRS Report for Congress: Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches 2 (Jan. 14, 2009), available at *http://fas.org/sgp/crs/intel/RL33616.pdf.*

[8] See, S. Rep. No. 108–301(2004), available at *http://www.gpoaccess.gov/serialset/creports/iraq.html;* S. Rep. NO. 109–331 (2006), available at *http://intelligence.senate.gov/phaseiiaccuracy.pdf* (Phase II Report).

[9] S. Rep. No. 109–331, at 6 (2006), available at *http://intelligence.senate.gov/phaseiiaccuracy.pdf* (Phase II Report).

[10] Bob Drogan and Greg Miller, *Curveball Debacle Reignites CIA Feud,* L.A. Times, Apr. 2, 2005, available at *http://articles.latimes.com/2005/apr/02/nation/na-intel2.*

[11] David Barstow, William J. Broad, and Jeff Gerth, *How the White House Embraced Disputed Arms Intelligence,* N.Y. Times, Oct. 3, 2004, available at: *http://www.nytimes.com/2004/10/03/international/middleeast/03tube.html.*

[12] Miriam-Webster's Dictionary of Law 171–72 (1996).

[13] Eric Lichtblau, David Johnston, and Ron Nixon, *FBI Struggles to Handle Financial Fraud Cases,* N.Y. TIMES, Oct. 18, 2008, available at *http://www.nytimes.com/2008/10/19/washington/19fbi.html?pagewanted=1&__r=1&dbk.*

"primary near-term security concern of the United States."[14] Intelligence programs that focus on the last crisis to the detriment of anticipating the next crisis do not provide real security.

All of the problems of unreliability of intelligence are compounded with a new system of collection, and the negative impacts are many times greater when the ears and eyes are not pointed outward but inward to the United States. When intelligence subjects are not foreign nations or their military and intelligence operatives, but citizens, lawful permanent residents, and visa holders of our country, the checks and balances must be significantly enhanced over the minimal supervision given other parts of the intelligence apparatus. Therefore, Congress must be especially mindful of the limits of intelligence as it evaluates DHS intelligence programs. Congress should demand empirical evidence that these programs actually enhance security before funding them, particularly where they impact the rights and privacy of innocent Americans. So many of the broad information collection programs the intelligence community instituted over the last 8 years were premised on the idea that data mining tools could later be developed to find meaning in these vast pools of data collected,[15] but a recent study funded by DHS found that such programs were likely a wasted effort:

"Automated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts. One reason is that collecting and examining information to inhibit terrorists inevitably conflicts with efforts to protect individual privacy. And when privacy is breached, the damage is real. The degree to which privacy is compromised is fundamentally related to the sciences of database technology and statistics as well as to policy and process."[16]

Congress cannot afford to allow DHS, or any other intelligence agency, to continue investing in unproven technologies that harm privacy but provide no real security benefit.

II. THE LIMITATIONS OF HOMELAND SECURITY INTELLIGENCE

Intelligence has traditionally been divided into two spheres, foreign and domestic, which operate under different legal regimes. "Foreign intelligence," which is directed at foreign powers and their agents and is conducted primarily outside the United States, has less restrictive regulations and oversight, while "domestic intelligence," directed primarily at U.S. persons and conducted inside the United States is generally more regulated. Randol suggests that the advantage of "homeland security intelligence" as a discipline distinct from foreign or domestic intelligence is that it allows a holistic approach that is free from constraints of geography, level of government, or mutual mistrust between the public and private sectors.[17]

The danger with this approach is that the constraints are often specifically designed, or at least operate in practice, to protect the privacy and civil rights of U.S. persons. Blending the two disciplines necessarily leads to a dilution of privacy protections for U.S. persons as less restrictive methods of gathering foreign intelligence are increasingly used against U.S. persons. For instance, more than half of the roughly 50,000 National Security Letters the FBI issues each year, which were originally designed for use only against agents of foreign powers, now target U.S. persons.[18] Moreover, the compelling mission to protect the homeland would likely drive routine overrides of minimization procedures restricting the dissemination of

---

[14] *Current and Projected National Security Threats to the United States: Hearing before the S. Select Comm. on Intelligence,* 111th Cong. 2 (Feb. 12, 2009) (statement of Admiral Dennis C. Blair, Director of National Intelligence), *http://www.dni.gov/testimonies/20090212_testimony.pdf.*

[15] Jeffrey W. Seifert, Congressional Research Service, CRS Report for Congress: Data Mining and Homeland Security: An Overview (Jan. 18, 2007), available at *http://www.fas.org/sgp/crs/intel/RL31798.pdf.*

[16] National Research Council, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessments, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals (Oct. 2007), available at *http://www.nap.edu/catalog.php?record_id=12452.*

[17] Mark A. Randol, Congressional Research Service, CRS Report for Congress: Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches 13 (Jan. 14, 2009), available at *http://fas.org/sgp/crs/intel/RL33616.pdf.*

[18] U.S. Department of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (Mar. 2007), available at *http://www.usdoj.gov/oig/special/s0703b/final.pdf.*

U.S. person information collected under a foreign intelligence rubric,[19] particularly as intelligence agents take the "better safe than sorry" approach that led to excessive number of nominations to the terrorist watch lists.[20]

More significantly, while DHS will undoubtedly require access to foreign intelligence collected by the other intelligence agencies to fulfill its mission, its focus on protecting the "homeland" will drive a primarily domestic intelligence program. The DHS intelligence mission statement, "to provide homeland security intelligence and information to the Secretary, other Federal officials, and our state, local, tribal and private sector partners," suggests a domestic focus.[21] And the DHS intelligence components, the U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Transportation Security Administration, will disproportionately gather U.S. person information in the course of fulfilling their mission responsibilities.

By their nature, all domestic intelligence operations pose a threat to civil liberties and democratic processes. Whenever the Government is involved in gathering information about Americans without a reasonable suspicion of criminal activity, there is substantial risk of chilling lawful dissent and association. As the Supreme Court observed in *United States* v. *United States District Court (Keith),* "[h]istory abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies."[22]

Evidence of Abuse

Several recent incidents seem to indicate DHS is ignoring this history in its zeal to establish an intelligence role, and improperly monitoring peaceful advocacy groups and religious and racial minorities. Charles Allen, DHS Under Secretary for Intelligence and Analysis, said one of the analytic elements his office assesses is the threat of radicalization and extremism. The ACLU is concerned that these terms are ill-defined and seem to suggest a connection between terrorism and advocacy against Government policies. Under Secretary Allen stated categorically in recent testimony that DHS does not monitor known extremists and their activities, but documents obtained by the ACLU suggest otherwise.[23]

The ACLU of Maryland recently uncovered a Maryland State Police (MSP) intelligence operation that targeted 23 non-violent political advocacy organizations based solely on the exercise of their First Amendment rights.[24] MSP spying activities were aimed at peace advocates like the American Friends Service Committee (a Quaker organization) and Women in Black (a group of women who dress in black and stand in silent vigil against war), immigrants rights groups like CASA of Maryland, human rights groups like Amnesty International, anti-death penalty advocates like the Maryland Citizens Against State Executions, and gay rights groups like Equality Maryland, among others. Many of the members of these organizations were referenced as terrorists in a Federal database.

The revelation that DHS was involved in collecting and disseminating the e-mails of one of the peace groups subjected to the MSP spying operation is alarming,[25] particularly because DHS representatives had previously denied that DHS had any information regarding the MSP investigations targeting these protesters.[26] In a letter to U.S. Senators Benjamin Cardin, Barbara Mikulski and Russ Feingold, DHS said it had done an "exhaustive" search of its databases and could find no information

---

[19] See, *National Security Agency, Report to Congress: Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (Feb. 2000), available at *http://www.fas.org/irp/nsa/standards.html* ("The overarching standard as implemented in both E.O. 12333 and FISA minimization procedures is that to disseminate personally identifiable information concerning a U.S. person, the information must be found necessary to understand a particular piece of foreign intelligence or assess its importance").

[20] Department of Justice, *Office of Inspector General Review of the Terrorist Screening Center* viii (June 2005), available at *http://www.fas.org/irp/agency/doj/oig/tsc.pdf.*

[21] Department of Homeland Security, Office of Intelligence and Analysis web page, *http://www.dhs.gov/xabout/structure/gc__1220886590914.shtm* (last visited Mar. 11, 2009).

[22] *United States* v. *United States Dist. Court (Keith),* 407 U.S. 297, 313–314 (1972).

[23] *Homeland Security Intelligence at a Crossroads: The Office of Intelligence and Analysis' Vision for 2008: Hearing before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security,* 110th Cong. 4 (Feb. 26, 2008) (Statement of Charles E. Allen, Under Secretary for Intelligence and Analysis, Department of Homeland Security), available at *http://homeland.house.gov/SiteDocuments/20080226165154-47048.pdf.*

[24] See, ACLU of Maryland "Stop Spying" info page, *http://www.aclu-md.org/Index%20content/NoSpying/NoSpying.html* (last visited Mar. 11, 2009).

[25] Lisa Rein, *Federal Agency Aided Md. Spying,* Washington Post, Feb. 17, 2009, at: *http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html.*

[26] Letter from Jim Howe, Acting Assistant Secretary, U.S. Department of Homeland Security, to Senator Benjamin L. Cardin, (Jan 29, 2009) (on file with author).

relating to the MSP surveillance operations. Yet MSP documents provided to the ACLU indicate that DHS Atlanta provided MSP with information regarding its investigation of the DC Anti-war Network (DAWN). An entry in the MSP files dated June 21, 2005 says:

"The US Department of Homeland Security, Atlanta, recently forwarded two emails from [REDACTED] an affiliate of the DC DAWN Network and the [REDACTED]. Activists from DAWN, [REDACTED] and other groups working under the banner of [REDACTED] are going to stage several small (12–15) weekly demonstrations at the Silver Spring Armed Forces Recruitment Center (AFRC). If there is enough support these will become weekly vigils."[27]

Not only was DHS apparently aware of the MSP investigation, it was actually monitoring the communications of DAWN affiliates and forwarding them to MSP. We want to know how and why DHS obtained these e-mails (which contained no reference to any illegal activity), why DHS disseminated them to the MSP, and why DHS could not find records documenting this activity in the DHS databases.

Contrary to what DHS told the senators, a DHS spokesman quoted in the Washington Post said that law enforcement agencies exchange information regarding planned demonstrations "every day."[28] Indeed, a March 2006 "Protective Intelligence Bulletin" issued by the Federal Protective Service (FPS) lists several advocacy groups that were targets of the MSP operations, including Code Pink, Iraq Pledge of Resistance and DAWN, and contains a "civil activists and extremists action calendar" that details dozens of demonstrations planned around the country, mostly peace rallies. FPS apparently gleans this information from the Internet. However, it is still not clear under what authority DHS officials monitor the Internet to document and report on the activities of "civil activists", since there is no indication anywhere in the document to suggest illegal activity might occur at any of these demonstrations. What is clear is that MSP and DHS spying operations targeting peaceful activists serve no legitimate law enforcement, intelligence, or homeland security purpose. The operations threatened free expression and association rights, and they were a waste of time.

This bulletin is not the only indication of abuse in DHS intelligence operations. Another intelligence report produced for DHS by a private contractor smears environmental organizations like the Sierra Club, the Humane Society, and the Audubon Society as "mainstream organizations with known or possible links to eco-terrorism."[29] Slandering upstanding and respectable organizations does not just violate the rights of these groups and those who associate with them; it undermines the credibility of all intelligence produced by and for DHS. There is simply no value in using limited DHS resources to generate such intelligence products—and yet these events continue to occur.

Last month a Texas fusion center supported by DHS released an intelligence bulletin that described a purported conspiracy between Muslim civil rights organizations, lobbying groups, the anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip-hop bands to spread Sharia law in the U.S.[30] The bulletin, which reportedly is sent to over 100 different agencies, would be laughable except that it comes with the imprimatur of a federally backed intelligence operation, and it directs law enforcement officers to monitor the activities of these groups in their areas. The ACLU has long warned that these State, local, and regional intelligence fusion centers lacked proper oversight and accountability and we hope the discovery of this shockingly inappropriate report leads to much needed examination and reform. In December 2008 the DHS Privacy Office issued a Privacy Impact Assessment of fusion centers that echoed the ACLU's concerns re-

---

[27] Maryland State Police Intelligence File on the D.C. Anti-War Network (DAWN), p. 13, (2005) (on file with the ACLU). This document was released pursuant to the Maryland's Public Information Act. See Public Information Act, Md. Code Ann., State Gov't § 10–630 (West 2008).

[28] Lisa Rein, *Federal Agency Aided Md. Spying,* Wash. Post, Feb. 17, 2009, at B01, available at *http://www.washingtonpost.com/wp-dyn/content/article/2009/02/16/AR2009021601131.html.*

[29] Universal Adversary Dynamic Threat Assessment, Eco-Terrorism: Environmental and Animal Rights Militants in the United States, (May 7, 2008), available at *http://wikileaks.org/leak/dhs-ecoterrorism-in-us-2008.pdf.*

[30] North Central Texas Fusion System Prevention Awareness Bulletin, (Feb. 19, 2009), available at *http://www.baumbach.org/fusion/PAB__19Feb09.doc.* For a discussion of DHS support of the North Central Texas Fusion Center, See U.S. Department of Homeland Security, Office of Inspector General, DHS's Role in State and Local Fusion Centers is Evolving (Dec. 2008), available at *http://www.fas.org/irp/agency/dhs/ig-fusion.pdf*; General Accountability Office, Homeland Security: Federal Efforts Are Helping To Alleviate Some Challenges Encountered by State and Local Information Fusion Centers (Oct. 2007), available at *http://www.gao.gov/new.items/d0835.pdf.*

garding the threat these rapidly expanding intelligence centers pose to the privacy of innocent Americans.[31]

Dilution of Effective Regulation

It isn't surprising that an intelligence operation with an overbroad "all hazards" mission and lax oversight would trample on individual privacy rights. The police power to investigate combined with the secrecy necessary to protect legitimate law enforcement operations provide ample opportunity for error and abuse, which is why in the 1970's the Federal Government sought to establish clear guidelines for State and local law enforcement agencies engaged in the collection of criminal intelligence information. Title 28, Part 23 of the Code of Federal Regulations was promulgated pursuant to 42 U.S.C. § 3789(g)(c) which requires State and local law enforcement agencies receiving Federal funding to

" . . . collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems further the purpose of this chapter and to assure that some systems are not utilized in violation of the privacy and constitutional rights of individuals."[32]

The regulation was part of a series of law enforcement reforms initiated to curb widespread abuses of police investigative authorities for political purposes, particularly by local police intelligence units or "red squads," which often amassed detailed dossiers on political officials and engaged in "disruptive" activities targeting political activists, labor unions, and civil rights advocates, among others. In commentary published during a 1993 revision of the regulation, the Department of Justice Office of Justice Programs (OJP) explained the risks to civil liberties inherent in the collection of criminal intelligence, and the need for regulation of criminal intelligence systems:

"Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential suspects of a criminal intelligence system."[33]

Part 23 is designed to ensure that police intelligence operations are properly focused on illegal behavior by requiring that criminal intelligence systems "collect information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." The "reasonable suspicion" standard is clear, well-defined, time-tested, and universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of law enforcement officers.

Unfortunately, there is a new theory of domestic intelligence that argues that collecting even outwardly innocuous behaviors will somehow enhance security. In 2006, former DHS Secretary Michael Chertoff said,

"Intelligence is about thousands and thousands of routine, everyday observations and activities. Surveillance, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, give us a sense of the patterns and flow that really is at the core of what intelligence is all about."[34]

---

[31] U.S. Department of Homeland Security Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative (Dec. 11, 2008), available at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_T3ia_slrfci.pdf.*

[32] 42 U.S.C.A. § 3789(g)(c) (WEST 2007). The provision instructing the Office of Justice Programs to prescribe regulations to assure that criminal intelligence systems are "not utilized in violation of the privacy and constitutional rights of individuals" was added when the Omnibus Crime Control and Safe Streets Act of 1968 was reauthorized and amended by the Justice System Improvement Act of 1979 (See, Justice System Improvement Act of 1979, Pub. L. No. 96–157, 1979 U.S.C.C.A.N. (96 Stat.) 1167, 1213, 2471–77, 2539).

[33] See Office of Justice Programs, *U.S. Department of Justice, Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operation Policies, 1993 Revision and Commentary,* 28 C.F.R. Part 23 (1993), at 4, *http://www.homeland.ca.gov/pdf/civil_liberties/1993RevisionCommentary_28CFRPart23.pdf.*

[34] Secretary of Homeland Security Michael Chertoff, Remarks at the 2006, Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing, Mar. 14, 2006, *http://www.dhs.gov/xnews/speeches/speech_0273.shtm.*

It is clear from this statement that Secretary Chertoff was relying on the extravagant promises of the now-debunked data mining technologies to make sense of the thousand routine observations that would be recorded each day. But suspicious activity reporting programs are moving forward nonetheless.

In January 2008 the Office of Director of National Intelligence (ODNI) Information Sharing Environment (ISE) Program Manager published functional standards for State and local law enforcement officers to report "suspicious" activities to fusion centers and the ISE.[35] The behaviors described as inherently suspicious included such innocuous activities as photography, acquisition of expertise, and eliciting information. We are already seeing the results of such a program as police increasingly stop, question, and even detain innocent Americans engaging in First Amendment-protected activity, to collect their personal information for later use by the intelligence community.[36] This type of information collection does not improve security; it merely clogs criminal intelligence and information sharing systems with irrelevant and useless data.

The ACLU and other privacy and civil liberties advocates are working with the ISE Program Manager, and with several State and local law enforcement agencies such as the Los Angeles Police Department, to modify these programs to avoid abrogation of First Amendment rights and the Part 23 reasonable suspicion standard. While these efforts show some progress in strengthening privacy guidelines for these programs, even the best internal controls have rarely proved sufficient to eliminate abuse in intelligence programs. This subcommittee should examine these programs closely, assess whether they demonstrably improve security and ensure that they operate in a manner that protects individual rights before authorizing DHS resources to support them.

III. THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY IN INTELLIGENCE

The Homeland Security Act of 2002 tasked DHS with the responsibility to manage programs for sharing law enforcement and intelligence information between the Federal Government and State, local, and tribal authorities.[37] Unfortunately, other Federal law enforcement and intelligence agencies, such as the FBI, already had well-established relationships and information-sharing arrangements with State and local law enforcement and resisted DHS efforts to manage these programs. In 2004, Congress established the ODNI Information Sharing Environment to address this on-going resistance to information sharing, but this only further complicated the question of DHS's intelligence role.[38]

As it stands now there are several mechanisms for State and local governments to engage with the Federal Government to share law enforcement information: the DHS Office of Intelligence and Analysis, the FBI Joint Terrorism Task Forces, the ODNI ISE, and the fusion centers. Likewise there are several different portals to receive information: Law Enforcement Online (LEO), the National Data Exchange (N–Dex), the National Law Enforcement Telecommunication System (NLETS), the FBI's Guardian and e-Guardian systems and the Homeland Secure Information Network (HSIN) to name just a few. With several different Federal agencies responsible for intelligence collection and analysis and several different mechanisms for sharing intelligence with State and local authorities, DHS intelligence operations risk being redundant or even superfluous.

The problem from a civil rights perspective is that the existence of competing intelligence programs creates the incentive for each agency to collect and report more information than the others to prove its value, to the detriment to the privacy and liberties of ordinary Americans. Intelligence offices are too often judged by the number of reports they disseminate rather than the value of the information in those reports, which is part of what drives the over-collection and over-reporting of innocuous information. In 2008, Under Secretary Allen boasted that I&A increased production of Homeland Intelligence Reports "from 2,000 to nearly 3,100" over the previous year but this statistic only represents an improvement if the information reported is correct, relevant, and unique.[39] Intelligence reports like those produced by

---

[35] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0, ISE–FS–200, (Jan. 25, 2008) (on file with authors).

[36] See, Mike German and Jay Stanley, American Civil Liberties Union, Fusion Center Report Update (July 2008), *http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf.*

[37] 6 U.S.C.A. § 101 et seq. (West 2006).

[38] See, Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C.A. § 401, et seq. (West 2006).

[39] *Homeland Security Intelligence at a Crossroads: The Office of Intelligence and Analysis' Vision for 2008: Hearing before the Subcomm. on Intelligence, Information Sharing, and Terrorism*

Continued

the North Central Texas Fusion Center provide nothing to enhance homeland security, and may actually undermine it by diverting attention from real threats.

DHS intelligence programs should not compete with other Federal programs. DHS should assess what State, local, and other Federal agencies need from DHS intelligence programs that they are not currently receiving from other sources. It is possible that there is no gap in intelligence, which would render DHS intelligence wholly unnecessary. If there is a gap, then DHS should evaluate the information produced by each of its intelligence components during the normal course of business to determine whether it can tailor this information to suit the specific intelligence needs identified. If DHS intelligence activities produce no demonstrably useful information, Congress should de-fund them. Where new types or sources of information need to be developed to fill intelligence gaps, DHS should carefully evaluate whether collection of this information is appropriate under the law, whether DHS is the agency best suited to collect this information, and whether the dissemination of such information can be accomplished without violating the privacy or civil rights of U.S. persons. Where DHS finds it can produce a necessary intelligence product, such programs should be narrowly tailored to fulfill that specific need and constantly reviewed to ensure conformance with all laws and policies. Finally, Congress should evaluate these programs regularly, and in public to the greatest extent possible. In the famous words of Supreme Court Justice Louis Brandeis, sunshine is the best disinfectant.

IV. CONCLUSION

Intelligence operations directed at Americans pose serious risks to liberty and democracy. First and foremost, we should not sacrifice our liberty for the illusion of security. Congress should not implement or fund new intelligence programs without empirical evidence that they effectively improve security. Intelligence programs like the CIA's Operation Chaos, the NSA's Shamrock, the FBI's COINTELPRO, and the red squads of local police departments are infamous not just because they violated the rights of innocent Americans and undermined democratic processes, but also because they were completely ineffective in enhancing national security in any meaningful way.[40] It turns out, not surprisingly, that spying on innocent people is not useful to uncovering true threats to security. Reforms instituted after the exposure of these abusive intelligence programs were designed not only to protect the rights of innocent Americans, but to help our law enforcement and intelligence agencies become more effective by focusing their resources on people they reasonably suspected of wrongdoing. Unfortunately these lessons of the past have too often been ignored, and we are increasingly seeing a return to abusive intelligence operations targeting protest groups and religious and racial minorities.

It would be an enormous mistake to ignore the lessons of past failure and abuse on a subject as critical as spying on the American people. We don't have to choose between security and liberty. In order to be effective, intelligence activities need to be narrowly focused on real threats, tightly regulated and closely monitored. We look forward to working with this subcommittee to examine DHS's involvement in monitoring peaceful advocacy organizations. As the Keith Court warned, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."[41]

Ms. HARMAN. Thank you, Ms. Fredrickson.

Mr. Nojeim, you are recognized for 5 minutes.

STATEMENT OF GREGORY T. NOJEIM, DIRECTOR, PROJECT ON FREEDOM, SECURITY & TECHNOLOGY, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. NOJEIM. Thank you, Chair Harman, Ranking Member McCaul and Members of the subcommittee. Thanks for the opportunity to testify this morning on behalf of CDT.

Risk Assessment of the H. Comm. on Homeland Security, 110th Cong. 4 (Feb. 26, 2008) (Statement of Charles E. Allen, Under Secretary for Intelligence and Analysis, Department of Homeland Security), available at *http://homeland.house.gov/SiteDocuments/20080226165154-47048.pdf*.

[40] Select Comm. To Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., Final Report on Supplemental Detailed Staff Reports on Intelligence Activities and The Rights of Americans (Book III), S. Rep. No. 94–755 (1976).

[41] *United States* v. *United States Dist. Court (Keith)*, 407 U.S. 297, 314 (1972).

Government agencies at the Federal, State, and local level have created a vast domestic intelligence apparatus. The goal is laudable: Connect the dots to prevent terrorism. But the risks to civil liberties are large. We have some ideas on how the subcommittee could mitigate those risks.

First we need to identify the problems. We see primarily two. The first, as Ms. Fredrickson pointed out, is the surveillance of protected first amendment activities. It is reminiscent of the spying that happened in the 1960's and 1970's. In one instance the Maryland State Police surveilled antiwar protesters and death penalty opponents for over a year. They found no evidence of crime and continued the surveillance. That is wrong.

The second problem is the increasing collection and sharing of information on primarily innocent activity through suspicious activity reporting. Conduct triggering only the thinnest of suspicions is being recorded and widely shared. Photographing bridges is described as suspicious activity, even though tourists do it all the time, and so do photography buffs.

These serious problems are exacerbated by digital technologies for the storage, retrieval, and dissemination of information. Nationwide sharing systems greatly magnify the risk that information will be taken out of context or misinterpreted, resulting in false inferences and unjustified adverse action.

The disparate guidelines that have been issued so far to govern these efforts fail to provide adequate guidance. They either permit intelligence collection without a predicate, or they provide generic unhelpful guidance like this from the Department of Homeland Security—I am sorry, from the Information Sharing Environment Privacy Guidelines: "All agencies shall, without exception, comply with the Constitution in all applicable laws and Executive Orders." Of course they should, but that is just not helpful advice.

While guidelines should be tailored to the entities that must follow them, there does not seem to be a set of principles that guides the overall intelligence effort and protects civil liberties. Remarkably there does not seem to be a set of intelligence guidelines at all for DHS itself.

The subcommittee could take a number of steps to better focus homeland security intelligence collection and sharing. First it should ensure that DHS entities follow principles of Fair Information Practices, or FIPs. FIPs establish a useful framework for using information to make fair decisions about people.

Second, the subcommittee should work to ensure that a criminal predicate is required where it is appropriate. It is probably the single most effective civil liberties protection that could be imposed on the collection and sharing of homeland security intelligence that includes personal information. Requiring a criminal predicate signals the person who gathers or shares the information that they need to focus on potential wrongdoers and not on everyone else.

Third, the subcommittee should sample intelligence products developed by DHS components and its partners. It should ascertain what is being collected, how it is used, and whether it is useful in preventing terrorism. It could test whether SARs reporting is effective and efficient in preventing terrorism and other crimes.

Finally, the subcommittee should review the training materials that DHS entities use. If they permit or invite inappropriate surveillance like that engaged by the Maryland State Police, they need to be changed. Oversight focused on adherence to privacy principles, compliance with strong privacy guidelines, and requiring criminal predication where appropriate would enhance both liberty and security.

Thank you very much.

Ms. HARMAN. Thank you, Mr. Nojeim.

[The statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM

MARCH 18, 2009

Chair Harman, Ranking Member McCaul, and Members of the subcommittee, thank you for the opportunity to testify this morning about homeland security intelligence on behalf of the Center for Democracy & Technology.*

INTRODUCTION AND SUMMARY

Without a definitive decision to do so, and on something of an ad hoc basis, government agencies at the Federal, State, and local level have created a vast domestic intelligence apparatus. Until recently, collection, analysis and dissemination efforts have been disjointed and uncoordinated, which may offer some comfort to civil libertarians. Now, a variety of efforts are underway to integrate the information that is being collected and to share it more widely. The goal, of course, is laudable: to collect and connect the dots that might reveal a terrorist scheme. However, there is no overall theme to this collection and sharing effort, no guiding principles. We continue to see homeland intelligence efforts that classify legitimate political activity as "terrorism" and that spy on peaceful activists; the revelations about the Maryland State Police are the latest example that has come to light. Also, there is a trend toward the collection of huge quantities of information with little or no predicate through "suspicious activity reports." There seems to us a high risk that this information will be misinterpreted and used to the detriment of innocent persons. Meanwhile, the security "bang per byte" of information gathered may be diminishing. While "stove piping" was yesterday's problem, tomorrow's problem may be "pipe clogging," as huge amounts of information are being gathered without apparent focus. All of this occurs in the context of a powerful digital revolution that makes it easier than ever to collect, store, exchange, and retrieve information in personally identifiable ways, making it available far removed from the context in which it was collected.

In our testimony today, we will consider what homeland security intelligence is and will identify some of the efforts being made to collect and share it. Then, we will turn to the risks to civil liberties posed by homeland security intelligence activities and offer some ideas on how they can be addressed.

WHAT IS HOMELAND SECURITY INTELLIGENCE AND WHAT RISKS DOES IT POSE?

So far, the term "homeland security intelligence" has not been officially defined.[1] "Homeland security information" is statutorily defined as any information that relates to the threat of terrorist activity and the ability to prevent it, as well as information that would improve the response to terrorist activity or the identification or investigation of a suspected terrorist or terrorist organization. Homeland Security Act of 2002, Pub. L. 107–296, Section 892(f)(1), 6 U.S.C. 482(f)(1). From what we can tell, the homeland security intelligence system is equally broad. The definition of homeland security information is as significant for what it does not say as for what it says: it does not distinguish between information collected abroad and infor-

*The Center for Democracy and Technology is a non-profit, public interest organization dedicated to keeping the Internet open, innovative, and free. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies, and associations interested in information privacy and security issues. CDT has offices in Washington, DC and in San Francisco, CA.

[1] CRS Report, Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches (August 18, 2006).

mation collected in the United States; it does not distinguish between information regarding foreign terrorist organizations and information regarding domestic terrorist groups; it does not distinguish among information collected under criminal investigative powers, information collected under the national security powers applicable to "foreign intelligence" or counterintelligence, and information collected under regulatory or administrative authorities or from open sources; it does not distinguish between information collected by Federal agencies and information collected by State, local, or tribal governments; and it does not distinguish between information collected with terrorism in mind and information collected for other purposes. It is broad enough to encompass all of these, and to some degree that is appropriate, since one of the reasons why the planning of the 9/11 attacks went undetected is that agencies observed various artificial distinctions that prevented information sharing and collaboration.

However, with such an all-encompassing definition, the cycle of collecting, sharing, and using homeland security information or homeland security intelligence clearly poses risks to constitutional values of privacy, free expression, free association, and democratic participation. The solution lies, we believe, not in a narrower definition, but in clear rules as to what can be collected and retained, under what standard and subject to what supervision, with whom it can be shared, and how it can be used. So far, this system of rules remains incomplete, while the creation of a broad homeland security intelligence system progresses apace.

In particular, this subcommittee should be concerned about two distinct problems: (1) The continuing, even if isolated, collection of information on First Amendment activities; and (2) the newly expanded efforts to collect, exchange, and use "suspicious activity reports" based on the thinnest of suspicions. Both issues involve the collection, retention, and dissemination of information collected without either the criminal predicate or the "agent of a foreign power" standard found in FISA.[2] Intelligence activities not tethered to the criminal predicate are dangerous to liberty because they can cast a wide net, may encompass First Amendment activities, and tend to be more secretive because the information collected is not likely to be subject to the after-the-fact scrutiny afforded by the criminal justice system. In both cases, the risks are exacerbated by the otherwise appropriate application of digital technologies for storage, retrieval, and dissemination. For example, although proponents of SARs argue that they are an extension of long-standing police practices, the power of information technology and the creation of Nation-wide sharing systems greatly magnify the risks that information will be taken out of context or misinterpreted, resulting in false inferences and unjustified adverse action.

In recommending serious application of the criminal predicate, we are not arguing against the need to prevent acts of terrorism before they occur. We are not seeking to force agencies with homeland security obligations to limit themselves to prosecuting past crimes. Furthermore, we fully recognize and support the integration, properly controlled, of domestic intelligence information with information collected overseas and information collected in the United States under the authorities of the Foreign Intelligence Surveillance Act and related laws. Instead, we are calling for adherence to a standard that focuses on the intentions, capabilities, and future actions of enterprises planning or otherwise involved in illegal activity. And we are calling for rules that take into account the ability of modern information technology to store and retrieve personally identifiable information on an unprecedented basis.

WHO COLLECTS HOMELAND SECURITY INTELLIGENCE INFORMATION?

As the subcommittee well knows, multiple agencies at the Federal level collect and analyze information that fits under the homeland security intelligence umbrella.

Within the Department of Homeland Security alone, there is a departmental Office of Intelligence and Analysis and there are intelligence activities within several of the Department's components as well, including the U.S. Citizenship and Immigration Service, the Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration.

Outside of the DHS, Federal agencies charged with collecting or analyzing information that could be considered homeland security intelligence include:

- The FBI, which conducts counterintelligence, counterterrorism and intelligence activities primarily, but not exclusively, within the United States.

---

[2] CDT has made recommendations for improving both the criminal investigative authorities and FISA in order to provide better privacy protection while still empowering the Government to collect the information it needs, but we focus today on the collection of information outside of either a criminal predicate or the FISA standards.

- The CIA, which collects foreign intelligence and conducts counterintelligence and counterterrorism activities related to national security primarily, but not exclusively, outside of the United States.
- The State Department's Bureau of Intelligence and Research.
- The Drug Enforcement Administration, which collects intelligence about organizations involved in growing and distributing controlled substances.
- The Department of Energy, which assesses nuclear terrorism threats.
- The Treasury Department, which collects information relating to the financing of terrorist organizations.
- Intelligence entities within the Department of Defense, including the Defense Intelligence Agency, the National Security Agency, and the National Reconnaissance Office (whose capabilities are available for domestic collection).

Outside of the Federal Government, State, local, and tribal police forces of varying sizes also engage in the collection of homeland security intelligence. The level of sophistication of these efforts varies widely. For example, the New York City Police Department has a sophisticated intelligence operation, which has grown and operates with little public oversight. Likewise, the Los Angeles Police Department has a very sophisticated intelligence gathering and integration program. Other cities, as well as tribal police forces, have much less sophisticated operations.

Some of the entities that engage in intelligence collection operate under guidelines. Indeed, there is no lack of guidelines on domestic intelligence. The guidelines in place include:

- The Attorney General's Guidelines for Domestic FBI Operations (September 29, 2008) *http://www.usdoj.gov/ag/readingroom/guidelines.pdf.*
- Department of Justice, Office of Justice Programs, Global Justice Information Sharing Initiative ("Global"), "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era—Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels—Law Enforcement Intelligence, Public Safety, and the Private Sector" (2006) *http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf.*
- Program Manager—Information Sharing Environment (PM–ISE), Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (2006) *http://www.ise.gov/docs/privacy/PrivacyGuidelines20061204.pdf.* See *http://www.ise.gov/pages/privacy-implementing.html* for related materials.
- PM–ISE, Nationwide Suspicious Activity Reporting Initiative—Concept of Operations (December 2008) *http://www.ise.gov/docs/sar/NSI_CONOPS_Version_1_FINAL_2008-12-11_r5.pdf.* For further information on governance of the SARs program, see *http://www.ise.gov/pages/sar-initiative.html.*
- Law Enforcement Intelligence Unit (LEIU), Criminal Intelligence File Guidelines (revised March 2002) *http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.*
- LAPD, Major Crimes Division Standards and Procedures (March 18, 2003) *http://www.lapdonline.org/search_results/content_basic_view/27435.*
- Memorandum of Agreement Between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center of Terrorism Information Contained within Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism (2008) *http://fas.org/sgp/othergov/intel/nctc-moa2008.pdf.*

Remarkably, there does not seem to be a set of intelligence guidelines for the Department of Homeland Security or for any of its intelligence-collecting components. However, the main problem we see is not the lack of guidelines per se, but the fact that the guidelines that have been issued so far fail to provide adequate guidance. They either permit intelligence collection without a predicate, as the Attorney General guidelines do,[3] or they provide generic, unhelpful guidance, stating that "all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders," as the ISE guidelines do. We appreciate that guidelines must be tailored to the nature and mission of the entity, the places where it conducts its operations (whether primarily within the United States or abroad), and the type of information it collects. However, there does not seem to be a set of principles that guides the overall intelligence effort and protects civil liberties. There are a lot

[3] CDT's analysis of the Attorney General Guidelines can be found here: *http://cdt.org/publications/policyposts/2008/16.*

of cooks in the homeland security intelligence kitchen, and they are each using different recipes.

WHO SHARES AND ANALYZES HOMELAND SECURITY INTELLIGENCE INFORMATION?

As the 9/11 Commission found, and numerous other reports have confirmed, better sharing of intelligence and criminal information is needed to uncover and head off terrorist plans. Just last week, the Markle Foundation Task Force on National Security in the Information Age called for a recommitment to information sharing:

"The President and Congress must reaffirm information sharing as a top priority, ensuring the policymakers have the best information to inform their decisions . . . If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place."[4]

A number of information-sharing structures have been established that could be effective in heading off terrorist attacks by sharing homeland security intelligence information. However, they have overlapping missions and insufficient guidance to protect civil liberties.

Information Sharing Environment.—The ISE, created by Congress and housed in the Office of the Director of National Intelligence, is a potentially revolutionary effort to create a means for sharing terrorism, law enforcement, and homeland security information across Federal agencies and among State, local, and tribal police forces. The types of information that will be exchanged are broadly defined, and tens of thousands of law enforcement and intelligence officials will have access to the information.

The ISE is scheduled to go operational this summer. However, the privacy guidance for the ISE is woefully inadequate. For example, the guidance calls for agencies to develop redress mechanisms to handle complaints about decisions made based on faulty information, but at the same time allows them to decide not to adopt redress mechanisms on the ground that they would be inconsistent with the agency's mission.[5]

National Counterterrorism Center.—The NCTC employs more than 500 people, drawn from 16 Federal departments and agencies to integrate and analyze counterterrorism intelligence, much of which fits under the homeland security intelligence umbrella. It produces detailed assessments to help senior policymakers make decisions. To facilitate information sharing, the NCTC has access to more than 30 intelligence, military, and law enforcement networks. Unlike the ISE—which operates more as a pointer system to data maintained by various agencies—the NCTC also takes in copies of data from other agencies, creating its own depository of data that is analyzed and shared. Among other functions, the NCTC maintains a consolidated repository of information about the identities of terrorists from which is derived, among other subsets of data, the watch list used to screen airline passengers.

E-Guardian.—E-Guardian can be thought of as the FBI's own version of the ISE. It permits the sharing of unclassified information relating to terrorism with 18,000 entities, including State and local law enforcement entities. It also helps them submit their own information to the FBI. According to a DOJ Inspector General's report, its companion system, Guardian, which contains terrorism tips and reports by Federal agencies, suffers from numerous data integrity failures, including failure of supervisors to conduct a review to determine whether a threat was adequately addressed, and failure to create a complete record for fully 30 percent of examined records.[6]

---

[4] Markle Foundation Task Force on National Security in the Information Age, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, p. 1. CDT was represented on the steering committee that produced the report and it receives financial support from the Markle Foundation.

[5] In February 2007, CDT issued an analysis of the ISE privacy guidelines. *http://www.cdt.org/security/20070205iseanalysis.pdf*. We noted that the guidelines never actually define what privacy is. The title and text of the guidelines refer to "other legal protections," but never explain what those are either. The guidelines never mention the First Amendment or free speech. The cover memorandum to the guidelines includes one reference to Fair Information Practices, and the guidelines themselves contain some of the FIPs. However, there is no engagement with the challenges of applying the Fair Information Practices in the terrorism context. CDT is preparing a further major study of all of the privacy materials associated with the ISE; our results should be available early this summer.

[6] U.S. Department of Justice, Office of the Inspector General Audit Division, November 2008, *The FBI's Terrorist Threat and Suspicious Incident Tracking System, http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf*.

Fusion Centers.—State and local governments have created at least 58 fusion centers to improve information sharing across all levels of government to prevent terrorism and other crimes, and in some cases, to respond to public health and other emergencies. Non-Federal law enforcement entities, such as State police, are the lead agencies in most of the centers, though most have Federal personnel, usually from the FBI and DHS. The National Strategy on Information Sharing that President Bush issued in October 2007 indicates that the Federal Government will provide grants, training, and technical assistance, and Congress has appropriated funds to provide financial support to fusion centers. Each fusion center is different, but there continue to be questions about their mission and effectiveness and they face significant challenges. Officials in over half of the fusion centers contacted by the Government Accountability Office for a recent report said that they had encountered challenges in accessing Federal information systems, while at the same time over half reported that the heavy volume of information they were receiving and the existence of multiple systems with redundant information were difficult to manage.[7]

Joint Terrorism Task Forces.—JTTFs are comprised of Federal, State, and local law enforcement officers and specialists. The JTTF concept pre-dated 9/11 by several decades but was expanded after 9/11 and there are now 100 JTTFs, including one in each of the FBI's 56 field offices Nation-wide. DHS entities involved in JTTFs include Customs and Border Protection and Immigration and Customs Enforcement. Fifteen other Federal law enforcement and intelligence agencies are involved in one or more JTTFs.

WHAT CIVIL LIBERTIES VIOLATIONS HAVE BEEN UNCOVERED?

Monitoring of Peaceful Political Activity.—Despite the secrecy surrounding the collection of homeland security intelligence, a number of abuses and instances of misguided focus on peaceful activity have already been uncovered, revealing a shocking lack of priorities that is inexplicable in a time of genuine threats. The ACLU has compiled some of these reports;[8] we mention only a few of the more egregious ones here:

- *Maryland State Police Surveillance of Peaceful Anti-War and Anti-Death Penalty Activists*.—As reported in the Washington Post: "Undercover Maryland State Police officers conducted surveillance on war protesters and death penalty opponents [from March 2005 until May 2006] . . . " "Organizational meetings, public forums, prison vigils, rallies outside the State House in Annapolis and e-mail group lists were infiltrated by police posing as peace activists and death penalty opponents, the records show. The surveillance continued even though the logs contained no reports of illegal activity and consistently indicated that the activists were not planning violent protests."[9] The State police classified 53 nonviolent activists as terrorists and entered their names in State and Federal terrorism databases.[10]
- *Reporting on Lobbying Activities and Concern about Tolerance*.—The North Central Texas Fusion System distributes a bi-weekly Prevention Awareness Bulletin to over 1,500 staff in 200 Texas agencies. The bulletin issued on February 19, 2009, under the headline "Middle Eastern Terrorist groups and their supporting organizations have been successful in gaining support for Islamic goals in the United States and providing an environment for terrorist organizations to flourish," cited incidents ranging from the installation of footbaths at the Indianapolis airport to the Treasury Department's hosting of a conference entitled "Islamic Finance 101," as signs of growing tolerance for "Shariah law and support of terrorist military activity against Western nations." The report expressly singled out "lobbying activities" and concluded by warning that "it is imperative for law enforcement officers to report these types of activities to identify potential underlying trends emerging in the North Central Texas region."[11]

---

[7] Testimony of Eileen R. Larence, Director of Homeland Security and Justice Issues at the Government Accountability Office before a subcommittee of the Senate Committee on Homeland Security and Governmental Affairs, April 17, 2008, *http://hsgac.senate.gov/public/_files/LarenceTestimony.pdf*, pp. 8–9.

[8] *http://www.aclu.org/privacy/gen/32966pub20071205.html.*

[9] Lisa Rein, "Police Spied on Activists in Md.," July 18, 2008 p, A1, *http://www.washingtonpost.com/wp-dyn/content/article/2008/07/17/AR2008071701287_pf.html.*

[10] Lisa Rein, "Md. Police Put Activists' Names on Terror Lists," October 8, 2008, P. A1 *http://www.washingtonpost.com/wp-dyn/content/article/2008/10/07/AR2008100703245.html.*

[11] The North Central Texas Fusion System Bulletin is available on the Defending Dissent web site, *http://www.defendingdissent.org/spying.html.*

- *Compiling Nation-wide Lists of Marches and Rallies*.—At least as of 2006, the Intelligence Branch of the Federal Protective Service in DHS was compiling a "Protective Intelligence Bulletin," mainly by using a "media reporting service" available on the Internet. The March 3, 2006 bulletin,[12] 17 pages long, listed dozens of events such as a "Three Years Is Too Many Demonstration" by the Central Vermont Peace and Justice Center to be held at 1400 hours on the sidewalk in front of Main Street Park in Rutland. Recipients were advised that the Bulletin should be shredded or burned when no longer required.

These reports are reminiscent of the 1960's or 1970's in their confusion between peaceful dissent and violent activity. The misallocation of resources alone is cause for serious concern when the Nation faces genuine threats. The potential for a chilling of the exercise of First Amendment rights compounds the concern. Department heads and elected officials, especially appropriators, at the Federal, State, and local level should hesitate before supporting continuation or expansion of homeland intelligence activities until there are rules in place that require a focus on the potential for violence, training programs that distinguish between political activity and terrorist activity, and oversight mechanisms to ensure that prohibitions against First Amendment monitoring are being adhered to.

Overbroad collection of information with SARs.—State, local, tribal, and Federal entities are collaborating to develop a Nation-wide system of Suspicious Activity Reporting. The SARs system is just getting off the ground, but so far, the standards for the program suggest that much innocent activity will be tracked. For example, photographing bridges is described as a suspicious activity, even though such sites are regularly photographed by tourists, journalists and photography buffs.

The risks we are concerned with develop when such "suspicious activity" is recorded and shared with information identifying the person engaged in the "suspicious activity." What prevents the mistaken conclusion that a person is a terrorist because he or she is the subject of two or more SARs, each reporting on innocent behavior? Won't the next official who encounters the same person in a different context and files a SAR to report other innocent activity assume that his or her suspicion is confirmed because of the initial SAR in the system? Will the subject even know how the data is being used or what further scrutiny he faces? How does an individual ever prove the legitimacy of his activity when the object of the process is not evidence but only suspicion? Taking in huge amounts of personally identifiable information about innocent activity and creating self-generating affirmations that make it more likely that yet more information will be taken in does not seem to be the most effective way of conducting intelligence.

WHAT CAN BE DONE TO ADDRESS THESE PROBLEMS AND PROPERLY FOCUS HOMELAND SECURITY INTELLIGENCE?

Require DHS entities to follow principles of fair information practices, including the minimization principle.—The internationally accepted principles of Fair Information Practice ("FIPs") establish a useful framework for using information to make fair decisions about people. There is no single authoritative statement of the FIPs, but the DHS Privacy Office on December 29, 2008 issued a memorandum[13] adopting FIPs as its privacy policy framework, and indicated that it would seek to apply them to the "full breadth and diversity of DHS programs and activities." The DHS Privacy Office language is attached as an appendix. If implemented, these principles would require DHS to:

- Give notice of collection and use of Personally Identifiable Information (PII);
- Seek consent, to the extent practicable, for collection and use of PII;
- Articulate the purpose for collecting PII;
- Collect only PII that is necessary to accomplish the specified purpose;
- Use PII only for the purpose specified;
- Ensure that PII collected is accurate, relevant, timely, and complete;
- Safeguard PII against unauthorized access and improper disclosure;
- Audit actual use of PII to demonstrate compliance with these principles.

Clearly, not all of these concepts can be implemented in the homeland security context in the way that they are applied in the government benefits context, where they originated. One cannot, for example, seek consent from the next Mohammed Attah for the sharing of information about his plotting with al Qaeda operatives among elements of the intelligence community. However, the principles do offer an

---

[12] The Bulletin is posted here: *http://www.defendingdissent.org/ICECalendar.pdf.*

[13] *Privacy Policy Guidance Memorandum,* issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.*

excellent framework for analyzing intelligence collection practices. While the DHS Privacy Office took its action at the end of the last administration, the new leadership of DHS could carry forward this effort to develop Department-wide policies in the detail necessary for effective implementation.

Applying these principles to, for example, the functioning of fusion centers, would help alleviate the civil liberties concerns that they have created. Indeed, the DHS Privacy Impact Assessment (PIA)[14] for the Fusion Center Initiative, also issued last December, goes some distance toward accomplishing this goal. The subcommittee should use its oversight authority to see that the recommendations in the PIA are being implemented.

However, because State and local governments run the fusion centers, the PIA recognizes that adoption of effective privacy guidelines to implement FIPS at each fusion center is largely within the control of local agencies. Materials that will address the privacy protections required of fusion centers participating in the ISE are still under development. The DHS Office of Intelligence and Analysis, which leads the effort to create effective fusion centers, could also work with the DHS Privacy Office to ensure that the fusion centers it helped create comply with these principles, especially the "Data Minimization" principle. Full fusion center compliance would mean that only the information necessary to accomplish the center's purposes would be collected.

Require a criminal predicate where appropriate.—Probably the single most effective civil liberties protection that could be imposed on the collection and sharing of homeland security intelligence that includes personally identifiable information would be to require criminal predication. This means that information is collected or shared only because it has some degree of relevance to a violation of the law. Requiring a criminal predicate in effect requires the person who gathers or shares information to focus on potential wrongdoers, and not on everyone else. Conversely, failure to require a tie to crime invites reliance on inappropriate predicates for collection and sharing of information, such as fear fostered by fiery speech, or by race and religion.

Requiring a criminal predicate for the collection and sharing of PII through homeland security intelligence is not inconsistent with the purpose of an intelligence system because at bottom, these systems are designed to prevent, investigate, or respond to terrorist activity that is a crime.

This principle is captured in 28 CFR Section 23, the guidelines that govern federally funded criminal intelligence systems. These systems are used to exchange information much of which constitutes homeland security intelligence information. The guidelines provide that any federally funded project shall collect and maintain criminal intelligence information concerning an individual or organization only if there is reasonable suspicion that the individual or organization is involved in criminal conduct. 28 CFR Section 23.20(a). To the extent that fusion centers operate federally funded criminal intelligence systems, those systems are bound by this regulation. Still, there is considerable concern that the protections of the reasonable suspicion standard are diluted when federally funded fusion centers collect and share vast amounts of SAR information that does not meet the standard. We would suggest that this is an area ripe for oversight by this subcommittee.

Guard Against Circumvention of Applicable Guidelines.—Circumvention of 28 CFR Section 23 requirements illustrates another danger of inappropriate use of intelligence sharing mechanisms such as fusion centers. Another circumvention problem that has not yet been adequately addressed relates to the investigative guidelines under which many law enforcement entities operate and under which the FBI operates. These guidelines can take a number of forms and will have a variety of provisions designed to protect civil liberties. For example, often following litigation, a police department may adopt guidelines that prohibit it from conducting surveillance of protest activity except when directly tied to criminal activity. The FBI operated under Attorney General Guidelines that included such a restriction, but it was largely removed in 2002. Such restrictions are designed to protect against a chilling of controversial political speech.

However, a partner agency, with which the restricted agency may share information through the ISE, a fusion center, or another mechanism, may have no such limitations. It could conduct the surveillance that its partner agency is specifically barred from conducting and share the fruits with the restricted agency. The civil liberties protections embedded in the guidelines that govern activity of the restricted agency would be circumvented. To our knowledge, no adequate mechanism or bind-

[14] *U.S. Department of Homeland Security Privacy Impact Assessment for the Department of Homeland Security State, Local and Regional Fusion Center Initiative,* December 11, 2008, *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.*

ing and enforceable rule precludes the circumvention of such guidelines. The circumvention problem can flow across State and local agencies, and from or to Federal agencies that participate in the information sharing enterprise.

Avoid redundancies.—As we mentioned above, there are already a lot of cooks in the intelligence information sharing and collection kitchen. The subcommittee should guard against adding more just because a specific new need for information has been identified. The first step should be to ask whether the information needed is already being collected and shared through a system that could be employed to this purpose.

Take a comprehensive look at homeland security intelligence collection now taking place.—The subcommittee, in exercising its oversight role, should sample intelligence products developed by DHS components to more fully ascertain what is being collected, how it is used, and whether it is useful in preventing terrorism. The subcommittee should consider whether more targeted collection efforts would be more effective. Finally, the subcommittee should review the training materials that DHS entities use. The review should be conducted with an eye toward ascertaining whether DHS officials are being trained to avoid inappropriate surveillance, such as the monitoring of death penalty opponents by the Maryland State Police.

The subcommittee could also identify processes that work at one agency and that might be a source of useful guidance to another component or agency facing similar challenges. For example, the Transportation Security Administration has developed redress procedures for air travelers who believe they have been watch-listed inappropriately. While the procedures are not perfect and there are reports that some travelers have found them ineffective, they are an example of an approach to redress in a security environment from which lessons could be learned and applied to other security environments.

Conduct an independent assessment of the value of SARs reporting.—The subcommittee should test whether SARs reporting is both effective and efficient in preventing terrorism. This may involve commissioning a GAO study or conducting an independent staff level assessment. SARs reporting may or may not be the best way to collect the "dots" that need to be connected to head off terrorist attacks; whether it is or is not should be tested. Because the SARs reporting system will result in the collection of so much information about innocent activities, it seems that it would be good to know at the front end that the results are likely to be worth the risks.

CONCLUSION

Many entities at the Federal, State, and local level gather and share homeland security intelligence. More and more information is being collected and shared about innocent activity, creating increased risks to civil liberties. Some of these risks have matured into abuses, including the monitoring of First Amendment activity without adequate cause. Oversight that is focused on ensuring adherence to principles of Fair Information Practices, requiring a criminal predicate to support collection and sharing of personally identifiable information, and compliance with strong privacy protective guidelines would enhance both liberty and security.

APPENDIX

PRINCIPLES OF FAIR INFORMATION PRACTICES AS ARTICULATED BY THE DHS PRIVACY OFFICE [15]

- *Transparency*.—DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- *Individual Participation*.—DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- *Purpose Specification*.—DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

[15] Privacy Policy Guidance Memorandum, issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.*

- *Data Minimization*.—DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- *Use Limitation*.—DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- *Data Quality and Integrity*.—DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- *Security*.—DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or intended or inappropriate disclosure.
- *Accountability and Auditing*.—DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Ms. HARMAN. Ms. Martin, you are recognized for 5 minutes.

STATEMENT OF KATE MARTIN, DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES

Ms. MARTIN. Thank you, Chair Harman, and Ranking Member McCaul and the other Members of the subcommittee, for the opportunity to testify today. I want to share Ms. Fredrickson's thank you for your leadership on the NAO issue. I especially appreciate the committee and the subcommittee taking the opportunity to reassess and take a new look at this very complicated and complex issue.

I want to start off by noting that the term "intelligence" itself is used in a wide variety of situations, and that, as some of the witnesses on the previous panel testified, there are definite intelligence tasks that don't pose the same kind of risk to civil liberties, dissemination of information about ricin. It doesn't oppose the risk to civil liberties, and I think that the LAPD has some examples of the use of SARs that don't pose risks of civil liberties; for example, keeping track of bomb threats in the city.

At the same time I think this subcommittee's inquiry could not be more crucial, because we are at a point in our history where we have seen an unprecedented and, I would say, a fundamental change in the intelligence capabilities of the U.S. Government in the last 7 years. Basically what we have seen is an enormous expansion in the collection authorities across the board, an expansion in the number of agencies in both the Federal Government and in State and local who are authorized to, "collect intelligence," and a weakening of the traditional safeguards and limitations on such collection.

I think that in looking at the problems that such collections pose for civil liberties and privacy, that it is important, as Caroline mentioned, to understand that it is not simply a privacy problem. I think Senator Sam Ervin, one of your predecessors, who was, of course, the author of the Privacy Act, put it best when he explained that when the Government knows all our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

The other problem, we have traditionally dealt with this issue in two fashions. One is by limiting the amount of information that the Government collects, which is also limited by technological and logistical capabilities and, second, by laws. I think that given the past history of the past 7 years, we have to be mindful that we may

not be able to rely upon laws as sufficient to limit Government abuses when faced with national crises. We have examples of an Executive branch claiming the authority to go around and violate the laws and to do so in secret.

So our recommendation to the committee is to begin with a more comprehensive review and assessment of where we are, and where we have come, and the risks, issues imposed by that. I would like to suggest that the committee begin with requiring and articulating specific missions for different kinds of homeland security intelligence.

Second, I think we need a threat assessment. With all due respect to the witnesses on the previous panel, I think there is much to learn from the Israeli example, not least of how to protect civil liberties and democratic processes while facing a true national security threat. I do not think that any objective assessment of the threat faced from homegrown terrorism in the United States will find very much in common with the Israeli experience, but that is an analysis that we need, and we need for it to be done publicly.

We also need to have a more complete picture of what the Government is doing, what its legal authorities are, and what it is actually doing. I think the American public are entitled to some metrics on how much information the Government has, how many Americans are referred to in how many databases, and how many Government officials have access to those databases.

I look forward to and I am certain that this committee will provide leadership on reviewing and making some of the information public with a classified annex if possible for us to begin the real public debate that is needed.

Ms. HARMAN. Thank you, Ms. Martin.

[The statement of Ms. Martin follows:]

PREPARED STATEMENT OF KATE MARTIN

MARCH 18, 2009

Chair Harman, Ranking Member McCaul, and distinguished Members of the House Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, thank you for inviting me to testify today. I am the Director of the Center for National Security Studies, a think tank and civil liberties organization, which for 30 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

I especially appreciate the committee using the opportunities created by the change in administration to hold this hearing and take stock, evaluate, and reassess the role of the Department of Homeland Security and in particular domestic intelligence. While there has been much work done on the enormously complex task of creating the Department of Homeland Security, defining its responsibilities and authorities, etc., it is now time to take a broader look at the role, usefulness, and risks of homeland security intelligence. The past 7 years have been marked by politicians using the rhetoric of fear for political advantage and as a substitute for in-depth analysis and public discussion of the admittedly difficult issues of counterterrorism, domestic intelligence, and civil liberties. The Executive branch has operated with unnecessary and in my view unconstitutional secrecy, the Congress has largely acquiesced (despite the objections of some, including Members of this subcommittee), and intelligence and security issues have been used to score partisan points. The result has been an unprecedented and insufficiently understood expansion of Gov-

ernment power to conduct surveillance on Americans, with very little evidence of its effectiveness, much less its necessity.

Congress needs to examine domestic surveillance and intelligence as a whole. There is no doubt that the Government made many mistakes before 9/11, that globalization has changed the vulnerabilities of the United States, that technology has outpaced the law in some areas, and that changes were needed to ensure the most effective possible counterterrorism effort consistent with our Constitution. The last administration, enabled by an explosion in technological surveillance capabilities took the opportunity to change basic principles and practices limiting Government surveillance of Americans in fundamental and far-reaching ways.

They did so, however, without any acknowledgment of the enormity of the changes. As Suzanne Spaulding has pointed out, the legal framework for surveillance is now a "Rube Goldberg"-like structure, and this patchwork of laws makes it very difficult to understand the full impact of the changes. Moreover, the issues that have been the focus of public debate have been largely technical and frequently subjected to less scrutiny than they deserved because of the political pressures surrounding the debate. There has also been a proliferation of agencies and entities with domestic intelligence responsibilities, although it is not clear that such arrangement was a deliberate effort to create redundancy or just an accident resulting from so many different initiatives by different actors.

Thus, this committee's examination of the role of DHS and "homeland security intelligence" is both timely and much needed. I hope it will serve as a key part of a comprehensive review of the changes made in domestic surveillance and intelligence in the past 7 years that will provide an understanding of the changes as a whole. Such a review is essential to evaluate the effectiveness and necessity of these changes and to recommend changes to make such activities more effective and less threatening to the balance of power between the Government and the people. I expect such review to be facilitated by increased cooperation by the Executive branch.

Today, I want to outline a few issues that I would urge the committee to consider in examining "homeland security intelligence" and the role of DHS in domestic intelligence. They will not be new ideas to the Members of this committee because they are essentially first principles. Yet an examination of recent testimony before the committee suggests that they are frequently overlooked and even lost sight of by witnesses focusing on the necessary details of bureaucratic authorities, funding, and organization.

When evaluating any homeland security intelligence capability, the first question should be whether it has a specific and concretely defined mission. This is especially crucial in the case of DHS, which has myriad and diverse departmental missions. It is not adequate to describe the mission of "homeland security intelligence" as providing intelligence to keep Americans safe or the "homeland" secure. While intelligence may well be useful for many if not all of the Department's missions, it is essential to distinguish conceptually between the different objectives; for example, between the activity of collecting and analyzing information in order to prevent another Katrina, and intelligence aimed at preventing another Mohammed Atta from being admitted into the United States.

Today, I will focus on domestic intelligence for counterterrorism and criminal law enforcement purposes. However, even that mission description is too general to be very useful. In the case of DHS, for example, it could encompass evaluating the vulnerabilities of domestic infrastructures, from water reservoirs to cyber networks; assessing how best to prevent al Qaeda terrorists from entering the United States; and trying to identify any "homegrown terrorists." It is also important to distinguish between activities intended to improve the Government response to terrorist incidents by helping victims and repairing property damage, and Government activities aimed at identifying and apprehending those responsible for such crimes. (There has been a fair amount of work done on analyzing such post-incident tasks and the appropriate legal authorities therefor with regard to Defense Department activities in such situations.)

While each of these objectives requires both information and smart analysis as well as coordination, the relevant information and analysis are quite different depending on the objective. Today, I will not address what intelligence is needed to assess and protect against infrastructure vulnerabilities. Members of this committee, and especially Chair Harman, have long played a leadership role on these issues. And much of the work necessary to protect against such vulnerabilities does not raise the same kind of constitutional and civil liberties concerns as other counterterrorism activities. Rather, I will focus on homeland security intelligence that is aimed at identifying, locating, and "disabling" individuals from carrying out terrorist acts, whether through arrest, deportation, or surveillance.

In evaluating homeland security intelligence, it is crucial to identify when the mission of such intelligence is to prevent or respond to acts of terrorism in the United States, by identifying and locating those individuals involved in such plans or responsible for such acts. It is then equally important to articulate whether the intelligence mission is focused on individuals inside the United States or the intentions and activities of overseas individuals and groups that threaten U.S. interests. It would be enormously useful to require DHS officials when describing and testifying about intelligence activities always to identify whether the activities under discussion include collecting or analyzing information about Americans.

Of course, communications and transactions between Americans and foreigners overseas can be a legitimate subject of inquiry and there must be coordination between intelligence aimed overseas and intelligence conducted in the United States. As the committee is aware, an enormous amount of work has been done to ensure such coordination, beginning with the most basic objective that foreign individuals identified by U.S. agencies overseas as plotting terrorist attacks be barred from entering the United States. But all too often, the mission lines are blurred. One example is the terrorist watch list, which is apparently designed as one list containing the names of both Americans and suspected foreign terrorists living overseas. Such commingling, which is unnecessary for operational purposes, misleadingly implies that the rules and protections for Americans and for foreigners overseas are the same. The civil liberties protections in the Bill of Rights limit Government surveillance in the United States, but have not been extended to foreigners overseas. Nevertheless, the claim is now made that Americans communicating with foreigners overseas, somehow lose their constitutional privacy protections because their correspondents do not enjoy any such protections.

The first step toward restoring the full measure of these protections is to require a fulsome accounting of when homeland security intelligence includes collection or analysis of information about Americans.

An objective threat assessment is needed of the terrorist threat inside the United States. An assessment of the likelihood, magnitude, scope, and source of terrorist threats inside the United States is crucial to any examination of what kind of domestic intelligence makes sense. This is perhaps the area that has been most subject to political and partisan grandstanding and least subject to rigorous analysis. Officials in the last administration regularly warned of "sleeper cells", while wrongfully jailing hundreds of individuals who were innocent of terrorist activities. The public needs a clear understanding of the true nature of the threats from within and without the country. When the Commission on Prevention of Weapons of Mass Destruction Proliferation and Terrorism announced that a WMD attack on the United States is likely in the next 5 years, the headline coverage gave the impression that the Commission had concluded that there are terrorist cells in the United States plotting such, when the report focused mainly on threat activities overseas. When officials talk about a new enemy operating in a networked world requiring a networked response, they do not distinguish between al Qaeda in Iraq and would-be terrorists in the United States. The impression gained from following the terrorism cases brought in the United States in the past 7 years, is that the alleged "home-grown terrorists" were by and large discovered not through network analysis, but through the old-fashioned use of undercover informants.

Assessment of the specific kinds of threats, including an evaluation of how much is known and unknown is essential for evaluating any program for homeland security intelligence. To date, there has been no such assessment available for rational examination and discussion. Instead, there has been a constant drumbeat to the effect that the threat is an existential one.

But as Secretary Chertoff acknowledged, it is not possible to prevent all acts of terrorist violence and keep everyone safe. It is crucial to acknowledge that such incidents are not likely to constitute existential threats to the Nation and that we must take account of the magnitude of the actual threat. It is misleading, for example, to compare the worldwide convulsions and horrors of World War II with the activities of the homegrown terrorists arrested in the United States since 9/11 or even with the attacks in Madrid, London, or Mumbai, terrible as those were. Moreover, recognizing the true extent of the domestic threat is important in order to avoid playing into terrorists' hands who recognize the asymmetry of the power confronting them and hope to provoke a disproportionate response by sowing fear through terror.

Current domestic intelligence capabilities create the risk of a mismatch between the domestic threat and the Government response. There is no doubt that information is key to preventing terrorism and crime and that analysis of information is even more important. But it does not follow that current domestic intelligence activities are necessary or the most effective means of prevention. The term "intelligence"

itself has a variety of meanings, including "criminal intelligence" referring to the analysis of information by police and law enforcement for prevention of crime and terrorism. But the more usual meaning of the term implies that the collection and analysis of information is not necessarily tied to law enforcement. Rather it refers to all the secret collection and analysis activities undertaken by Government agencies to counter threats to the national security. By definition it enjoys a high degree of secrecy and it is seen as the province of experts, both of which make difficult any informed examination of its reliability and usefulness.

In 2003, I wrote an analysis of domestic intelligence and counterterrorism arguing that domestic intelligence should be closely tied to law enforcement in order to protect civil liberties and to insure the most effective counterterrorism. See Kate Martin, "Domestic Intelligence and Civil Liberties" SAIS Review, Vol. 24, No. 1, Winter-Spring 2004. At that time, I wrote in part to argue against the creation of a new domestic intelligence agency rather than tasking the FBI to improve its counterterrorism activities. Since then, no new stand-alone agency has been created, but there has been an unprecedented increase in the number of agencies and entities engaged in domestic intelligence and the scope of their activities. The legal authorities permitting collection of information on Americans have been expanded and the limitations and safeguards against abuse have been weakened. Over the past 7 years, Government agencies have collected enormous amounts of data on enormous numbers of Americans, which is stored in electronic databases virtually forever, and is accessible to enormous numbers of Government employees. Advances in technology have meant that information about individual Americans is no longer "practically obscure" by being hidden within enormous data sets, but instead can be quickly, easily and cheaply retrieved, analyzed, and disseminated to a wide range of Federal, State, local, and tribal officials and employees.

Such developments pose enormous challenges to the balance of power between the Government and the citizens. As Senator Sam Ervin explained in 1974:

"[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.

"Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words."[1]

Senator Ervin is not describing the risks of individual misuse and wrongdoing, such as identity theft or other illegal uses of personal information by unauthorized Government officials. Rather, he is describing a systemic danger to our form of Government.

Indeed, domestic intelligence activities—the secret collection of information by a government on its own citizens and residents—have always posed a serious threat to individual liberty and to constitutional government. There is virtually no domestic intelligence agency, including MI5 in Great Britain, untainted by scandal, political spying and dirty tricks, activities that threaten not only individual rights, but the proper functioning of democratic government. Risks to civil liberties are inherent in the very nature of domestic intelligence. This is because intelligence necessarily operates in secret and, as a result, it is exceedingly difficult to subject intelligence activities to the checks and balances that the framers of the Constitution understood as essential to prevent abuses of power. Secrecy operates to make congressional oversight less vigorous than usual, even though it is more needed in this case to compensate for the lack of the usual forms of public scrutiny over Government activity. In addition, the Executive branch has been very successful in arguing that judicial review of intelligence activities should be extremely deferential and limited, even when constitutional rights are at stake. Perhaps the greatest barrier to strong oversight and accountability is the always-present notion that the interest

[1] Senator Sam Ervin, June 11, 1974, reprinted in *Committee on Government Operations, United States Senate and The Committee on Government Operations, House of Representatives, Legislative History of The Privacy Act of 1974* S. 3418, at 157 (Public Law 93–579) (Sept. 1976).

served by intelligence—national security—is of paramount concern and always outweighs other interests.

While the 9/11 attacks are a reminder of the extent of national security threats to the United States, the response by the last administration confirmed the insights of the Founders concerning the temptations of power and the ever-present need to defend the principles of democratic government. In the name of national security, the President claimed the authority to violate the laws passed by Congress protecting individual liberties and to keep such claims a secret not only from the American public, but even from the Congress. While the warrantless surveillance and illegal interrogations are well known, the administration also rounded up and jailed without due process hundreds of individuals in the United States because of their religion or ethnicity. We can have no confidence that such claims will not again be made by an administration in the name of necessity when faced with inevitable future crises.

It is against this backdrop, that Congress should examine homeland security intelligence. A specific threat assessment is needed that is targeted to the specific missions tasked to such intelligence. Equally important a comprehensive understanding and public report is needed concerning domestic surveillance authorities and the potential uses of intelligence information against individuals, e.g., to place them on watch lists, to deny them security clearances, jobs, legal residency, or to prosecute them. Intelligence information also gives the Government the power to pressure unwilling individuals to become Government informants. Finally, the American public is entitled to metrics concerning the amount of data that has already been collected on them; how many individuals are referenced in how many Government databases; how much information is stored in those databases; and how many requests is the Government making to how many entities for more information about Americans. What kind of information is the Government collecting on how many Americans concerning their lawful political or religious activities?

There is no doubt that all such data will be available to the Government to be used as has happened repeatedly in the past, against political, racial, or religious minorities, against dissenters or against political opponents. We count on this committee and others to examine how to prevent this, to consider whether more narrowly targeted collection programs may be more effective in preventing terrorism while posing fewer risks to constitutional government and individual liberties.

We are grateful for the opportunity to do so with less fear-mongering and partisanship and more public dialog and discussion.

Thank you for considering our views.

Ms. HARMAN. Two votes have been called, and we all agreed to limit our questions to 4 minutes each strictly so that we can make the votes and not inconvenience any of you. So here I go.

First let me say that the witnesses on the first panel all talked about privacy and civil liberties issues. I applaud them for doing that. I think all of them are mindful of this. Whether they have got it perfectly right, I don't know; whether you have got it perfectly right, I don't know either. But fortunately, the debate does include every time, every time I hear the debate, the collection of information necessary to protect against terror threats consistent with privacy and civil liberties and constitutional concerns. So I like hearing that.

I want to know whether you all agree with Ben Franklin and me that security and liberty is not a zero-sum game. I want to start with you, Ms. Fredrickson, because the other two witness put forward some things that they feel should be done, tightening of definitions and other efforts, so that we can carry on with necessary activities to collect intelligence to protect us against homegrown threats while we are very, very focused on the need to protect innocent Americans and others from abusive efforts.

So do you agree that security and liberty are not a zero-sum game?

Ms. FREDRICKSON. Absolutely, and I think those acts show that. When you look at law enforcement that makes a very deliberate ef-

fort to get to know different communities and have relationships, that is probably the most effective way of ensuring that concerns are brought to them, that people are not afraid of them and of keeping us all much safer. I think that is an example that proves your point completely.

I would have to say that we commend Commander McNamara for her interest in having dialog with the ACLU. I understand there are civil liberties concerns in the process of collecting information about people's daily lives and daily activities and ensuring that there is not an improper overcollection of activities such as taking photographs. I think we are continuing to have discussion with her about how to put greater protections into the SARs. We do think they are still overbroad, but I think there is a way of refining it.

I was very pleased with the testimony of the prior panel. I think that there were many quotes that we usually use at the ACLU that were used by the law enforcement professions who were here, and it is music to our ears. I think we are all trying to sing from the same hymnal if we can and reach the same results.

Ms. HARMAN. Thank you.

Could each of you answer very briefly so I keep within my time?

Mr. NOJEIM. Yes.

Ms. HARMAN. Thank you, Mr. Nojeim.

Ms. MARTIN. Yes, and I would agree as well. How to reconcile that it is not as——

Ms. HARMAN. I agree, but let us retire the word "balance." It is not that you get more of one and less of the other. We have got to do it right on the front end, or, let us hope not, comes the next terror attack, and I think we are at serious risk of shredding our Constitution, which to some extent, in my view, happened in the last years since 9/11 because Congress and the public were not part of the dialog about what policies made sense.

The Chair now yields 4 minutes to Mr. McCaul.

Mr. MCCAUL. I thank Madam Chair. I, too, join you in your comments. We will not violate the Constitution in the name of national security; that is what defines us from the terrorists. I thank the witnesses for very thoughtful testimony.

I want to make a few quick points and then turn it over. One, Mr. Nojeim, the idea of intelligence guidelines to test SARs, I am very intrigued by that idea, and I think that is something that the committee should follow up on.

Criminal predicate versus reasonable suspicion would be something I would be interested in your thoughts on. There is a little bit of a difference there.

Ms. Martin, the idea of studying the Israeli model and how they deal with the privacy is something I would like to hear from you on.

Then finally there is an Office of Civil Rights and Civil Liberties at the DHS that did respond to the north central Texas Fusion Center issue that you raised. How can they do a better job? I guess if I can throw that out.

Ms. HARMAN. In 3 minutes and 14 seconds.

Ms. FREDRICKSON. I will be brief. I think the privacy and civil liberties offices need to be strengthened. They have not had enough

independence from the departments that they sit in. They don't have adequate authority to review documents, subpoena documents, in effect, within the Department. So we have regularly recommended that these offices, as well as the Privacy and Civil Liberties Oversight Board, be strengthened so that they can perform a role that is much more of an ombudsman type of role rather than a subsidiary of Department of Homeland Security.

Mr. MCCAUL. Thank you.

Ms. Martin, can you expand on the Israeli model and how we can learn from that?

Ms. HARMAN. Please turn on your microphone.

Ms. MARTIN. Sorry.

The Israeli Supreme Court issued some extraordinary decisions about how—the importance of protecting individual liberty even when faced with the threats that Israel faces. I think at the same time that the day-to-day threats that are faced in Israel are quite different and perhaps not so useful in looking at the day-to-day activities of the local police and State police in the United States, and I would not urge that as a model.

We do not have a history of people getting on buses to blow themselves up and the passengers. I think one of the things I would really like to see is a threat assessment that distinguishes, for example, between the threat posed to U.S. interests by persons overseas, some of whom want to attack U.S. interests overseas, some of whom will try to get here, and the terrorist threat posed by people who are already here. I think that the discovery will be that the resources have been mismatched, that the real threats to the United States are overseas, that is what the Commission on WMD concluded, and that we need to understand that in organizing for, "homeland security".

Mr. MCCAUL. Thank you. I see my time has expired.

Ms. HARMAN. We have 5 minutes and 13 seconds on this vote. Mr. Carney, you get 4.

Mr. CARNEY. Wow. Thank you, ma'am. I will skip the verbs.

I had twice at least sworn an oath to protect and defend the Constitution as a naval officer and as a Member of Congress, and I take those oaths very seriously obviously. But when we look at sort of the post-9/11 world in which we are living and connecting the dots, I am still a practitioner of intelligence as a Navy intelligence officer. How do we kind of make the—I guess the legal term was that I have always heard—the Chinese wall between national intelligence issues and domestic issues; how do we reach that in a way that protects and defends the Constitution for all of you?

Mr. NOJEIM. May I? I don't know that the constitutional inquiry is actually the right one at this point, and I don't think we have to reerect walls between domestic and intelligence activities, because when you think about the Constitution, what is it that protects privacy in the Constitution? It is really the fourth amendment. Often we are not talking about fourth amendment searches when we talk about problems that information collection and sharing creates. We are talking about a privacy value that is not based solely on the fourth amendment.

So where I think would be a good place to start looking and to start thinking about this problem would be to ask what is the bang

for our buck out of all of the intelligence sharing and collection that is going on right now? Are SARs that are being collected worth, if you will, the number of arrests that they generate, or is there a more efficient way to do it, a more efficient way that focuses more on wrongdoing and less on the collection of information about innocent people? That is where I think the inquiry ought to be.

Ms. MARTIN. If I might add in a sound bite kind of way, I think that the mission ought to be to determine how to do smart information sharing, how to determine what information about what is going on overseas is actually useful and helpful to people in the United States who are tasked with this mission, and that there has been very little of that. Instead, all of the bureaucratic incentives are, you better make sure you have shared the information, whether or not the information has been analyzed. It is a hard problem, but that that is what we need to look at. That is what the NCTC is about, about trying to do, but we need more of that.

Ms. FREDRICKSON. I would just add a little bit to that. I think if my dear friends and colleagues would excuse me from using a metaphor that we all use regularly, it is the haystack. We are looking for the needle in the haystack.

Mr. CARNEY. No, you are looking for the needle in the stack of needles.

Ms. FREDRICKSON. Well, when you make the haystack much bigger, it gets harder to find the needle. So what we are suggesting is making sure that the programs that we fund and that are operating are actually efficient and effective, and not letting fear drive our resources.

Mr. CARNEY. Well, when we have more time, I would love to kind of specifically drill down on those recommendations when we can, perhaps at another hearing. Thank you, Madam.

Ms. HARMAN. Thank you, Mr. Carney, and we certainly can. I regularly call on all these witnesses for information and want to suggest that you not be shy and help us get these policies right.

I kind of like what Ms. Martin said about smart information sharing. Dumb information sharing doesn't seem to be a value we should support. Both panels, I believe, get that. I am glad the first panel stuck around to talk to the second panel. That is a form of information sharing, and we appreciate it. This was a great first hearing.

The hearing stands adjourned.

[Whereupon, at 11:56 a.m., the subcommittee was adjourned.]