S. HRG. 111–211

# PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES: STRATEGIES FOR TERRORISM INFORMATION SHARING

## HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM,
TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

APRIL 21, 2009

**Serial No. J–111–15**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
54–241 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
RON WYDEN, Oregon
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware

ARLEN SPECTER, Pennsylvania
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
NICHOLAS A. ROSSI, *Republican Chief Counsel*

---

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

BENJAMIN L. CARDIN, Maryland, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
RON WYDEN, Oregon
EDWARD E. KAUFMAN, Delaware

JON KYL, Arizona
ORRIN G. HATCH, Utah
JEFF SESSIONS, Alabama
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BILL VAN HORNE, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS



## WITNESSES



## QUESTIONS AND ANSWERS



## SUBMISSIONS FOR THE RECORD

# PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES: STRATEGIES FOR TERRORISM INFORMATION SHARING

**TUESDAY, APRIL 21, 2009**

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
*Washington, D.C.*

The Subcommittee met, pursuant to notice, at 2:35 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Benjamin L. Cardin, Chairman of the Subcommittee, presiding.

Present: Senators Cardin and Kyl.

## OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Chairman CARDIN. Good afternoon, everyone. Let me welcome you all to the first hearing of the Terrorism and Homeland Security Subcommittee of the Judiciary Committee for the 111th Congress.

First, I want to acknowledge and thank Chairman Leahy for allowing me to chair this Committee and to convene this Subcommittee. This Subcommittee has a proud tradition. I know that Senator Kyl will be joining us shortly, who is the Ranking Republican member. But the leadership on this Subcommittee under Senator Feinstein and Senator Kyl has established, I think, a record for our Subcommittee to follow. I just want to acknowledge that up front that I very much rely upon the leadership of Senator Feinstein and Senator Kyl in going through the agenda that we hope to handle in our Subcommittee.

We have several issues that we will be taking up. Of course, today we are going to be starting with, I think, the most important responsibility we have, and that is the security of our country, and whether we are getting the maximum information, intelligence information to keep the people of this Nation safe.

This Subcommittee will also have to deal with the PATRIOT Act. Several provisions of the PATRIOT Act will expire this year, and Congress will need to consider extending those provisions or modifying them. I intend for this Subcommittee to play an active role in that regard.

We also have the detainee issues, those that will be leaving Guantanamo Bay, and we will be reviewing with the administration how they intend to deal with the detainees.

We will be dealing with passport fraud. The GAO report recently showed some weaknesses in our system, and we will be taking that

issue up. We will be dealing with cyber security, biological research security, in which I have a direct interest in Maryland, considering it was breached in my own State; encryption policies, espionage laws. So we have a full agenda for our Subcommittee. But today we start with what I think to be one of the most important functions of Government, and that is to keep our people safe. We want to make sure that we have the best intelligence information against the threats of terrorism and the tools that are appropriate for the collection of reliable intelligence information.

I think it is our responsibility to make sure that we have the proper use of resources. After all, these are scarce resources that are taxpayer dollars, that we get reliable intelligence information that can be shared with those who can keep us safe, and that we have the protections for civil liberties. That is our obligation, and that is what we are looking to do.

As a result of the attack on our country on September 11th, the agencies that are responsible for intelligence have been reorganized, and we now have a Department of Homeland Security. We have a Director of National Intelligence. We have a National Counterterrorism Center. And the question is: Is this the right mechanism, the right structure to make sure that we get the most reliable information to keep our Nation safe?

There have been major issues raised about sharing of information, whether we are sharing the information in the most effective way. The Department of Justice has the Joint Terrorism Task Force, which I have worked with in my own State, and is that the best way in order to share information? Are there more effective ways to get information back and forth to keep people safe?

The Department of Homeland Security has their Fusion Centers. I think we need to evaluate whether they are working as appropriately as we think they should.

Have we overcome the bureaucratic obstacles to get information to those who can prevent a terrorist attack? That is a question I hope our witnesses will deal with during the course of this hearing.

We know that the Maryland State Police were involved in a 14-month investigation of peace groups in my State who protested against the use of capital punishment in a very lawful way. There appears to be no reason whatsoever that that investigation should have taken place. We know information was made available to Federal intelligence agencies. The question is: Do we have adequate protection for privacy and civil liberties in our system? Are we doing the right oversight?

Congress passed a law providing for a privacy and civil liberties oversight board in 2007 that has not been appointed yet. Should that board be appointed now? Should we move forward on those issues?

I hope these would be issues that we will take up during the course of this hearing. The 9/11 Commission concluded that, "The choice between security and liberty is a false choice," quoting from the report, "as nothing is more likely to endanger Americans' liberty than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet if our liberties are curtailed, we lose the values that we are struggling to defend."

I think the 9/11 Commission got it right. I think that is the balance that we are trying to achieve in protecting the security of the people of our country and protecting the civil liberties which are the values of our Nation.

I hope that today's hearing will help Congress and the new administration work together to figure out the most effective way to organize our intelligence-gathering capacities and establishing better guidelines for privacy and civil liberties.

Well, we are very proud to have a very distinguished panel of experts who I hope can help us sort through what we need to do.

Zoe Baird serves as the President of the Markle Foundation and also served as the Co-Chair of the foundation's Task Force on National Security in the Information Age. Her task force issued a March 2009 report on the subject of today's hearing entitled: "Nation at Risk: Policy Makers Need Better Information to Protect the Country."

Of course, it is a pleasure to welcome back former Senator Slade Gorton to the U.S. Senate, to the Judiciary Committee, former Senator from the State of Washington, who has a very distinguished record in the U.S. Senate and served as a member of the Markle task force and also as a member of the 9/11 Commission.

We will also hear from J. Thomas Manger, the Chief of Police of Montgomery County, Maryland. I have worked with Chief Manger, and I thank him very much for his work in law enforcement. He represents the largest jurisdiction in the State of Maryland and one of the most diverse jurisdictions, I think, in our Nation. He certainly knows a lot about how these issues affect local law enforcement. Chief Manger also serves as the head of the legislative committee for the Major Cities Chiefs Association.

Our final witness will be Caroline Fredrickson, who is the Director of the Washington Office of the American Civil Liberties Union. I want to thank the American Civil Liberties Union for working closely with us in trying to make sure that we are asking the right questions and that Congress exercises its responsibility of oversight.

I was just checking the protocol of swearing in the witnesses because I have never sworn in a former Senator before. But the tradition of the Judiciary Committee is for the witnesses to take the oath, so if you would all stand. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth?

Ms. BAIRD. I do.

Mr. GORTON. I do.

Chief MANGER. I do.

Ms. FREDRICKSON. I do.

Chairman CARDIN. Thank you. We will start with Ms. Baird.

**STATEMENT OF ZOE BAIRD, PRESIDENT, MARKLE FOUNDATION, AND CO-CHAIR, TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE, NEW YORK, NEW YORK**

Ms. BAIRD. The real breach of protocol is probably to have me testify ahead of Senator Gorton, but as a member of our task force, he has graciously suggested that as co-chair of it, I should start. Thank you very much for having us, and I am really grateful to

all the staff who is here. It is such a wonderful showing of interest on the part of the staff.

Senator Gorton and I, in addition to both coming from Washington State, have had the privilege of working together on the Markle Task Force on National Security in the Information Age, which I have co-chaired with Jim Barksdale, the former CEO of Netscape. The Task Force has been made up of a lot of experts on national security from every administration since the Carter administration, civil liberties advocates, and experts on information technology. We have worked since 9/11 to try to work our way through the challenging questions of how the country can use information in order to better protect us against threats to national security while at the same time preserving traditional civil liberties and privacy interests.

Our recommendations were adopted very substantially by the 9/11 Commission and have been part of both intelligence reform laws that have been passed by Congress—the original Intelligence Reform Act and then the law that was passed that was H.R. 1 and became the intelligence reform law a couple of years ago.

The principal thing I would encourage you to take away from this hearing—and it is apt that you are starting your hearings with this topic—is that our country will not be able to address any of the threats your Subcommittee intends to take up unless we have the best information and we are able to use that information effectively to understand those threats; and to use that information in a way that builds public confidence in the Government; and in the Government's understanding of its constraints as well as its powers.

So with that overview of what this is all about, I would say that our Task Force, after working in the 7 years since 9/11, concluded in our report that we just put out that, unfortunately, this Nation still cannot connect the dots. We have been very fortunate that we have not had another major terrorist incident since 9/11, and a lot of that is due to good work by the Government. But we still are unable to really know what we know, and certainly we are unable to know what we know adequately.

And, in addition, this Nation is still at risk because we do not have the governmentwide privacy policies that we need. Those policies are very important to have the public confidence in the Government's development of intelligence against these new threats we face, whether they be terrorism or energy security or cyber security. While they are important for public confidence, the privacy and civil liberties policies that are needed governmentwide are also critical to empower Government officials, because, by and large, most Government employees do not want to do something that is wrong, and they do not want to be up here in front of you explaining to you why they did what they did that looks wrong.

So there is a great deal of reluctance to act on the part of the intelligence community and law enforcement officials as well, if they do not have clear guidance. So both to achieve our objectives of obtaining and using the information that we need to provide national security and to ensure the protection of privacy and civil liberties, we need governmentwide policy guidelines on privacy and civil liberties. This is a very important area for your Subcommittee

to encourage the administration and to provide continuing guidance.

We made in our report four principal recommendations on how to achieve this. I will go through these very briefly, and then obviously I am very happy to answer any questions you have.

First of all, we encourage you to press the administration and your colleagues in Congress to give priority to this. It is critical that we are able to connect the dots. We need to get information sharing right with good policies for privacy and civil liberties, and we are concerned that this has been languishing and that we may have lost our focus. And as I say, nothing else you want to achieve, whether it is cyber security or border security or anything else you want to achieve, can be achieved without good information so that policymakers can make good decisions.

Second, we really have encouraged two elements of information sharing that require more focus and may be of interest to you. One is the concept of discoverability. Our task force does not believe in creating large centralized data bases. We believe that information should stay with those who collect it and who can keep it accurate enough and up to date. That is a privacy protection as well as a protection to make sure that the information we use is the best information that we have; that is not out of date; that it has not been discredited. But it needs to be discoverable, so whether it is someone in the Maryland State Police who needs to find out if anyone else has information on a particular subject, or whether it is a CIA analyst, people need to find information. They do not need all the content. No one needs all the content. But they need electronic directories. Information needs to be tagged. Even paper directories are better than what we have now so that people can find out who else is working on a problem, who else might have information.

Then the second concept that goes with that we believe is authorized use. In the last intelligence reform law, the law asked the administration to advise us—because they never held hearings on our concept of authorized use, but they put it in the bill anyway—whether this is something Congress should adopt. This really needs to be dug into more, because the authorized use concept basically says that if you want to get access to information, the rules have to say that you are authorized for your mission, for your need, for the predicate that you articulate, the purpose you articulate for why you want to have access to the information. And then if you meet those tests, you can get access to the information in a way that we can audit against it. So later, in a review of whether someone was appropriately looking at information, you can go back and audit whether it was an appropriate authorization, whether they indeed articulated a predicate that was related to their mission. And this is very important because the old classification systems do not really work well anymore. We cannot get collaboration between the Justice Department and the CIA if the only principles we have for what defines what information people have access to are classifications. It is too crude, and it is not oriented toward the current threats.

So that is the second area of focus. The first is leadership, making this a priority; the second is developing the notions of discoverability and authorized use.

The third are the governmentwide privacy policies which I have talked about already.

And then the fourth area of recommendations that we have made are related with what I would sum up by saying, "Old habits die hard"; that both Congress and the administration need to find ways to encourage people to come into the modern age, to encourage people to change their work habits, to become collaborative, to understand that agency lines are not written around the current-day problems that we face. And that can be through setting metrics, through expectations Congress has for the executive branch, through awards, rewards for employees who get it right. But that cultural issue of how do you change old habits is one that really deserves attention, and my guess is something that you are looking at in other areas of reform that you want to see as well.

Thank you very much.

[The prepared statement of Ms. Baird appears as a submission for the record.]

Chairman CARDIN. Thank you for your testimony.

Senator Kyl, of course, is now here. I just wanted to point out, Ms. Baird, that one of the reasons that we—I never make excuses for my fellow Senators, but there is a major bill signing this afternoon on the Volunteers Act with Senator Kennedy and President Obama, and I know that there are members of the Judiciary Committee that are at that bill signing. So I just really wanted to point that out to the witnesses. I know some of the members of this Committee had that conflict, and that is where they are this afternoon.

I want to give Senator Kyl a moment. I said before you came, I thank you and I thank Senator Feinstein for your leadership on this Subcommittee. You have established a bipartisan record of putting our Nation's security first on dealing with terrorism in the work of this Subcommittee. It is a model that I intend to follow, and I personally want to thank you for the work that you have done, both as Chairman and Ranking Member of this Committee. And we hope to follow in that tradition.

**STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA**

Senator KYL. Mr. Chairman, thank you. I will just put my opening statement in the record but return the thanks. It has been wonderful working with Senator Feinstein. We have been both Chairman and Ranking in turn, and there has never been anything partisan about our activities. It has always been focused on how to protect our constituents and fellow citizens.

You have been very helpful in the same vein in organizing this hearing and others, and so it is really a pleasure to work on a Subcommittee like this where that is the attitude that prevails, and I thank you very much. And my sincere apologies to everyone. From time to time you cannot get exactly where you need to be on time, and I very much apologize. I will catch up on the reading here and not make any further statement, but thank you all.

Senator Gorton, it is great to see you again.

[The prepared statement of Senator Kyl appears as a submission for the record.]

Chairman CARDIN. Senator Gorton?

**STATEMENT OF HON. SLADE GORTON, FORMER UNITED STATES SENATOR FROM THE STATE OF WASHINGTON, AND MEMBER, MARKLE FOUNDATION TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE, SEATTLE, WASHINGTON**

Mr. GORTON. The Markle Task Force on National Security in the Information Age is now some 7 years old and has issued three reports on that subject, the latest of which focuses on information sharing and the vital importance of appropriate information sharing at all levels of government toward our national security.

At one level, I have good news, Mr. Chairman and Senator Kyl. We are not asking you for any new laws. We believe that the two statutes that were passed pursuant to the recommendations of the 9/11 Commission, which in turn depended significantly on the Markle Commission's earlier reports, are sufficient to do the job. The problem is in their implementation. The problem is in a very slow-moving bureaucracy which takes a long time in changing its habits. And we want a major change in habit. We have lived for generations on a basis of sharing intelligence on a need-to-know basis. We think the philosophy ought to be "need to share," with the burden being on those who would not share rather than the other way around.

The 9/11 Commission reported on ten lost operational opportunities to derail the 9/11 attacks. Now, we cannot say that any one of them or even all of them would absolutely have done so, but we had ten chances that were missed, and every one of them involved a failure to exchange, to share information which was in the possession of one Government agency or another. And so the current Markle Task Force report, which you have and which you and your staff have read, says that even 7 years after 9/11, our Nation is still at risk. We need better information to defend the homeland.

I am sure that Chief Manger is going to report that it is much easier today to share information upwards from his level than it is downwards from the national level to the law enforcement agencies that are on the front line of our defense. And that is only one example of where we have not done the job exactly right.

We have a couple of very specific requests directed more at the administration than they are here at the Congress. The first one is that the program manager for the information-sharing environment be lodged in the White House. That seemed to be at the present time something of a bureaucratic morass somewhere in the Intelligence Committee. In the White House, that officer would have the ability to see to it that information is shared appropriately.

And, second—and you mentioned this yourself, Mr. Chairman, in your opening remarks—these two statutes have set up a privacy board which is not yet appointed and in being. We also believe that while the Obama administration has started very well in setting out a philosophy for privacy, it needs to enforce a uniform policy on all of the agencies of Government, and it needs to make that policy enforceable, not just a set of suggestions.

Finally, I want to express a real admiration for the two of you and for your Subcommittee in one very important matter. You are not going to get very much publicity or political credit for doing the

kind of oversight job that needs to be done. Success breeds complacency, and we have now gone 7½ years without a terrorist attack in the United States—partly due to better laws and better enforcement, even though they are still inadequate. And that means that people are paying attention to other matters, and that complacency, in my view, is the cause of the great risks that we run at the present time.

So you need to be on the forefront of harassing and talking to people in the administration and getting them to do their jobs right in a way that is probably not going to bring you very much credit. But if you do it right, you will see to it that that 7½ years of no attacks on the United States will be many, many more years in the future.

[The prepared statement of Mr. Gorton appears as a submission for the record.]

Chairman CARDIN. Thank you, Senator Gorton. I appreciate that very much.

Chief Manger?

**STATEMENT OF J. THOMAS MANGER, CHIEF OF POLICE, MONTGOMERY COUNTY, MARYLAND, AND CHAIRMAN, LEGISLATIVE COMMITTEE, MAJOR CITIES CHIEFS ASSOCIATION, ROCKVILLE, MARYLAND**

Chief MANGER. Chairman Cardin, Ranking Member Kyl, I appreciate the invitation to be here this afternoon speaking on behalf of the Major Cities Chiefs of Police, which represent the 56 largest police departments in the United States.

I am pleased to report that the relationships and information sharing between and among Federal, State, local, and tribal police has never been better. But we were coming from a time when it was not very good. So the rest of the story remains that there is still a great deal more to do to fully engage the more than 18,000 law enforcement agencies in this country as full partners in the quest for homeland security.

Federal agencies, despite their ever-improving efforts, have still yet to completely leverage the vast resources of our Nation's police and sheriffs.

Since September 11, 2001, the FBI and the Department of Homeland Security—and all other agencies included in the intelligence community—have made tremendous progress in incorporating State, local, and tribal law enforcement into the national effort to protect our homeland.

But as with any effort so monumental, any effort that has achieved progress so quickly, we need to take a good, long look at what has been created and make certain that what we have is what we intended. Keep what is working and build on it, eliminate duplicative efforts, and fix what is not working as it should.

The areas of oversight for this Subcommittee are far-reaching and critical. But because my time here is limited, I want to focus on just a limited number of topic areas. I will focus on the role of local law enforcement in homeland security; several systems in place to facilitate the exchange of information; establishing and maintaining safeguards for everyone's privacy and civil liberties;

and, finally, some shortcomings from the perspective of local law enforcement.

Law enforcement's role in uncovering and disrupting terrorist activities is well documented. Sergeant Robert Fromme from the Iredell County (North Carolina) Sheriff's Office saw two men enter a discount tobacco shop with over $20,000 cash in a plastic grocery bag. These men came into the shop almost daily buying many cartons of cigarettes. Fast-forward several years and a long-term Federal investigation later, and the ATF and FBI indicted 26 individuals who were using the proceeds from a cigarette-smuggling operation to fund a terrorist group based in Lebanon. A suspicious activity noted by local law enforcement, appropriately documented and legally investigated, results in a terrorist operation being shut down.

This type of story is repeated over and over again because of the relationships and information-sharing mechanisms in place within the Nation's law enforcement community.

I think everyone would agree that the key lesson that 9/11 taught us is that law enforcement is more effective when relationships, protocols, and information exchange systems are established and in place before a crisis strikes.

The national Suspicious Activity Report System—or SARS—is an effort still in its infancy that needs to be invested in and allowed to grow.

The SARS process has directly enhanced the ability of local police to protect our communities from violent crime including terrorism. And, most important, the SARS process can and will be done in a manner that protects the privacy, civil liberties, and civil rights of all.

The two greatest values of SARS are: one, the ability to connect events that in the past would never have been connected; and, two, it is a nationwide initiative that for the first time is providing consistent criteria and consistent training to all law enforcement personnel.

We are training our first responders how to identify behaviors associated with terrorism-related crime and providing them the training they need to distinguish between those behaviors that are reasonably associated with criminal activity and those that are not.

No police chief wants his officers involved in confrontational interactions with people engaged in innocent, constitutionally protected behavior.

Not every person wearing baggy pants is a gang-banger and not every person videotaping the Washington Monument is a terrorist.

Public safety is not enhanced and homeland security is not increased by filling data bases with information about people, organizations, and activities that have no nexus to criminal activity or terrorism.

I firmly believe that the SARS system can operate with strong protections for privacy and civil liberties while it provides the Nation's best practice for information sharing among law enforcement agencies. JTTFs and fusion centers can also operate effectively with these protections. From a local perspective, involvement in the JTTFs and fusion centers remains the most effective way to stay on top of the latest terrorist threat information.

Unfortunately, one of the harshest realities remains that only if a police agency is capable of assigning someone to the local JTTF, or a state or local fusion center, that agency is likely to get its most timely threat information that it can. Those agencies that cannot assign folks to those JTTFs and fusion centers are still likely to get their most timely threat information from the media.

The Montgomery County Police Department, like many large police agencies, has the resources to assign our own personnel to the FBI's JTTF and two fusion centers in this region. We have assigned personnel to the Maryland Coordination and Analysis Center, the MCAC, and the Washington, D.C., Regional Threat and Analysis Center.

While there is some overlap in the intelligence and threat information we receive from these three operations, at any given time one center will have information that is of interest to Montgomery County that the other two do not have. By virtue of our proximity to the Nation's Capital, it is best that we be plugged into all three sources. It is staff intensive and highlights the importance of Federal funding of intelligence analysts that work for the State and local agencies.

Another area that has been a long-term issue is the need for a nationwide system for Federal security clearances. DHS has been very accommodating for sponsorship of security clearances, and the FBI likewise has sponsored clearances for police officials that have membership in the JTTF. Constant promotions, retirements, and transfers make it very difficult for the FBI and DHS 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 the Committee. The chiefs and the sheriffs ask for your help to resolve this issue once and for all.

Another issue involves the sharing of some information with the JTTFs. While fusion centers allow law enforcement agencies to share information generally, there is a problem when the information goes through the vetting process at the JTTF. If the FBI decides to enter the information into the Guardian system for further investigation by the JTTF, the information immediately becomes classified, thus limiting access to the information.

So if, for example, a Guardian lead is investigated involving fraudulent identifications, and it is later determined that the individuals involved have no nexus to terrorism, the lead is then closed by the JTTF. Local police, however, may be interested in working the case from a local crime perspective—an identity theft case. Unfortunately, the information gathered by the JTTF remains classified and often unavailable to local police. These issues require continued work between the FBI and local authorities.

Let me summarize. SARS is working. Let's find a way to get it fully implemented around the Nation—the training, the accountability, and the technology.

Fusion centers are working. Let's ensure safeguards are in place to protect our civil liberties and that all centers are equipped to combat both crime and terrorism. Done legally and done effectively, these centers have been responsible for the arrests of bank robbers, criminal street gang members, money launderers, and terrorists. The cases were made because multiple jurisdictions quickly linked crimes, patterns, and individuals involved in criminal wrongdoing. The value of fusion centers is the information they put out to all stakeholders.

Every local police or sheriff's department has the particular mission of protecting neighborhoods—protecting communities from crime and terrorism. Cops on the street are uniquely positioned to receive and document information from a variety of sources that could assist the Federal Government in maintaining our homeland security.

We have systems in place to facilitate the sharing of that information. Let's make sure all agencies are plugged in. We have systems in place to facilitate the sharing of that information. Let's ensure effective analytic capability so that we do not go down the wrong road.

These systems are in place to facilitate the sharing of that information. Let's establish safeguards so that information is used appropriately and hold people accountable.

We have systems in place to facilitate the sharing of that information. Fund these systems and allow them to mature and improve. It will make our neighborhoods safer and our homeland more secure.

Thank you.

[The prepared statement of Chief Manger appears as a submission for the record.]

Chairman CARDIN. Thank you very much, Chief Manger.

Ms. Fredrickson.

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

Ms. FREDRICKSON. Thank you very much, Chairman Cardin, Ranking Member Kyl, for holding this very important hearing.

We all agree, clearly, from this panel that law enforcement has a legitimate need to share lawfully collected information regarding terrorism and other criminal activity in an effective and efficient manner. But we should also all agree that increasing the Government's authority to collect and disseminate personally identifiable information about Americans can pose significant risks to our privacy and civil liberties.

Last year, as Senator Cardin mentioned, the ACLU of Maryland exposed an extensive Maryland State Police spying operation that targeted at least 23 non-violent political advocacy organizations based solely on the exercise of their members' First Amendment rights. The Maryland State Police spied on an array of political and religious organizations, including religious groups like the American Friends Service Committee, 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. None of the Maryland State Police reports from these operations suggested any factual basis to suspect these groups posed any threat to security. Not surprisingly, no criminal activity was discovered during these investigations, some of which lasted as long as 14 months. Despite this lack of evidence, the Maryland State Police labeled many of these activists "terrorists," distributed information gathered in the investigations widely among law enforcement and intelligence agencies, and uploaded the activists' personal information into a Federal drug enforcement and terrorism data base.

The Department of Homeland Security was also involved, collecting and disseminating e-mails from one of the peace groups to assist the State police spying operation. From a pure information-sharing perspective, things were working well. But the sharing of such erroneous and irrelevant information provided no security benefit to the people of Maryland and only undermined the credibility of State and Federal intelligence systems.

In recent years the ACLU has uncovered substantial evidence that domestic intelligence powers are being misused at all levels of government to target non-violent political activists. In addition to the Maryland State Police investigations, the ACLU of Colorado and the ACLU of Northern California uncovered widespread illegal spying by Federal, State, and local officials. ACLU Freedom of Information Act litigation revealed Joint Terrorism Task Force investigations targeting peace activists in Pennsylvania and Georgia, and Department of Defense intelligence operations targeting anti-military and anti-war protestors from around the country.

The ACLU has produced two reports warning of problems at intelligence fusion centers, so we were not surprised when intelligence products written by fusion centers in Texas, Missouri, and Virginia targeted a wide variety of political and religious groups. And a well-publicized assessment published by DHS this month warned that right-wing extremists might recruit and radicalize "disgruntled military veterans." And a DHS contractor's report smeared environmental organizations like the Sierra Club, the Humane Society, and the Audubon Society as "mainstream organizations with known or possible links to eco-terrorism."

Abusive intelligence reports that share misleading information about the ideologies and activities of non-violent activists do nothing to improve security and only undermine public support for law enforcement. While effective and efficient information sharing among law enforcement agencies is an important, and critical goal, intelligence activities that target political dissent as a threat to security lead only to misguided investigations that violate rights, chill free expression, and waste the time and resources of our security agencies.

Frederick the Great warned that those who seek to defend everything defend nothing. Guidelines and regulations that require law enforcement officers to have a reasonable factual basis to suspect illegal behavior before collecting and distributing personally identifiable information help curb this abuse and focus finite police resources where they belong—on criminal activity.

Congress has an obligation to examine and evaluate all Government intelligence and information-sharing programs regularly and withhold funding from any activities that are unnecessary, ineffective, or prone to abuse.

We do not have to choose between security and liberty, and I think it was in the Markle report that said this is not a zero sum game. Security and liberty both support each other. But 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 establish and enforce reasonable standards that protect both privacy and security.

Thank you.

[The prepared statement of Ms. Fredrickson appears as a submission for the record.]

Chairman CARDIN. Well, once again, let me thank all four of our witnesses. I found your testimony very helpful.

Senator Gorton, let me start, if I might. You said something which I agree with, and that is, it looks like our primary responsibility of this Committee is going to be oversight. We have passed a lot of laws, and there is a lot of authority, and it is a matter of getting it right. But much of it is administrative more so than passing any new laws.

Then, Ms. Baird, you pointed out something that I found interesting, and that is, rather than sharing the information directly by transferring it to different data banks, as I understood your testimony, you are saying that the collector agency should maintain it, keep it current, and then make it accessible for those who have use for that type of information. That would certainly have handled one of our major concerns in Maryland. We were concerned in Maryland not only with what the Maryland State Police did, but the fact that they made that information available to a Federal data bank, and we were concerned that it was then being used extensively in a Federal data bank when it should not have been in a Federal data bank to start off with.

My question basically is: How does one access the information if they do not know it exists? If you are doing a criminal investigation or you stop someone, and if you do not have access within your data bank to that information through appropriate sharing, how do you get timely access to information that allows you to deal with a terrorist threat?

Mr. GORTON. We came up with an analogy, the analogy to a public library and the card catalogue and the old-fashioned way of footing that. And under that kind of system, the gathering agency would not publish it to every other agency by any means, but it would have a short and anonymous index to the subject matter, something of that sort. That would be available to the other agencies, and then if another agency was in that subject matter, they could seek through appropriate means to get a hold of the entire bed of information that—the entire bed of information itself. Just as, you know, you do not go to a public library and wander up and down the aisles hoping that you will find a book on the subject that you want; you look in the card catalogue which has that very brief summary.

This is one way of keeping the information anonymous, not spreading it willy-nilly to every potential reader by any stretch of the imagination, but at least telling the searcher who is looking for a particular subject that something on the subject exists.

Chairman CARDIN. But let me just give you an example. Chief Manger is investigating some criminal enterprise in Montgomery County that may very well be local, or it could very well be connected to terrorist activities. How would he know that the individuals that are participating in this activity are of interest to the collectors of intelligence information nationally as potential terrorists?

Mr. GORTON. If he came up with a particular name, I think—and I am going to let Zoe correct me on this, if she wishes to do so—about which he had reasonable grounds to feel might be of national interest or some such thing, presumably he would be able to find out whether or not the Federal Government had information on that individual or on the type of the activity in which he was presumably engaged.

Is that an accurate description, Zoe?

Ms. BAIRD. Yes, I think that is fair, and I think the point is twofold: One, he has to be able to articulate why it is he thinks this person is connected to terrorism, and he will be accountable for that. But, secondly, the rules that need to be written are rules which would say in passing that information along to the relevant Federal agencies, say the FBI, does he need to pass on the name, or should he pass on the character of the activity that he is seeing to see if it might be related to other activity that the FBI is concerned about?

Obviously, if a local police officer has hard information or reasonable suspicion that someone is engaged in a terrorist activity, they know what to do today. That is, you know, an area that is pretty well worked out. But what we are talking about is the use of intelligence information where the piece of information one individual has does not tell the whole picture. So you need to be able to ensure that that information gets connected up with other people who might have other pieces of information. And we could go back to the 9/11 story. You know all those stories about the bits of information the FBI had, the bits of information the CIA had, and how those dots were not connected.

In fact, in our first report we showed how you could have identified all 19 terrorists from publicly available information, but terrorists are probably a little smarter. Those terrorists were using the same addresses, even the same frequent flyer numbers.

But the key answer to this is that we need the governmentwide policies, and this is an area where you could call in the agencies to account to you what are the policies that they are using to answer these questions. How does a local police officer know, with care, how to share information with other agencies?

Chairman CARDIN. Here is my concern. I do not know whether the local law enforcement has enough dots to connect, and they may very well need to access the national data bank in order to get the missing dot that makes the connections.

Chief Manger, does this work the way——

Ms. BAIRD. If I could add one more comment before you respond, because this may help in your response.

Chairman CARDIN. Sure.

Ms. BAIRD. Take the scenario where, at the Federal level, we have picked up information abroad that terrorists are looking at the possibility of major terrorist attacks on shopping centers—Mall of America, for example. There needs to be a way for the national apparatus, even short of an actual threat warning, to inform local police that they should be observing shopping centers, and if they see information that is suspicious, there is a place where that can be brought together with what the foreign intelligence is. But there is no need for the local police officer to know the details of the foreign intelligence, and there is no need for everyone involved in that information-sharing exercise to know the names of the people who are being observed.

Chairman CARDIN. And I think that is probably handled through the Joint Terrorism Task Force and the fusion centers; that if there is a reason for concern, that information should get to law enforcement through those mechanisms. But my concern is if there is not a red flag nationally about a problem that would warrant notifying Montgomery County, but Montgomery County has part of a scenario but not everything, how does it fill in the blanks without having greater access than I think you would normally give the local law enforcement to be able to check that information?

Ms. BAIRD. The local law enforcement officer, if he is concerned about something he is seeing in a shopping center, should have a directory which says these are the other people who have been looking at threat warnings related to shopping centers, talk to them, create an ad hoc group that is going to discuss what the problem is what they are observing. And that is what we hope the overall information-sharing exercise will encourage, is the forming of groups that share information based on identifying that others are working a similar problem.

Mr. GORTON. Let me give you a specific example, if I can, from 9/11. I believe, from my memory, that FBI agents in Phoenix, I think, discovered that a significant number of people were taking flying lessons but only how to take off and never how to land. Now, the same thing was going on with Moussaoui in Minnesota. But even within the FBI, you know, if the FBI agents in Phoenix had said, "Is this going on somewhere else?" they would not have gotten the information back. If both of them had known it, it might very well have been that the FBI would have authorized going after a subpoena for Moussaoui's laptop—you know, which it did not do.

Now, if that did not happen in the FBI, just imagine what would happen if the Chief of Montgomery County had found people doing the same thing and, pre-9/11, had asked the FBI if it were going on anywhere else. He would have gotten a blank wall from doing that.

But take those bits of information. No one needed to know the names to begin with. The fact that there were people in various parts of the country taking these peculiar types of flying lessons might have been something that brought them together to the point at which they all went forward to the next step. It would have been—it could have been anonymous, would have been anonymous in the original instance. But it did not even happen within

the FBI, much less between the FBI and any local law enforcement agent.

Chairman CARDIN. And I agree with you on scenarios that should be shared. I still have a concern about local law enforcement. With Senator Kyl's permission, I am going to give Chief Manger a chance just to respond.

Chief MANGER. Just a couple of reactions. The system that has been described, you initially asked would that work. And I guess the short answer is I am not sure. Ideally, if we can put the guidelines in place and have them be consistent throughout the country, I think that absolutely needs to be done. And I will tell you an example.

We have gang data-bases that we use regularly, every day, in Montgomery County where there are individuals and information about specific gangs as well as specific individuals in this data-base. There is a specific set of criteria, and it has been—we have discussed it with the community, I think even with the local chapter of the ACLU knows our criteria of how someone can get entered into our gang data-base. The information is scrubbed every so often, but I bring this up because if one of my officers stops somebody for running a stop sign and, you know, because we have the computers in the cars, we just routinely make "Wanted" checks on someone, you know, is that a bad thing? Now, all this person has done is run a stop sign. But shouldn't that officer know that this person is listed in the gang data-base and in the information in the gang data-base, they were arrested a year ago and they were carrying a gun? I think that is information that is good for that officer to know.

Now, again, the officer can deal with the running of the stop sign and that is it, but that is information that I believe is necessary for my personnel to have.

If there are criteria for how someone gets into a data-base and that criteria is agreed on and has protections in it, then I think that it makes sense for that officer who, you know, stops that individual for running a stop sign, if they are on a terrorist watchlist or have some nexus to terrorism, I think it is good that the Federal authorities are made aware that this person ran a stop sign, just for their information. Now, is that going to open up a case? No. But that kind of information sharing could end up being useful. We do not know.

Another example. We had a case where a maintenance person in an apartment complex called us and said, "I have got a suspicious activity. We have a group of men who have rented an apartment. They pay their rent in cash at the end of every month. We just had to go in to change the furnace filters. We went in there. There is not a stick of furniture in this apartment, but there are magazines. There are flight instruction magazines in the apartment."

They called us. Now, there is not a law that has been broken. There is no law that says you have to have furniture in your apartment. There is no law against subscribing to flight instruction magazines. But what you have here is, in my view, a situation that warrants further looking into.

You know, my folks are not equipped to do terrorism investigations, but, you know, that kind of information needs to be shared

with the JTTF. And that is what it was. We turned all the information we had over to the JTTF.

And so I think the key here is having a set of guidelines for information. If information is in the data-base, then it has already been scrubbed. It has already been verified as being appropriate to be in a data-base. And if that is the case, then we should be able to share it with anybody.

Chairman CARDIN. Let me turn to Senator Kyl. We may come back to this in the second round.

Senator KYL. Thank you, Mr. Chairman. I am interested in the same thing, so you are doing a good job of cross-examination there.

Ms. Fredrickson, just on that last point, anything wrong with the Chief's folks sharing with the Joint Terrorism Task Force information that they came across, including, let's say, the names of the people who leased the apartment, just as something that they might want to look into?

Ms. FREDRICKSON. Well, I would like to go back to something that the Chief said in his testimony, which I think puts us exactly in the same place. He said that it is important to make sure that the officers are looking at individuals or events that are reasonably associated with criminal activity. And I think this is an example similar to the running of the stop sign.

What we have a problem with is what the Maryland State Police was involved with——

Senator KYL. OK. I heard you testify about that. But there is no obvious criminal activity in the circumstance that he discussed. In retrospect, knowing what we know about 9/11, you know, a light bulb would go on in our mind. Pre–9/11, I am not sure that your guy seeing that would have necessarily called a joint task force, if it existed at that time.

Chief MANGER. You are right.

Senator KYL. I am just presupposing that.

Ms. FREDRICKSON. And I think this is why there is a need, exactly what Ms. Baird also called for earlier, there is a need for standards. There is a need for standards governmentwide. I think we have a lot of different government entities—the JTTFs, we have the fusion centers, we have a lot of different—I am getting back to your——

Senator KYL. Let me just interrupt you there. What kind of a standard would be appropriate for the circumstance, just the real-life circumstance that the Chief just talked about.

Ms. FREDRICKSON. Well, I think you have to be very careful not to start putting people's names in data-bases if there is not something some reason to believe that they are associated with some criminal activity. I think bringing to Federal task forces this paradigm, I think, again, to refer to what my colleagues have said on this panel, you know, you have to disassociate personally identified information from circumstances——

Senator KYL. But if I can interrupt you, how do you—some three people rented an apartment that had only magazines in it. Well, can you give us their names so we can see if they have some previous terrorist activity? No, I cannot do that. I mean, what good is the info that there was an apartment rented by three people that had no furniture, but just a bunch of——

Ms. FREDRICKSON. Well, I would say that in most circumstances, that information would probably not be worthwhile, and you really do have to be careful about putting—every time you discover an apartment with only magazines, and you look at the people's names on those magazines, and they go into a Federal terrorism data-base, I think that is probably quite problematic.

Senator KYL. Are you maybe jumping some—they go into a Federal terrorist data-base. I think you are skipping one step. The names are reported to someone who determines whether or not they have any kind of information on them. Wouldn't there be a standard before they are actually put into the data-base to try to connect them? Chief, would that be the normal step that would be taken?

Chief MANGER. Yes. I think the key there is, you know, we reported the information to the JTTF. I would be very discouraged if the JTTF just took the names of those four people that were on the lease and stuck them in the data-base. What they need to do is an investigation at this point.

Senator KYL. Right.

Chief MANGER. And I think it is prudent to do that investigation and then, based on the results of that investigation, then determine whether those names should go in the data-base or not.

Senator KYL. Could I ask any of you—and maybe, Chief, you are the one to answer this—what kind of information generally is in the SARS data-base?

Chief MANGER. It is suspicious activity reports, and it is anything that has a nexus to terrorism. I mentioned that——

Senator KYL. Is it terrorism only? Or could it be drug running or——

Chief MANGER. SARS is primarily for terrorism.

Ms. BAIRD. I could maybe jump in try to shed some light on this in terms of the kinds of guidelines that are needed. The circumstance that we do not want to miss is a situation where the FBI in its Intelligence Unit, for example, has information from the CIA that is causing it to look for terrorists who might be living in Baltimore, and then to find that the local police find this apartment, find the flight manuals, and we have some other information which says that there is a terrorist group that is trying to use airplanes to commit a terrorist act.

The situation we do not want to be in is where that information cannot be looked at as a whole by someone who is analyzing the situation. On the other hand, we also do not want to be in a situation where we are taking the names of people, where we have no information at all that they have committed any crime, and we are running them against law enforcement or Federal data-bases.

So I would say that this is a very good example of the care with which these guidelines need to be written because I would think that in a circumstance like this, the local law enforcement can say we got a report of this apartment, these magazines, no reason to think anybody is involved with a crime, but someone was suspicious about this. It is just like the original stories of the time of 9/11 where the Attorney General was talking about the need for the UPS truck driver who sees something suspicious to be able to have someone to call, and the magnificent op-ed written by a UPS

truck driver in the New York Times which said, "I do not want to start becoming a law enforcement officer and reporting on the people I see on the street." Well, we have to figure that out as a country.

So what I would say is you need a place, a circumstance, a guideline which says something that low level—an empty apartment with some magazines lying on the floor—I would not jump to the belief that that person is engaged in terrorism, or we will have laws passed which say we cannot look at any information, because that is not the country we live in.

Senator KYL. Well, if I——

Ms. BAIRD. But we need to—if I could just finish, we need to be able to have someone who might be looking for a terrorist cell in that city, maybe even in that neighborhood, have some suspicion brought to their attention without necessarily having to identify the names, but the ability to go back and find out those names if someone has a reason, can document a reason to obtain them.

Senator KYL. Well, with all due respect, a lot of police work is based on hunches and suspicions, and this reminds me of another suspicious activity that turned out to be a problem and so on. And I think if you try to put too many restrictions on what police officers can follow up—they are not accusing anyone of a crime. They are not putting him into a data-base. What they are doing is saying here are names of three guys on magazines that we picked up under somewhat suspicious circumstances to the Federal authorities, is there anything about these three guys that you already know that might lead us to want to follow it up? I see absolutely nothing wrong with that. Do you? Ms. Baird?

Ms. BAIRD. Well, I think the really important part of what you said is the police officer's knowledge of what is suspicious. I think we have to honor that and certainly enable that. But I think we also have to ensure that that professionalism is carried through and that by opening up an information-sharing environment and an intelligence role for law enforcement officers, that we do not say to law enforcement anything goes now, there are no rules. And that is the problem we have had. And, quite frankly, it has been more an inhibition on the law enforcement officers who want to participate in an information-sharing environment because they are used to following rules and laws, and they need the new rules and laws that operate in the intelligence context, which is different than the law enforcement context.

One of the reasons that the rules might be less stringent in the intelligence context is that the way we act against that information is to not take away someone's liberty by locking them up. In other words, a law enforcement investigation brings the power of Government behind it; whereas, an intelligence investigation might not have the same consequences for an individual.

Senator KYL. So there could be different standards, depending upon the nature of the investigation.

Ms. BAIRD. Right.

Senator KYL. Thank you.

Chairman CARDIN. Well, continuing this line, because I think this is really the critical part, we are trying to get it right on sharing of information. And it is interesting, I think we might be draw-

ing a distinction between information and intelligence. If we gather too much information, we can clog the system and violate privacy, make it very tempting to violate privacy. If we do not collect enough information, then good leads go—you do not follow them up. You do not deal with what we should do to keep people safe.

Now, do not oversell the Maryland situation. The Maryland situation, they did a full investigation. There was nothing there. Nothing should have been forwarded to the Federal Government. It was. It was wrong—violation clearly of laws and privacy—and the Maryland Legislature has taken action. I have not had a chance to review their statute. I know the summary of it, and I would be curious. We can maybe talk later about how effective you believe the Maryland Legislature will be. I am also interested in Chief Manger's view as to what the Maryland Legislature did.

But I think the challenge we have here, we need uniformity on guidelines. We have got to know what the right rules are, and they have to be enough to share information so that when you get information that requires a follow-up for you to complete an investigation, either you turn it over to the appropriate agency to complete the investigation, or you complete the investigation with access to information and intelligence that have been gathered that you should be able to get access to. That is what we are trying to achieve.

I am somewhat concerned about having to draw too many conclusions locally before local law enforcement has access to actionable intelligence information. And I know this is a difficult balancing act, but I do have that concern. And I think we are going to need to follow that up in more detail.

But, Chief Manger, I want to ask you a question because you pointed out a real practical problem we have for local law enforcement in getting information. We have the fusion centers. We have the Joint Terrorism Task Forces. But if you cannot either participate in that or you do not have the resources to assign an intelligence officer to participate, your chances of getting timely intelligence information may be lost.

So I look at some of our smaller law enforcement agencies in Maryland who cannot afford to hire full-time intelligence officers to participate in this and wonder how they get access to information they need in order to participate in keeping our communities safe from terrorism.

Chief MANGER. That is the million-dollar question, and I do not have the answer other than to say the FBI offers LEO, Law Enforcement Online. That does provide some information to anyone who gets an account. It is restricted to law enforcement only, and you can get into that data-base and get some information.

For instance, in the smaller jurisdictions within Montgomery County, I try and maintain a very good dialog with those jurisdictions so that when we get information about a threat, we share that information. But, I mean, I cannot worry about sharing it with the city of Frederick or, you know, Hagerstown or somewhere else. So, you know, they are sort of at the mercy of the agencies that are plugged in whether they get that information in a timely manner. The fact is they usually get it from CNN. That is where it ends up getting to them. By that time, everybody has got it.

Chairman CARDIN. Yes. Senator Gorton?

Mr. GORTON. Mr. Chairman, I would like to go back to Senator Kyl's question, and I must tell you that sitting here and listening to a question de novo, I do not believe that I know the answer to that question in any highly positive fashion. But I believe that is the very reason that we made our recommendation that while this administration has taken a good first step in coming up with information-sharing guidelines for the Federal Government, it ought to make certain that those guidelines are, one, mandatory and, two, you know, apply to all of the agencies, because under those circumstances, people who spend a lot of time thinking very carefully about the values on either side of those questions will have thought them out, I trust, with great care.

And then if we get this privacy board actually appointed and in business, you know, there will be an entity, again, that focuses, I think, very, very carefully on this kind of question. Both the 9/11 Commission report and Ms. Fredrickson in her testimony stated something that ought to simply be a truism. We are not engaged in a zero sum game here in which every enhancement of national security can only come because we are limiting civil liberties or every attempt to validate civil liberties is going to decrease our national security. The two can work together. They can be self-reinforcing.

When I get asked a specific question like that, I just hope there is someone who has thought about it more than I have in 5 minutes right here and can come up with a set of rules and a set of policies that will make it work. And I believe that is clearly possible, and that your function here as a Subcommittee is to try to push the administration into doing that as promptly and effectively as possible.

Chairman CARDIN. Thank you.

Ms. Fredrickson, I wanted to give you a chance to respond as to what you would urge us to look at on guidelines are our highest priorities on protecting the legitimate privacy and rights of our citizens.

Ms. FREDRICKSON. Well, we have a fuller set of recommendations in the testimony we provided to the Committee, but I think one of the important parts is to go to 28 CFR Part 23 and codify that regulation, which would establish a reasonable suspicion standard for all criminal intelligence information collection programs and limit dissemination absent a legitimate law enforcement need.

I think it is very critical that there be standards that are governmentwide, that will be clear for law enforcement and will prevent the kind of surveillance based on First Amendment-protected activities that we have seen not just in Maryland, although that was one of the more recent examples, but across the country.

Chairman CARDIN. Under that guideline, would Chief Manger be able to enter information concerning that apartment that he observed?

Ms. FREDRICKSON. Well, I think there was a general agreement that information would be entered into a data-base without some kind of corroboration of actual criminal activity. But whether there would be an ability to talk to fellow departments and speak with the Federal Government about whether or not there were similar

activities that had been observed, you know, I do not think that would be precluded at all.

Chairman CARDIN. Senator Kyl?

Senator KYL. Chief, one of the things you said was that we need to make the SARS more broadly available, or words to that effect. Two questions. How available? What exactly are you talking about? And, second, what is keeping that from happening? Which would lead us, obviously, to the third point, which is how to make it happen.

Chief MANGER. It is still a very new program, and each individual police agency—and there are 18,000 police agencies in this country—has to make the decision to hook into this. And it takes technology, it takes, you know, funding, and some departments—the Los Angeles Police Department has been a pioneer, done a nice job at getting in there.

The Montgomery County Police is just getting plugged into the SARS program, and it is a pilot agency for the State of Maryland.

Senator KYL. So it basically requires you to get the funding to physically by computer tie your system into that system so that your officers, or at least some of them, can access that information.

Chief MANGER. That is correct. And then also the key here is having an analyst who knows what should go in and what should not go in, and the training, the guidelines, everything——

Senator KYL. So this is interactive in the sense that your guys can put stuff into it as well. They are not merely gaining access to information somebody else has already put in.

Chief MANGER. That is correct.

Senator KYL. One reason I mention this is that yesterday Senators Lieberman, McCain, and I held a hearing in Phoenix about the drug cartel activity coming through Mexico and spilling over into the United States. It is an awful situation, and we asked the Phoenix police chief, for example, what to do about it. He had several stories, and one of the points he made was that they need to be able to get into the SARS system. I did not ask him at that point, "What do you need to do that?" But they will stop someone on a traffic charge and then only later find out that the car was owned by a drug dealer or had been stolen or was operated by someone known to be a carrier for the cartel or something of that sort. And so he was lamenting the fact that they were not tied into it. So it is primarily a matter of resources for local police to tie into the system. Is that correct?

Chief MANGER. That is correct.

Senator KYL. Well, it is good to know that it is only resources.

One of the questions that I had was this comment that, Ms. Fredrickson, you made. You said the current method of homeland security is an "all crimes, all hazards" approach. And I would just like to know from the members of the panel, is that OK? Or were you suggesting that that is a real problem?

Ms. FREDRICKSON. I was suggesting that is a problem because it is wasting resources that should be focused on criminal and terrorist activity.

Senator KYL. But the example that the Subcommittee—in 2004 we had a Subcommittee hearing, and here is a quotation from the testimony: "Three of the 19 hijackers on September 11th were

stopped by State or local law enforcement officials in routine traffic stops in the weeks leading up to the attacks on the Nation. For example, on September 9th, 2 days before the September 11th attack, Maryland State Police stopped Ziad Jarrah for driving 90 miles an hour in a 65-mile-an-hour zone in a rural section of I–95 near the Delaware State line. A videotape of the stop shows the State trooper approaching the car, obtaining the driver's license and registration, returning to his patrol car for a radio check of the credentials. Jarrah, who was on the CIA watchlist, was given a ticket and allowed to go." And there are other similar situations.

Now, that is an example where if we had really applied the "all crimes, all hazards" approach, we might have been able to identify him, is it not? And that would have been a good thing, would it not?

Ms. FREDRICKSON. Well, what we were referring to in the testimony was actually the examples that we discussed, which is of law enforcement mistaking First Amendment-protected activity for suspicious activity and using resources to track, for example, in Maryland anti-death penalty activists or anti-war activists or gay rights activists. That is what we are talking about when we are talking about—the gathering of this kind of information, the sharing of that kind of information with Federal law enforcement and the clogging of the data-bases with that irrelevant——

Senator KYL. Well, if I could just interrupt, these are your words, not mine, the "all crimes, all hazards" approach. I interpreted that to mean that you had to have a crime, that you are not just targeting free speech activity, but you have to have a crime, first of all, and then see whether or not that leads you to something else.

Ms. FREDRICKSON. Well, that is not what was intended in that statement. It really is "all hazards" point of view, and what we are saying is that there needs to be appropriate, effective attention actually to crimes and to terrorist activities.

Senator KYL. So just the general proposition that when a crime is committed, let's say a traffic stop, and then something else is investigated or the data-base is accessed to see whether this would lead to anything else, as a general proposition that is not what you were criticizing, is that——

Ms. FREDRICKSON. No.

Senator KYL. Anybody else on the panel want to refer to that?

[No response.]

Senator KYL. It seems to me that, just as a general proposition—let me get your reaction to it—that while guidelines are really important when you are investigating these kinds of activities, you also need to be very careful that you do not get into a situation analogous to the wall of separation that existed before 9/11, where an arbitrary legal standard prevented the sharing of data. And I can just see one of the officers pulling out a manual about the size—I mean, if you have ever seen a flight manual, they are about that thick—and trying to figure, OK, now here is what happened, what can I try to find out and where do I find it out? I mean, I think you would all agree, would you not, that this has to be done in a very usable way, and that argues against really complicated legalese that is going to make it very difficult for the people on the

spot to be able to access the information in a quick and profitable way. Ms. Baird?

Ms. BAIRD. Senator Kyl, if I could comment on that, in my opening statement I made a statement I would like to reiterate, which is that we need these guidelines not just to constrain Government employees but to empower them, that there is a great deal of uncertainty now about what people are authorized to do, and so they are not doing it.

And the second comment I would make is that you are absolutely right that this has to be very easy to understand and you need to be able to walk around the building, stop somebody in the hallway, and ask them the question and have them be able to answer it. It has got to be that, you know, real time that they know what the answer is of what they are able to do. And we can help that with technology. We can facilitate it by having automatic authorizations or approvals of things that happen because a particular individual enters their identification code and the reasons why they think they need the information. So if we can get the technology systems built as well as the policies written, we ought to be able to facilitate this.

But the lack of adequately robust policies now is really slowing things down more than the technology question, and if anything, the technology is getting out ahead of the policies. And so you are creating more and more ways that we might collect or analyze information, but people are not using it or do not know what they are empowered to do because they do not have robust enough policies.

So I think you are absolutely right, the objective here is not to write a rule book. You know, when I first went to work as general counsel of the chairman, they handed me a 2-inch thick glossary of terms of that industry, and I said, "If I have to learn this, I cannot do my job." You cannot weigh people down with things that make it impossible for them to understand what they have to do. But we do need these rules to empower people so that they are not afraid to act because they do not want to wind up here in front of you saying why they did something without any real authorization that they can point to to say that they were supposed to do it.

Mr. GORTON. I just want to emphasize my full agreement with Zoe in that respect. In this report we say we want a paradigm of need to share rather than need to know. And traditionally in the Federal Government—on this point, I am speaking only of sharing within the Federal Government—there have been great penalties for the unauthorized sharing. And that is why you absolutely had to prove you needed to know something before you got it, and you did not know what you did not know so you could hardly look for it.

We need a set of policies that is at least as encouraging for the sharing of information with people and agencies that have some reasonable access to it than there are penalties for unauthorized sharing. And, again, you are absolutely right, it has got to be clear. People have got to be confident in what they are doing.

Chairman CARDIN. Let me again thank the witnesses for their testimony. As I said at the beginning, this is the first hearing of this Subcommittee. It is intentional to be the first hearing because

I consider this to be our most important responsibility in making sure that actionable intelligence information is gathered in a way that is made accessible to those who can prevent terrorist activities in our country. And I think the comments that have been made about the laws are adequate, provided that there is proper oversight and there are clear guidelines, which we have not yet implemented in our Government. So it is an issue that our Committee will clearly be continuing to have interest in and conduct additional oversight in these areas.

So, once again, let me thank our four witnesses for participating in this hearing. The hearing record will remain open for 1 week for any additional statements or questions, and with that, the Subcommittee will stand adjourned. Thank you.

[Whereupon, at 3:55 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

# QUESTIONS AND ANSWERS

**Senate Judiciary Committee Hearing**

**"Protecting National Security and Civil Liberties:**
**Strategies for Terrorism Information Sharing"**

*

***Tuesday, April 21, 2009***

**Questions Submitted by**

**U.S. Senator Russell D. Feingold to Zoe Baird**

**Question 1:**

Mr. Manger described the information sharing system used by the Montgomery County Department of Police. One of the problems with the current system that he pointed out, however, is the unwillingness of agencies to cooperate and recognize security clearances issued by other agencies. You talked extensively about the importance of "authorized use" of shared information; what solutions do you see to this lack of cooperation between agencies?

**Answer**:

As noted by Mr. Manger in his testimony, the current situation is that the federal government, and state and local authorities, lack clear and consistently interpreted rules for accessing and sharing information that are adapted to the current threats and technology environment. As a result, government officials too often (i) fail to share information due to risk-aversion; and (ii) engage in ad hoc sharing practices without adequate regard for civil liberties; or (iii) undertake uncoordinated collection activities outside the confines of their defined missions. As Mr. Manger also mentioned, the federal agencies too frequently fail to recognize security clearances granted by other agencies.

In order to improve information sharing between agencies, it is imperative that these challenges are addressed with clear procedures that support increased

sharing while continuing to protect civil liberties. The procedures require that we:

a) Develop and issue new guidelines and rules for information sharing based on the purpose for which the party seeking access intends to use the information. These guidelines should be based on the legal authorities for and specific mission of each agency, and should reflect the sensitivity of the information and how the receiving official will use it. Such **authorized uses** should be mission- or threat-based justifications to demonstrate that information was accessed or shared for a reason that the government has determined beforehand to be appropriate and allowable. In most cases, predetermined authorized uses would not apply to individual information items, but rather, to categories or types of information.
b) Build an efficient oversight and technology system that enables users to select, articulate, and electronically certify an "authorized use" as the basis for their access of information.
c) Mitigate risk aversion by establishing carefully considered "safe harbor" protections to ensure that no punitive action will be taken against a government officer for having shared information with another agency, as long as there is a record of a proper authorized use , and there is no indication of bad faith motives.
d) Establish a government-wide dispute resolution mechanism to resolve potential information sharing conflicts.
e) Implement audit-logs to monitor use and compliance of procedures and rules.

**Question 2**:

You mentioned as you were answering one of Senator Cardin's questions that you hope "ad hoc groups" will be formed through use of a subject matter index that shares information on specific searches that have been conducted by other law enforcement agencies. Given that a major issue right now appears to be lack of collaboration between agencies, do you think this is a realistic expectation?

**Answer**:

As noted in my testimony, one of the most important steps to foster an effective information sharing framework is to give users the ability to access - or discover – data that exists elsewhere, a capability that can be called "discoverability". To be able to discover information, we need to develop data indices much as a card catalog in a library guides readers to a particular book. The Director of National Intelligence (DNI) has recognized the need for data to be tagged and indexed at the point of collection, and has recently signed an Intelligence Community Directive (ICD 501), that requires Intelligence Community (IC) agencies to make all information collected and all analysis produced available for discovery by automated means. The objective is to create a "responsibility to provide" approach to sharing information.

The establishment of "ad hoc" groups sharing information through use of a subject matter index is one of the next logical next steps to increase discoverability across federal, state and local agencies. The information sharing framework must enable users to form communities of interest and drive information sharing. Concrete examples of user-driven information already exist, such as the Global Domain Awareness Program (GMDAP), a program developed by the Department of Transportation and the Navy that tracks the movements of more than 10,000 vessels from over 40 nations in real time. Information sharing is no longer an abstract concept, but a key practical tool to foster cooperation between agencies. In our judgment, the lack of cooperation between agencies, when and where it still exists, can only be overcome by a combination of high-level policy attention from the President and Congress and appropriately deployed technology that can allow increased discoverability coupled with the gradual implementation of a trusted authorized use standard.

**Question 3**:

Many of Mr. Manger's comments suggest he supports a much more open information sharing system than the one that exists currently. How much would a more open system conflict with your perception of "authorized use", which seems to be very important to your information sharing paradigm.

**Answer**:

As explained earlier, authorized use both empowers and constrains government officers. It will allow a much more open information sharing framework

operating in combination with a trusted mechanism ensuring users accountability and public confidence. Authorized use ensures that users obtain what they need, when they need it, but only for the purposes defined and authorized.

**Question 4**:

At the hearing, witnesses discussed the hypothetical of a landlord discovering that tenants who pay in cash every month have no furniture in their apartment, just a number of flight instruction manuals. In this instance, no laws have been broken but some law enforcement officials might think this presents a "suspicious" situation. You suggested that it would be important to defer to police officers' knowledge of what is "suspicious" or not. But some might say that an understanding of what is suspicious or not would necessitate use of a database of information, which points away from authorized use and more toward more open sharing. How would you respond to this argument?

**Answer**:

In addition to police officers' judgment, it might be necessary to "discover" information made accessible to authorized users to make an assessment of a potential threat. In addition to the authorized use, the Markle Task Force has recommended the use of technology to anonymize information to enable information analysis without disclosure of personally identifiable information before there is a basis for doing so. Commercially available technology allows for removal of personally identifiable information (PII) so that the index that allows for discoverability can be created without any information that identifies an individual by name or other specific identifier. Therefore, the risk of unintended disclosure of PII contained in the data indices is reduced, while allowing access to information databases in ways that both enhance national security and the protection of civil liberties.

In this respect, Congress should revisit the determination of the program manager for the Information Sharing Environment that adequate removal of PII via data anonymization is technologically infeasible.

**Senate Judiciary Committee Hearing on "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing"**
**Tuesday, April 21, 2009**

**Questions submitted by U.S. Senator Russell D. Feingold**
**to Caroline Fredrickson**

**1. While information sharing between law enforcement agencies is important, civil liberties and privacy must also be protected. The discussion at the hearing was fairly abstract. What are some particular safeguards that the ACLU advocates to ensure the protection of Americans' civil liberties?**

History demonstrates that the police power to investigate is easily abused, particularly where the secrecy necessary to protect legitimate law enforcement activities thwarts effective oversight, constitutional checks and balances, and public accountability. Protecting against this abuse requires a multi-faceted approach that includes strong guidelines, audit mechanisms to ensure compliance, external oversight and effective redress mechanisms for those whose rights are infringed. Congress should also address problems with the over-classification of terrorism-related information and the misuse of control designations on unclassified information, as these twin problems impede effective information sharing and prevent adequate oversight of counter-terrorism programs.

1). Strong Guidelines

Privacy and civil liberties protections must be built in at each stage of the intelligence process: when personally identifiable information is collected, when the decision is made to retain the information in an intelligence system or database, when the information is analyzed, and when it is disseminated. The current federal regulation governing criminal intelligence systems, 28 Code of Federal Regulations Part 23, effectively addresses the collection, retention and dissemination issues. The regulation's "reasonable suspicion" standard for information collection is clear, well defined in law and has been universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of police officers for over thirty years. Unfortunately the federal government has not been enforcing the regulation, and it contains no mechanism for outside entities to compel compliance. Congress should codify relevant portions of the regulation to establish a reasonable suspicion standard for all criminal intelligence collection programs and to limit dissemination absent a legitimate law enforcement need. As required in the current regulation, dissemination of criminal intelligence information to non-law enforcement entities should be prohibited unless necessary to avoid imminent danger to life or property.

Part 23 also requires data within a criminal intelligence system to be reviewed and re-validated at least every five years to assure that all the information in an intelligence system is relevant and important. Any information that cannot be re-validated, or is

found to be "misleading, obsolete or otherwise unreliable," must be destroyed. This fundamental data management policy would be appropriate for any data management program, but it is essential for criminal intelligence systems where unreliable information could easily misdirect law enforcement resources, with potentially devastating consequences for innocent individuals improperly subject to police scrutiny. Congress should establish this five-year re-validate or purge practice for all U.S. person information contained in federal intelligence systems.

Data is now being used in ways that could not have been contemplated when the regulation first went into effect almost three decades ago. The increased use of data mining technologies can amplify discriminatory collection policies when the skewed data sets are used to establish "patterns" justifying increased surveillance of the suspect class. Congress should ban racial profiling in all federal law enforcement and intelligence programs by prohibiting the use of race, ethnicity, national origin and religious affiliation as factors in all data collection, investigations or data mining activities.

Congress should also address the overbroad authorities given to the FBI under guidelines produced by former Attorney General Michael Mukasey just weeks before the Obama administration came into office. This was the fourth major re-write of the FBI's investigative authorities under the Bush administration alone. Congress should end this instability by establishing a legislative charter for the FBI that places reasonable limits on the FBI's investigative authorities. An effective charter would require a factual predicate establishing a reasonable suspicion that a person or organization is or will engage in illegal activity before the FBI may employ intrusive investigative techniques that implicate the privacy and civil rights of U.S. persons.

Finally, statutory guidelines should also provide a remedy for individuals harmed by abusive investigations or intelligence activities conducted in violation of law, the Constitution, or regulatory standards.

2). Audit Mechanisms to Ensure Compliance

A recently released audit of the Massachusetts Criminal Justice Information system revealed that dozens of law enforcement officials improperly accessed state criminal records systems, FBI III and NCIC files, motor vehicle records and firearms registries hundreds of times to obtain information about local celebrities.[1] This type of misconduct should come as no surprise when information collection and sharing programs expand without adequate internal controls governing access to this potentially damaging information and where external oversight mechanisms are rare or nonexistent. We suspect that audits of FBI, DHS or other federal intelligence databases would likely reveal similar improper activity. In addition, today's information sharing initiatives are often multi-jurisdictional, so which of the several participating entities is responsible for compliance with applicable state, local or federal laws and regulations is often obscured. This ambiguity in authority creates loopholes of accountability, and establishes an environment where abuse can flourish.

This result is particularly true with respect to intelligence fusion centers, which incorporate federal, state and local law enforcement, emergency services agencies, military personnel and even private companies. In many of these centers it is difficult to determine what rules apply to the collection activities of the many different participants, or regulate the sharing of information among them. Most fusion centers receive federal resources and Congress should tie these resources to the adoption of regulations that require routine audits evaluating compliance with all applicable federal, state, local and/or tribal information sharing laws, regulations and policies. The audits could be conducted by the Government Accountability Office, the Inspectors General of the federal agencies, state and local authorities, or a combination of these. The critical component, however, is the requirement that all fusion center participants document and retain an auditable record regarding information access, use and dissemination activities taking place through fusion centers. The Massachusetts audit revealed the state information systems did not have user identification and authentication safeguards to document which officers made the inappropriate requests. Without proper records, no audit can be successful and abuse will not be curbed.

3). External Oversight and Effective Redress

Congress should also intensify its oversight of all government intelligence collection, sharing and analysis programs. A recent audit of the FBI's Terrorist Screening Center (TSC) Watchlist found a 35 percent error rate, leaving hundreds of thousands of innocent people listed while known terrorists are not.[2] This report, which makes findings similar to those in two previous audits of the TSC, should be the beginning of Congress's examination of the federal government's data collection and management practices, not the end. Congress should immediately stop funding any programs that are ineffective, illegal or prone to abuse. A comprehensive approach to the oversight of intelligence activities would also reveal which programs are redundant or superfluous, allowing Congress to eliminate wasteful projects and focus resources where they can be more effective.

Congress also should create effective redress mechanisms for innocent persons who have their private information improperly collected, accessed or used by an intelligence or law enforcement agency in a manner that violates their First Amendment rights.

4). Reform Classification Policy

Over-classification and improper control designations on unclassified information impede effective information sharing and prevent the type of independent outside oversight that is necessary to curb abuse. The failure to share information, which according to the 9/11 Commission, could have been used to prevent the attacks, such as the refusal to disseminate NSA and CIA information regarding the travel of hijacker Khalid al Mihdhar to Kuala Lampur and into the U.S. to FBI agents investigating the U.S.S. Cole bombing, were due in large measure to the classified nature of the information collected. Yet little has been done since then to reduce the over-

classification of terrorism intelligence, and it remains a major impediment to information sharing. Chief Manger testified that even today information provided by state and local police to the FBI Joint Terrorism Task Force "immediately becomes classified," and that the results of any JTTF investigation therefore become unavailable to the police officers who initiated the inquiry. Such a system is nonsensical, and makes it less likely police will provide information to federal authorities. Excessive secrecy also impedes congressional and public oversight. As Chief Manger said, these issues require work, and we encourage Congress to take on this longstanding problem that harms both our security and our democracy.

To add to this problem, federal government entities have been using over one hundred different control markings to limit the distribution of unclassified information. These are the real barriers to information sharing, and Congress should act to eliminate over-classification and the improper use of control markings to restrict access to unclassified information.

**2. Many of Mr. Manger's comments suggest that he supports striking a balance in favor of a much more open information sharing system than the one that exists currently. Are you bothered by the possibility of an information system that shares information even more widely? What additional civil liberties safeguards would be required if his recommendations were followed?**

Yes, the more widely personal information is shared the more likely privacy and civil liberties can be harmed. We all want law enforcement officers to be able to effectively and efficiently share lawfully collected information when necessary to conduct a legitimate law enforcement activity, but collecting information that is not relevant to illegal activity and sharing information with non-law enforcement entities creates unnecessary risks. Under the guidelines suggested above, personally identifiable information could only be collected in an intelligence system when the police have reasonable suspicion the information is relevant to criminal activities. Information should only be disseminated to other law enforcement agencies to fulfill a law enforcement purpose, and with other non-law enforcement entities only when necessary to prevent imminent harm.

**3. At the hearing, there was a discussion of the need for standards and review before simply "dumping names" into a database. Do you have specific suggestions of how such a system could and should work?**

Intelligence is only valuable if it is relevant, reliable and timely. This is why phone books are updated every year. Clearly not all, or even most of the telephone numbers change each year, but enough do that the telephone book itself becomes an unreliable source of information. Intelligence systems work the same way. Once agents, analysts discover they cannot rely on information in a system they will stop using it, destroying the value of the entire program.

The idea that all data is valuable to intelligence is simply wrong. The Joint House/Senate Select Intelligence Committee investigating 9/11 determined the NSA did intercept communications relevant to the attacks, but the importance of those intercepts was not recognized until after 9/11.[3] The Joint Intelligence Committee report indicated that these intercepts and other bits of critical information were lost in the "vast streams" of data being collected by the intelligence community at the time. Too much data, particularly when some of it is erroneous or misleading, hurts our intelligence efforts. Unfortunately, that "vast stream" has now turned into an ocean of data that is being collected today, primarily without particularized suspicion. These programs proceed with the hope that data mining technology can later make sense of the information collected. But a recent National Research Council study funded by DHS concluded that data mining for counterterrorism "is neither feasible as an objective nor desirable as a goal of technology development efforts," and would infringe on the privacy of innocent persons.[4]

Effective intelligence collection must be narrowly focused on real threats. Requiring a reasonable suspicion standard for the collection and retention of personally-identifiable information is the first step. Establishing a process to evaluate the reliability of the information before placing it in a criminal intelligence system is an essential component. Finally, employing a process to review and re-validate the information at least every five years will ensure that inaccurate, obsolete and otherwise unreliable information is purged from criminal intelligence systems on a regular basis. These are processes most law enforcement agencies already employ, as they are requirements of the federal regulation governing criminal intelligence systems. Following effective regulations that have been in effect for three decades, rather than collecting private information with the blind hope that technology can make sense of it, would be the appropriate method of addressing the problem.

---

[1] Commonwealth of Massachusetts Office of the Auditor, Report on Information Technology Controls at the Criminal History Systems Board, (May 5, 2009), at: http://www.mass.gov/sao/Audit%20Reports/2009/200808574t.pdf

[2] DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GENERAL, AUDIT DIVISION, FEDERAL BUREAU OF INVESTIGATION'S TERRORIST WATCHLIST NOMINATION PRACTICES, (May 2009).

[3] S. Rept. No. 107- 351, H. Rept. No. 107-792, 107th Congress, 2d Session, Dec. 2002, p. xii, http://a257.g.akamaitech.net/7/257/2422/24jul20031400/www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf

[4] 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.

**Senate Judiciary Committee Hearing on "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing"**
**Tuesday, April 21, 2009**

**Questions submitted by U.S. Senator Russell D. Feingold**
**to J. Thomas Manger**

1. You stated in your testimony that "[w]e have systems in place to facilitate the sharing of that information … let's make sure all agencies are plugged in." MCAC (Maryland Coordination and Analysis Center) is the entity that facilitates the sharing of information. Some of the "systems" they utilize to disseminate information and intelligence are electronic (e-mail) disseminations of officer-safety bulletins, threat assessments, and guardian leads.

   A law enforcement agency need only complete an application in order to receive daily briefs from MCAC. In order for information to have value, however, sharing of information *MUST* go vertically (up/down) and horizontally. Maryland law enforcement agencies must forward information and intelligence (activities, behaviors, indicators, and incidents) to the MCAC in order for MCAC to "connect the dots" through analytical processes and disseminate intelligence back out to any and all affected agencies. Quite simply, MCAC is the mechanism to facilitate the sharing of information but it is dependant upon federal, state, local and tribal entities to forward their respective "piece of the puzzle" to MCAC so that analysis is conducted and actionable intelligence is disseminated. Similarly, Sen. Gorton testified that we don't need new laws to grow the information sharing system we have. But Ms. Fredrickson says the systems we have, while potentially adequate for sharing information, are incapable of protecting civil liberties, meaning that we might potentially need new systems or new laws to protect that information. How would you respond to that concern? All projects utilizing **federal funding** to operate criminal-intelligence systems must comply with a number of regulations and policies: 28 CFR – Code of Federal Regulations - Part 23, is a guideline for implementing criminal-intelligence systems projects. It specifically provides guidelines in five primary areas (submission and entry of criminal intelligence information, security, inquiry, dissemination, and review and purge). The purpose of 28 CFR Part 23 is to ensure that all federally funded criminal-intelligence systems are utilized in conformance with the privacy and rights of individuals. Furthermore, there is a statutory provision within the Omnibus Crime Control and Safe Streets Act (of 1968) which requires that no funding be used to support any intelligence system that would be in violation of any constitutional rights or the right to privacy. 28 CFR Part 23 is designed to strike a balance between the legitimate need of law enforcement to fight crime, to investigate crime, and the rights of individuals to be secure in their persons and the right to have freedom of speech and association, religion, *etc.*

If, however, an agency develops and maintains an internal criminal-intelligence operating system, does not utilize federal funding to operate said system, and does not share their intelligence with outside agencies, they are not held to the standards of 28 CRF Part 23 guidelines. It is **MY personal opinion** that if additional legislation were considered, it would mandate that any and all criminal-intelligence operating systems (federally funded or not, shared or not) must comply with 28 CFR Part 23 guidelines.

2. You pointed to funding as a major impediment to information sharing by the Montgomery County Department of Police. Other than the costs of the computers themselves (which you mentioned), can you explain in more detail how any additional funding would be spent? Post-9/11, sharing the collection product is absolutely vital, underscoring the unavoidable fact that law enforcement agencies cannot use or share evidence or intelligence that they can't collect. To that end, MCAC purchased and acquired a "SARS" software package (vendor – MEMEX) which they intend to incrementally roll out state-wide to all MCAC participating agencies. MCAC will eventually need to purchase hundreds (if not thousands) of additional-seat licenses (at a cost of approximately $2,000 per-seat license) to allow the "end users" of the system (Maryland law enforcement agency personnel) to gain access to search and upload information and intelligence to the SARS system. The purchasing of computers is not the issue, as the SARS seat license for access can be uploaded to any computer. The purchase of thousands of seat licenses, however, is a cost issue. Additionally, law enforcement agencies cannot "connect" the dots unless they first "collect" the dots. That can't be accomplished by computers and software alone. The SARS software will help, but funding is required to place multiple trained analytical personnel at those computers in order to have an effective analytic capability. In order to walk the walk of intelligence-lead policing, analytical support personnel are desperately needed to coordinate with area agencies and Fusion Centers such as MCAC, WRTAC (Washington Regional Threat Analysis Center), NVRIC (Northern Virginia Regional Information Center), and others in order to conduct an all-crimes approach to information-sharing and analysis.

###

# SUBMISSIONS FOR THE RECORD

**Testimony**
**Zoë Baird**[1]
**Subcommittee on Terrorism and Homeland Security of the Senate Judiciary Committee**
April 21, 2009

Chairman Cardin, Senator Kyl, it is a privilege for me to appear before the Subcommittee today to discuss the risk our homeland faces because of insufficient progress on information sharing. Today, we are still vulnerable to attack because—as on 9/11—we are still not able to connect the dots. At the same time, our civil liberties are at risk because we don't have the government-wide policies in place to protect them as more powerful tools for intelligence collection and sharing information emerge.

The United States confronts a stark set of national security challenges including terrorism, the global economic crisis, energy security, climate change, cybersecurity, and weapons of mass destruction. Our government cannot identify, understand, and respond to these threats without the collaboration and sharing of information among officials across the federal, state and local levels in a manner that protects civil liberties so fragments of information can be brought together to create knowledge. To improve decision making, Congress and the President need to take immediate steps to enhance information sharing. Otherwise, despite all the United States has invested in national and homeland security, we will remain vulnerable because we have not adequately improved our ability to know what we know about these threats.

I hope my comments today will give this Subcommittee a clearer idea of the steps that should be taken to provide policy makers at all levels of federal, state and local government better information so they can make the best decisions to protect the country.

---

[1] President of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies to address critical public needs, particularly in the areas of health care and national security.

The Markle Foundation Task Force on National Security in the Information Age

Since 2002, I have served as the Co-Chair of the Markle Foundation Task Force on National Security in the Information Age, a diverse and bipartisan group of experienced former policy makers and national security experts from the Carter, Reagan, Bush, Clinton, and Bush administrations, senior executives from the information technology industry, and privacy advocates. The Markle Task Force has released four reports[2] recommending ways to improve national and homeland security decision making by transforming business processes and the way information is shared while at the same time protecting civil liberties. The Task Force has worked closely with government officials, and I am pleased to report that the government has taken many of our recommendations to heart.

On March 10, 2009, the Markle Task Force released its most recent report entitled 'Nation At Risk: Policy Makers Need Better Information to Protect the Country.' Over the last seven months, the Task Force has interviewed numerous officials in the Executive Branch and the Congress on the state of information sharing in order to identify priorities for the new administration, which now includes several former Task Force members. Common themes and findings emerged from these interviews, forming the basis of our recent report's four core recommendations, which are outlined below.

Although the Task Force's recent work has largely focused on the federal government, our recommendations are applicable at the state and local level as well. Much work on the state and local level still needs to be done, such as a careful examination of the role of fusion centers.

[2] The four Markle Task Force reports are *Nation at Risk: Policy Makers Need Better Information to Protect the Country* (2009), *Mobilizing Information to Prevent Terrorism* (2006), *Creating a Trusted Network for Homeland Security* (2003), and *Protecting America's Freedom in the Information Age* (2002). All reports are available at http://www.markle.org/.

I commend the Subcommittee for its oversight efforts in this area because, where there have been improvements, they have been aided a great deal by Congressional attention.

Four Core Recommendations from the Markle Task Force's 2009 Report

First, the Congress and President Obama should reaffirm information sharing as a top priority, ensuring that policy makers at all levels of federal, state and local government have the best information to inform their decisions. Information sharing must not get ahead of strong protections for privacy and civil liberties. We are at a critical moment, where immediate action at the start of the new administration is required. There is unfinished business in implementing an information sharing framework across all government agencies that have information important to national security, including state and local organizations. The 111th Congress and the Obama administration should take this opportunity to get the right policies and structures in place. An information sharing framework will allow government to collaborate effectively across diverse areas to better inform policy makers without undermining civil liberties.

Second, the Obama administration and Congress should ensure that all government information relevant to national and homeland security is discoverable and accessible to authorized users while audited to ensure accountability. Otherwise we will remain vulnerable. When federal, state and local government officials have the capacity to locate relevant information and to make sense of it, they can find the right information in time to make better-informed decisions. Such a decentralized system of discoverability, rather than the creation of large centralized databases, simultaneously improves our security and minimizes privacy risks because it avoids bulk transfers of data. When combined with an authorized use standard, discoverability ensures that users obtain what they need, but only what they need. This authorized use standard would permit data users, such as fusion centers or CIA analysts, to

obtain information based on their role, mission, and a predicated purpose. We also recommend strong auditing throughout the system, which allows for improved enforcement of the authorized use standard as well as contributing to enhanced information security.

Third, the new administration should develop government-wide privacy and security policies for information sharing to match increased technological capabilities to collect, store, and analyze information. These policies should be detailed and address the hard questions not answered by current law—who gets what information for what purpose under what standard of justification and where should information be maintained to provide for security and accuracy. Without such policies, the American people won't have confidence in their government, while the users of the information sharing framework won't have confidence that they have what they are expected and allowed to know, and that their work is lawful and appropriate.

Finally, the President and Congress should overcome bureaucratic resistance to change. Old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. The adoption of the "need to share" principle and the responsibility to provide information, and actions to transform the culture through metrics and incentives, are necessary to the success of the information sharing framework. In addition, those federal, state and local officials who depend on information to make decisions and accomplish their mission should be empowered to drive information sharing, to ensure they get the best possible data.

These are broad recommendations but our recent report, which I would like to submit for the record, sets out very detailed measures to achieve these objectives. The Markle Task Force's recommendations are not complicated. We believe that technology currently exists to achieve them. But they do require strong, sustained leadership and attention to implementation.

I would like to take the remainder of my time to focus on two of our four recommendations: (1) making government information discoverable and accessible to authorized users, and (2) enhancing security and privacy protections to match the increased power of shared information.

Making Government Information Discoverable and Accessible to Authorized Users

In an effective information sharing framework, information is not simply shared without restraint. The Markle Task Force recommends two critical features that regulate access in the information sharing framework: (1) discoverability and (2) authorized use. When combined, increased discoverability and an authorized use standard ensure that federal, state and local users can obtain what they need, but only what they need. This system of selective revelation ensures that, in time-critical situations, authorized users can locate, get access to, and make sense of, relevant information, while protecting privacy and enhancing information security.

**Increased Discovery**. Perhaps the single most important step to foster an effective information sharing framework is to give users the ability to discover data that exists elsewhere—a capability that can simply be called "discoverability." The traditional information sharing model requires either the sender to know what information to send to whom ("push") or requires the end-user to know who to ask for what ("pull"). Whether push or pull, there are too many doors on which to knock. The chances of the right data holder and the right end-user locating each other and sharing the right information are slim at best.

Discoverability through use of data indices is therefore the first step in any effective system for sharing information. Such indices serve as a locator service, returning pointers to data holders and documents based on the search criteria used. If information is not registered in data indices, then it is essentially undiscoverable. Think of data indices as a card catalog at a

library. In this analogy, every aisle of the library is the equivalent of an isolated information silo. It would be unimaginable to roam the aisles expecting to find a relevant book. Rather, the card catalog provides a user with pointers to the location of books.

Both privacy and security protections are enhanced through this approach to discoverability. Locator and topic information are transferred to the index, but the underlying information isn't transferred until the user requesting it is authorized and authenticated. This decentralized system avoids bulk data transfers minimizing both privacy and security risks. Further, with commercially available technology that allows for removal of personally identifiable information (PII)—so called anonymization—the index can be created without any information that identifies an individual by name or other specific identifier. Therefore, the risk of unintended disclosure of PII contained in the data indices is reduced. Congress should revisit the determination of the Program Manager for the Information Sharing Environment (PM-ISE) that adequate removal of PII via data anonymization is technologically infeasible.

In order to build a system that enables users to discover data elsewhere, each agency's data needs to be tagged at the point of collection with standardized information that can be indexed and searched. Many agencies, however, do not adequately tag and index their data, so it is not readily discoverable, which undermines not only an agency's ability to share the data with others, but also the agency's ability to share within its organization.

The Director of National Intelligence (DNI) has recognized the need for data to be tagged and indexed at the point of collection. The DNI recently signed an Intelligence Community Directive (ICD 501), which establishes policies for discovery that require Intelligence Community (IC) agencies to make all information collected and all analysis produced available for discovery by automated means. ICD 501 is an important step toward increased discovery

because it creates a "responsibility to provide" information. Although ICD 501 tackles a number of hard questions, its implementation presents challenges and many important details need to be resolved. Moreover, ICD 501 only applies to the IC. An effective information sharing framework will require increased discoverability across many federal, state and local agencies.

The Congress and President Obama should place a high priority on discoverability as the first step toward effective information access. The technology is readily available. What is needed now is clear government-wide policy guidance, accountability, and the painstaking work of implementation. The Obama administration should establish a policy obligating all agencies with a national or homeland security mission to make their data discoverable. This policy should require departments and agencies to: (1) tag their data at the point of collection; (2) contribute key categories of data (*e.g.*, names, addresses, passport numbers, etc.) to data indices; and (3) follow through on implementing widely available means to search data indices.

**Authorized Use and Identity Management**. Improved discoverability must go hand in hand with a trusted system that will facilitate access to the data indices and the information these indices point to (in the library analogy, access both to the card catalog and the book itself). An authorized use standard provides a model for building such a trusted system that can overcome some of the systemic challenges of classification, data categorization, and compartmentalization. Under such a standard, data users would be required to provide a predicate in order to access data. To establish a predicate, a federal, state or local user seeking information would need to state a mission- or threat-based need to access the information for a particular purpose. Thus, a fusion center or its employees could obtain mission-based or threat-based permission to discover, access, or share information, as opposed to the current system that relies on place-of-collection rules, US persons status, and originator control limitations.

Congress asked President Bush to consider adoption of an authorized use standard in the 2007 9/11 Commission Recommendations Implementation Act. The PM-ISE's 2008 Feasibility Report discussed what he viewed as potential obstacles to implementation of an authorized use standard. All of the technical objections, however, can be addressed through commercial off-the-shelf technology, which continues to become more widely available, enabling the use of such a standard even in today's environment of multiple and differing authorities and standards.

The Markle Task Force believes that a combination of high-level policy attention from the President and Congress and appropriately deployed technology can allow phased implementation of an authorized use standard. ICD 501 has started the IC down the path toward phased implementation of an authorized use standard. For example, ICD 501 requires that information collected or analysis produced must be available to authorized IC personnel who have a mission need for information and an appropriate security clearance.

The main hurdle that is often asserted as preventing implementation of an authorized use standard is the lack of an effective identity management system—a system that verifies the identity of individuals in a network and controls their access to information by associating user rights and restrictions with each individual and his or her role. The DNI is currently trying to complete the plan for an "Enterprise Architecture" to put technology in place that will enable identity management across all of the IC agencies, which, in turn, will make possible discoverability, disclosure control, and information access.

Overcoming identity management obstacles must be a priority. Technology to implement such a standard is commercially available today and phased implementation should begin now. Using existing technology to create an effective system for identity management will not only help improve information sharing—it will also be an important tool to enhance cybersecurity

because it will identify all data users and, with appropriate protections, flag attempts to go beyond authorized access and use, or to cause damage to systems or information.

Congress has a critical role to play in ensuring effective implementation of authorized use and discoverability. Congress should hold regular hearings to oversee the development of the information sharing framework, including how much data is discoverable and progress toward an authorized use standard. Congress must also adequately fund these efforts.

Enhancing Security and Privacy Protections to Match the Increased Power of Shared Information

Building the information sharing framework should entail the development of new and more powerful privacy protections. As the 9/11 Commission stated, the change in governmental need for information "calls for an enhanced system of checks and balances." No information sharing framework will succeed unless the American people are confident that it will respect their privacy, and the analysts and operatives using the framework have confidence that it protects against inappropriate disclosure. The Markle Task Force believes that the President and Congress should develop clear, detailed, government-wide policies that address the hard questions associated with information sharing and increased use of technological capabilities to collect store, share, and analyze information.

Privacy and security are not a zero-sum game. In developing these government-wide policies, the administration needs to recognize that an effective information sharing framework can enhance both privacy and security simultaneously. From its inception, the Markle Task Force has focused on the "twin objectives" of preventing terrorism through improved information sharing while at the same time preserving and protecting the civil liberties that are a bedrock of our national values. The importance of privacy should not be dismissed as an impediment to security. Indeed, the Markle Task Force's latest report found that many of the

measures that should be taken to improve privacy protections will actually enhance the effectiveness of the information sharing framework by improving the reliability of information.

**Enhanced Information Security**. In a "need to share" culture, greater sharing of sensitive information increases the risk of damaging security breaches. Therefore, increased sharing must be accompanied by protections to assure that information is used appropriately.

Technology already exists that can help create an environment where sharing can increase because users trust the security measures that are in place. Immutable audit logs should be used to protect privacy and security of information. Additionally, regular, automated compliance and behavior audits are an indispensable element of an information sharing framework. Such audit capabilities enable oversight and accountability and are a critical protection against misuse and abuse. Real-time audits of user compliance and behavior and immutable audit logs should be implemented immediately. Such audits and network monitoring will play a key role in efforts on information security and protecting against cyber threats.

**Greater Privacy Protection**. Much more needs to be done to develop policies to assure both the public and government officials that privacy and civil liberties are protected while information is shared. The DNI and several other agencies now have Civil Liberties and/or Privacy Officers, but many agencies do not have clear policies to implement. To date, PM-ISE guidelines and associated documents are more advisory than directive—they tell the agencies that they must address various privacy and security principles, but do not tell them how to do so. The guidelines state, for example, that all agencies must comply with the Privacy Act, but the Privacy Act does not address many of the hard questions surrounding who gets what information for what purpose under what standard of justification. So far, the privacy guidelines issued for the ISE do not require agencies to provide any more protections than they offered before the ISE.

Government-wide, there should be measurable changes. The new administration should promulgate government-wide policies on privacy and civil liberties that provide direction on hard issues and provide consistency, even as they allow agencies the flexibility that their different missions and authorities require. These government-wide policies should address: (1) auditing of both data quality and data flows, (2) enhanced fidelity of watchlists, (3) deployment of access and permissioning systems based on carefully defined missions and authorities, (4) clear predication for collection and retention of data, (5) redress systems that offer a meaningful opportunity to challenge adverse action and that ensure that corrections or qualifications catch up with disseminated data. In addition, agency heads should ensure that Civil Liberties and/or Privacy Officers are engaged at all stages of the policy development and implementation process.

Congress and the President should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Over 19 months ago, Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs.

Commercially available technologies, such as anonymization, strong encryption, and digital rights management, are also critical tools for protecting privacy.

Congress should engage in vigorous oversight with respect to privacy and civil liberties. The Obama administration should fully inform the relevant Committees and appropriately cleared staff of the challenges the government faces as a result of rapidly developing communications technology and of tools the administration is currently employing to collect information, including any new technology that may be needed to adequately collect and analyze information.

***

In conclusion, Mr. Chairman, I appreciate your invitation to appear before this Subcommittee today. This Subcommittee deserves special recognition for the role it has played on these critical issues.

Yet more needs to be done. We are still vulnerable to attack because, despite the information sharing reforms that have taken place, federal, state and local decision makers still need better information to protect the United States. At the same time, privacy and civil liberties are not adequately protected because we don't have detailed government-wide policies in place.

Our nation cannot allow recent reforms or the absence of a new attack on our homeland to lull us into complacency. What America urgently needs is renewed leadership on this issue from Congress, the President, and state and local governments.

The Markle Task Force will continue to work with Congress and the Obama administration to find practical solutions to this critical national security challenge. The Task Force has concrete recommendations for steps that can be taken today to ensure that decision makers at all levels get better information so they can protect the nation.

The threat of terrorism is the impetus for the information sharing framework, yet its value is enhanced knowledge creation to improve decision-making and policy implementation across all levels of government. Improved information sharing can make the government more effective in areas like energy security, bio-defense, and healthcare. There is also a clear connection between cybersecurity and information sharing. The same technology that will help improve information sharing is a critical part of protecting against cyber threats.

It is important to have a public dialogue about the vital issue of information sharing. I would like to thank the Subcommittee for having this hearing to facilitate that discussion. I look forward to working with you and am happy to answer any questions you may have.

Statement of

# The Honorable Benjamin L. Cardin

United States Senator
Maryland
April 21, 2009

---

OPENING STATEMENT SENATOR BENJAMIN L. CARDIN, CHAIRMAN

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

U.S. SENATE JUDICIARY COMMITTEE

HEARING: "PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES: STRATEGIES FOR TERRORISM INFORMATION SHARING"

April 21, 2009

The subcommittee will come to order. Let me note for the record that this is the first subcommittee hearing of the Terrorism and Homeland Security Subcommittee of the Senate Judiciary Committee in the 111th Congress. I am privileged to have been named as chairman of this subcommittee when the Judiciary Committee organized in February.

I want to pay a special tribute to the former chairman of this subcommittee, Senator Feinstein, who has now become the chairman of the Select Committee on Intelligence. Senator Feinstein has served as either chairman or ranking member of this subcommittee since the 105th Congress convened in 1997. I am pleased that she will remain a member of this subcommittee and will continue her valuable contributions to this subcommittee and the full committee.

Senator Feinstein's partner over this many years on the subcommittee is Senator Kyl, the distinguished Minority Whip. Senator Kyl will continue in this Congress as the ranking member of the subcommittee, and I look forward to working with him. I would note that Senator Kyl has also served as either chairman or ranking member of this subcommittee during the same 12 years as Senator Feinstein.

Let me also welcome our new two members of the subcommittee, Senators Wyden and Kaufman.

Our top priority in Congress is to protect the American people, and the primary charge of this subcommittee is to oversee anti-terrorism enforcement and policy. We must make sure that our law enforcement and intelligence professionals have the tools they need at

their disposal to prevent and disrupt terrorist attacks. At the same time, we must insure that our government uses its scare resources wisely, and that it strikes an appropriate balance between national security and protecting civil liberties.

In this Congress the Judiciary Committee will have a full agenda on terrorism issues, under the able leadership of Chairman Leahy. I expect our subcommittee to move forward on renewing parts of the Patriot Act that are due to expire, review the Administration's developing policy toward detainees at Guantanamo Bay, and work to restore the credibility of the Office of Legal Counsel through a review of its opinions on government policies and practices relating to terrorism. Over the next few months I expect the subcommittee to hold hearings on a broad range of issues, including passport fraud, cybersecurity, and biological research security. The subcommittee will also examine laws within its jurisdiction relating to encryption policy, export licensing, and espionage laws.

Today the subcommittee turns its attention to a critical issue that President Obama's Administration is already reviewing: the need to strengthen coordination and information sharing between government agencies charged with preventing and disrupting terrorist attacks inside the United States. As we learned from the 9/11 Commission, several intelligence and law enforcement agencies – at all levels of governments – missed key opportunities to "connect the dots" regarding the years-long plot leading up to the September 11, 2001 terrorist attacks on U.S. soil.

We have made much progress in coordinating our anti-terrorism efforts in the government since the 9/11 attacks, including the creation of the Department of Homeland Security, the Director of National Intelligence, and the National Counter-Terrorism Center. I am concerned, however, that the U.S. Government still does not have in place a comprehensive strategy to overcome bureaucratic hurdles to sharing of information that could prevent a terrorist attack. We still see too many examples of stovepiping of information at one government agency, and a reluctance to release that information to another government agency that has a legitimate need for that information.

At the same time, I remain concerned that the government does not have adequate privacy and civil liberties protections in place when it comes to sharing this sensitive information. The 9/11 Commission reminded us that "the terrorist have used our open society against us. In wartime, government calls for greater powers, and then the need for those powers recedes after the war ends. This struggle will go on. Therefore, while protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right."

We need to insure that our law enforcement and intelligence agencies are focusing their scarce resources on terrorists that are intent on inflicting harm in the United States. In my own state of Maryland, we have seen cases where the Maryland State Police have misused their authority and conducted a 14-month undercover investigation by using confidential informants to infiltrate non-violent peace activist groups. This leads to a chilling effect of the First Amendment rights of Americans, does not make America any safer, and makes citizens more distrustful of the government and less likely to cooperate

with legitimate investigations.

The Maryland General Assembly recently adopted legislation to put restrictions on undercover police surveillance, by requiring a finding of reasonable, articulable suspicion of criminal activity before proceeding. I am also trying to insure that information on these Maryland activists were not improperly entered into federal databases.

Let me highlight one of the 9/11 Commission's recommendations on this point. The Commission found that "as the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared."

The 9/11 Commission concluded that "the choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose that values that we are struggling to defend."

I am pleased that the Administration has already undertaken a comprehensive review of information sharing issues relating to the prevention of terrorist attacks. Specifically, I commend President Obama, Homeland Security Secretary Napolitano, and the Office of the Director of National Intelligence for ordering top-to-bottom reviews of federal agencies efforts to share homeland security intelligence information with their federal, state, local, and private sector counterparts.

I hope that today's hearing will help Congress and the new Administration work together to come up with a common approach that improves information sharing for intelligence information while establishing better guidelines for privacy and civil liberties protection.

Today the subcommittee will hear from a distinguished panel of witnesses on this critical subject. Zoe Baird serves as the President of the Markle Foundation, and also served as the Co-Chair of the Foundation's Task Force on National Security in the Information Age. Her task force issued a March 2009 report on the subject of today's hearing, entitled: "Nation at Risk: Policy Makers Need Better Information to Protect the Country." And I welcome back to the Senate former Senator Slade Gorton of Washington State, who also served as a member of the Markle task force and as a member of the 9/11 Commission.

We will also hear from J. Thomas Manger, the Chief of Police of the Montgomery County Police Department in my home state of Maryland. Chief Manger also serves as the head of the legislative committee for the Major Cities Chiefs Association.

Our final witness is Caroline Fredrickson, the Director of the Washington Office of the American Civil Liberties Union.

Before swearing in the witnesses, let me turn to my ranking member, Senator Kyl, for any comments he would wish to make at this time.

CENTER FOR
DEMOCRACY
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

May 12, 2009

The Honorable Benjamin Cardin
Chairman
Subcommittee on Terrorism and Homeland Security
Senate Committee on the Judiciary
509 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Cardin:

We are pleased to submit this letter for the record of the April 21st Terrorism and Homeland Security Subcommittee hearing on information sharing and civil liberties.

As you noted at the hearing, our national security depends on getting accurate, timely and relevant intelligence to the right personnel. And, as you also stated, any information sharing system must take care to protect civil liberties and preserve public trust. We at CDT strongly agree, and we believe that it is crucial to adopt and implement a set of rules to reliably distinguish between beliefs and lawful activities on the one hand and activities that are truly indicative of terrorist planning on the other.

This fundamental issue – how to conduct domestic intelligence without infringing on legitimate dissent – has been highlighted by recent media coverage of various homeland security intelligence reports, including the report on "rightwing extremism" that leaked from the Department of Homeland Security and the reports from fusion centers in Virginia, Missouri and Texas. In addition, this issue of focusing law enforcement resources on true threats and not on protected political activity was at the heart of the controversy over the Maryland State Police surveillance of anti-death penalty and peace activists in 2005-2006.

The inappropriate surveillance of lawful dissent is especially troubling today because the product of such surveillance can be shared broadly within regional fusion centers, and nationally through the federal government's Information Sharing Environment (ISE). These powerful new mechanisms for sharing and analyzing information broaden civil liberties risks to a national scale. This heightened risk requires heightened oversight by Congress to ensure that surveillance does not chill legitimate political dissent.

To begin to address this issue, we offer the following suggestions: First, we recommend that your subcommittee and other appropriate committees of Congress seek from fusion centers and the Department of Homeland Security information that will help Congress assess the extent to which information about lawful dissent is being collected and shared

in connection with the various domestic intelligence activities. In particular, we suggest that you secure access to of the following key categories of information:

(i) a sampling of the reports that various police departments submit for inclusion in the Suspicious Activity Reports (SARs) system and the SARs reports themselves, which are typically put into the ISE by fusion center analysts and shared widely;
(ii) materials used to train local and state police, fusion center analysts, and DHS personnel about domestic intelligence;
(iii) DHS and fusion center intelligence reports.

Second, we urge you to consider the extent to which the training materials mentioned above can, and should, be made public. Public disclosure would foster an understanding of the extent to which law enforcement officials are being trained to protect lawful dissent. At the April 21st Subcommittee hearing, Ranking Member Kyl identified the training of law enforcement officers and analysts as a key to civil liberties protection. That is certainly true, but only if the officers and analysts are being trained properly and their surveillance activities are consistent with that training. A first step therefore is public scrutiny of those training materials. We also urge you to make public the results of your review of the SARs system and the intelligence reports being produced by federally-supported fusion centers and the DHS.

Finally, we recommend that intelligence reports like the DHS' "Rightwing Extremism" threat assessment should expressly discuss the civil liberties issues and provide explicit instruction on the dangers of using ideology as an indicator of terrorist tendencies. The controversy over Rightwing Extremism report and the reports out of fusion centers in Virginia, Missouri and Texas is rooted in the conflation of innocent activity with terrorist activity. The reports should address that very problem by cautioning law enforcement officials that people should not be put under surveillance solely on account of their ideology, political views, political or religious beliefs, and even radical beliefs. Ideally, the cautionary statement should be tailored to the particular threats addressed in the intelligence report in which the statement appears.

Ultimately, the government, the public and the civil liberties community want the same thing: databases filled with accurate information on real threats, not innocent and Constitutionally-protected activity. The foregoing recommendations, while they do not represent a comprehensive or final response to the problem, would advance that goal. We look forward to working with you on these and other civil liberties issues.

Sincerely,

Leslie Harris

Leslie Harris, President and Chief Executive Officer

Harley Geiger, Staff Counsel

cc: Senators Coburn, Cornyn, Durbin, Feinstein, Hatch, Kaufman, Kohl, Kyl, Schumer, Sessions, Wyden


**Statement of Caroline Fredrickson, Director**

**American Civil Liberties Union Washington Legislative Office**

**On**

**"Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing"**

**Before the Subcommittee on Terrorism and Homeland Security**

**Senate Committee on the Judiciary**

**April 21, 2009**

Good morning Chairman Cardin, Ranking Member Kyl, 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 fifty-three affiliates nationwide, regarding terrorism-related information sharing among federal, state, local and tribal law enforcement. The ACLU recognizes a legitimate need to share lawfully-collected information regarding terrorism and other criminal activity among law enforcement agencies at the federal, state, local and tribal levels in an effective and efficient manner. Improving information sharing sounds like a fine goal in the abstract, but increasing the government's authority to collect and disseminate personally identifiable information about Americans in the absence of reasonable suspicion and a specified law enforcement purpose poses significant risks to our privacy and civil liberties.[1] In our view, any effort to expand information sharing among law enforcement agencies must be accompanied by independent oversight mechanisms and a rigorous set of standards to ensure the use of proper methods, to preserve the privacy of innocent individuals, and to maintain the accuracy and usefulness of the shared information.

The police power to investigate, when combined with the secrecy necessary to protect legitimate law enforcement operations, provides ample opportunity for error and abuse. The potential for abuse expands as the amount of information collected and the number of entities it is shared with increases. By its very nature, criminal intelligence information is often uncorroborated, inadequately vetted and fragmentary. At its worst, it is unreliable, misleading or just plain wrong. Just one thing is certain about 'intelligence:' it is only valuable to our security when it is true. If the information collected and shared among law enforcement agencies is inaccurate or irrelevant to a legitimate law enforcement function, sharing it will not improve security, and very well may damage it. Our concerns about information sharing lie in the details. We want to know what information is being collected, who is collecting it, what is done with the information once it has been collected, what authorities regulate these activities, and who is ultimately responsible for ensuring compliance with applicable federal, state, and local laws?

Our testimony examines historical abuses of police intelligence collection and information sharing practices, the guidelines and regulations implemented to curb this abuse, and the steady erosion of these regulations after the terrorist attacks of September 11, 2001. In just the past few years the ACLU has uncovered numerous examples of abusive police intelligence operations at all levels of government targeting non-violent individuals and organizations engaged in First Amendment-protected activity. These unjustified and unnecessary investigations don't just violate the rights of the individuals involved. They harm security by misdirecting resources away from real threats and by polluting terrorism databases with erroneous information. They damage our democracy by suppressing free expression and chilling participation in the political process. The ACLU urges this Subcommittee to intensify its oversight of information collection and sharing practices at all levels of government and to restore appropriate standards to regulate law enforcement information collection and sharing, both to reduce the instances of abuse and to focus our security resources against real threats.

## I. HISTORY OF ABUSE OF DOMESTIC INTELLIGENCE PROGRAMS

Last year the ACLU of Maryland exposed an extensive Maryland State Police (MSP) spying operation that targeted at least 23 non-violent political advocacy organizations based

solely on the exercise of their members' First Amendment rights.[2] The MSP surveillance activities were aimed at an array of political and religious organizations, including 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. None of the MSP reports from these operations suggested any factual basis to suspect these groups posed any threat to security. Not surprisingly, no criminal activity was discovered during these investigations, some of which lasted as long as 14 months. Despite this lack of evidence, the MSP labeled many of these activists "terrorists," distributed information gathered in their investigations widely among Maryland law enforcement and intelligence agencies – including a local police representative of the FBI's Joint Terrorism Task Force, a National Security Agency security official, and an unnamed military intelligence officer –and uploaded the activists' personal information into a federal drug enforcement and terrorism database.[3] The Department of Homeland Security (DHS) was also involved, collecting and disseminating e-mails from of one of the peace groups to assist the MSP spying operations.[4] From a pure information sharing perspective, this case worked well. But the sharing of such misleading, erroneous and irrelevant information provided no security benefit to the people of Maryland, and only undermined the credibility of state and federal intelligence systems.

Such misguided police activity may seem shocking, but anyone who has studied law enforcement intelligence operations in the United States could have predicted it. History has shown that whenever a law enforcement agency takes on an intelligence gathering mission separate from its criminal justice mission, abuse follows and civil rights suffer. Untethered from a criminal predicate, police agencies begin to target people they feel don't fit in: political protesters, immigrants, and minorities.

During the Cold War, the FBI ran a domestic intelligence/counterintelligence program called COINTELPRO that quickly evolved from a legitimate effort to protect the national security from hostile foreign threats into an effort to suppress domestic political dissent through an array of illegal activities. The Senate Select Committee that investigated COINTELPRO (the "Church Committee") found that a combination of factors led law enforcers to become law breakers, including their perception that traditional law enforcement methods were ineffective in addressing the security threats they faced and their easy access to damaging personal information as a result of the unrestrained collection of domestic intelligence.[5] According to the Church Committee report, these agents saw themselves not just as law enforcement officers, but as "guardians of the status quo" responsible for "upholding decency and established morality, [and] defending the correctness of U.S. foreign policy..."[6] The Committee said the "unexpressed major premise of... COINTELPRO is that the Bureau has a role in maintaining the existing social order, and that its efforts should be aimed toward combating those who threaten that order."[7] In testimony before the Committee, White House liaison Tom Charles Huston, author of the infamous "Huston Plan," explained the hazards of expanding a law enforcement agency's mission beyond law enforcement:

> The risk was that you would get people who would be susceptible to political considerations as opposed to national security considerations, or would construe political considerations to be national security considerations, to move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate.[8]

The FBI used the information it gleaned from these improper investigations not for law enforcement purposes, but to "break up marriages, disrupt meetings, ostracize persons from their professions and provoke target groups into rivalries that might result in deaths."[9] The Church Committee noted that the covert nature of these activities left the targets of this abuse with no protection in the law:

> Intelligence activity... is concealed from its victims and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him.[10]

FBI headquarters opened over 500,000 domestic intelligence files between 1960 and 1974, and created a list of 26,000 individuals who would be "rounded up" in the event of a national emergency.[11]

The abuse of intelligence powers was not limited to federal authorities, however. State and local police forces long maintained political intelligence units (also known as Anti-Subversive Squads, or Red Squads), which illegally spied upon and sabotaged numerous peaceful groups throughout the twentieth century.[12] They often amassed detailed dossiers on political officials and engaged in "disruptive" activities targeting political activists, labor unions, and civil rights advocates, among others. During the 1960's the New York City Police Department's radical squad, known as the Bureau of Special Services (BOSS), opened an average of one thousand political investigations a year, targeting such groups as the ACLU, the National Association for the Advancement of Colored People, and the Congress of Racial Equality.[13] By 1968 BOSS accumulated a master index of over one million individual entries.

## II. REFORM AND REGULATION: FEDERAL, STATE AND LOCAL GUIDELINES

Revelations of these abusive law enforcement intelligence activities during the Watergate era led to a series of reforms. Congress sought to establish a statutory charter delineating the FBI's investigative authorities, as it had for the Central Intelligence Agency. To forestall such legislation, in 1976 Attorney General Edward Levi issued guidelines to regulate the FBI's activities. These "Attorney General Guidelines" (AGG) authorized the FBI to conduct "full" investigations only "on the basis of specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence."[14] The Levi guidelines did include some flexibility to allow the FBI to conduct "preliminary" and "limited" investigations when it had "information or allegations" that were not sufficient to open a full investigation, but these investigations were strictly limited in both time (90 days with the possibility of one 90 day extension) and in the techniques the FBI could employ, and their purpose was "confined to determining whether there is a factual basis for

opening a full investigation." The shortcoming of regulating FBI authority through AGG rather than through statute was that guidelines could be easily amended. Several different sets of guidelines were promulgated and they were altered many times over the ensuing years. In 1983, the "specific and articulable facts" standard was changed to a "reasonable indication" standard, which remained in place until 2002.[15]

The federal government also sought to establish clear guidelines for state and local law enforcement agencies engaged in the collection of criminal intelligence information. In 1979 Title 28, Part 23 of the Code of Federal Regulations was promulgated, requiring 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... systems are not utilized in violation of the privacy and constitutional rights of individuals.[16]

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.[17]

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 Supreme Court had established "reasonable suspicion" as the necessary standard to allow a police officer to stop and frisk an individual for weapons in *Terry v. Ohio* in 1968, so it was a concept police already understood.[18] Over time, "reasonable suspicion" has become universally accepted by law enforcement agencies around the country as the appropriate standard for regulating the intelligence collection activities of law enforcement officers.

The Institute for Intergovernmental Research (IIR), a law enforcement training organization, devotes a website to Part 23 that explains why this decades-old regulation is relevant to today's law enforcement operations:

> The purpose of 28 CFR Part 23 is to ensure the constitutional and privacy rights of individuals. Today's environment of aggressive, proactive information collection and intelligence sharing is very similar to the environment that motivated Congress, in the Justice Systems Improvement Act of 1979, to require the issuance of 28 CFR Part 23 in the first place.[19]

The Association of Law Enforcement Intelligence Units called Part 23 "a valuable guide for all agencies with a criminal intelligence function, regardless of their funding sources."[20]

## III. EROSION OF RELIABLE STANDARDS

### A. AUTHORIZATION OF SURVEILLANCE WITHOUT SUSPICION

After the terrorist attacks of September 11, 2001, law enforcement agencies at all levels of government abandoned the traditional criminal justice approach in favor of an intelligence model. The federal government initiated a series of broad electronic surveillance and data collection programs based not on reasonable suspicion, but on an unproven theory that threats to our security could be detected and countered through massive data collection coupled with predictive data mining technology. Some of these efforts were authorized by Congress, while others were not.

Through the USA Patriot Act, for example, Congress expanded the FBI's authority to use National Security Letters (NSLs) to obtain telephone, credit and financial information so that these secret demands for information could be used against not just suspected terrorists or agents of foreign powers, but against anyone "relevant" to an FBI investigation.[21] Not surprisingly, a 2007 audit by the Department of Justice Inspector General confirmed widespread FBI mismanagement, misuse and abuse of this unchecked authority.[22] The audit revealed that the FBI managed its use of NSLs so negligently that it literally did not know how many NSLs it had issued. The IG found that FBI agents repeatedly ignored or confused the requirements of the NSL authorizing statutes, and used NSLs to collect private information against individuals two or three times removed from the subjects of FBI investigations. Twenty-two percent of the audited files contained unreported legal violations.[23] Most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[24]

In 2008, the IG released a second audit report covering the FBI's use of NSLs in 2006 and evaluating the reforms implemented by the DOJ and the FBI after the first audit was released.[25] The new report identified many of the same problems discovered in the earlier audit. The 2008 NSL report showed that the FBI issued 49,425 NSLs in 2006 (a 4.7 percent increase over 2005), and confirmed the FBI was increasingly using NSLs to gather information on U.S. persons (57 percent in 2006, up from 53 percent in 2005).[26] The 2008 IG audit also revealed that high-ranking FBI officials improperly issued eleven "blanket NSLs" in 2006 seeking data on 3,860 telephone numbers.[27] None of these "blanket NSLs" complied with FBI policy and eight imposed unlawful non-disclosure requirements on recipients.[28] Moreover, these "blanket NSLs" were allegedly written to "cover information already acquired through exigent letters and other informal responses," which seemed to indicate intentional misconduct.[29]

But NSLs weren't the only surveillance authority abused. In December of 2005 the *New York Times* revealed that shortly after the 9/11 attacks the National Security Agency (NSA) began conducting warrantless domestic eavesdropping in violation of the Foreign Intelligence Surveillance Act.[30] Subsequent articles in *USAToday* alleged that major telecommunications companies "working under contract to the NSA" also provided the government domestic call

data from millions of Americans for "social network analysis."[31] Congress expanded the government's authority to eavesdrop on international communications without particularized suspicion, but a recent article in the *New York Times* revealed the NSA exceeded even those broad limits.[32]

Yet the information collected with these NSA warrantless wiretapping programs was reported to be of little value to FBI agents investigating terrorism.[33] Data produced by the Executive Office for United States Attorneys and analyzed by the Transactional Records Access Clearinghouse (TRAC) shows that from 2002 to 2008, as these surveillance programs increased, prosecutions of FBI international terrorism cases steadily dropped.[34] Perhaps more critical to evaluating the effectiveness of post-9/11 surveillance programs, however, is DOJ's increasing tendency to refuse to prosecute FBI international terrorism investigations. In 2006, the DOJ declined to prosecute a shocking 87% of the international terrorism cases the FBI referred for prosecution. Considering that only a tiny fraction of the many thousands of terrorism investigations the FBI opens each year are even referred for prosecution, it has become clear that the vast majority of the FBI's terrorism-related investigative activity is completely for naught – yet the FBI keeps all of the personally identifiable information it collects through these dubious investigations forever.[35]

Like so many of the broad information collection programs the intelligence community instituted over the last eight years,[36] these unfocused, ineffective collection programs appear to have been premised on the idea that data mining tools could later be developed to find meaning in these vast pools of collected information. A recent National Research Council study funded by the Department of Homeland Security calls this premise into serious question, however, and may explain why these programs do not seem to have produced demonstrable results. The study concluded:

> 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.[37]

B. AMENDING THE ATTORNEY GENERAL GUIDELINES

The AGG underwent four separate changes under the Bush administration alone.[38] Attorney General John Ashcroft first amended the guidelines in 2002 to expand the investigative techniques the FBI could use during preliminary inquiries, and to increase the time limits to 180 days with the possibility of two or more 90 day extensions. [39] Under the Ashcroft guidelines only mail openings and non-consensual electronic surveillance were prohibited during preliminary inquiries, meaning the FBI could conduct intrusive investigations of people for an entire year without facts and circumstances establishing a "reasonable indication" that the subjects were engaged in criminal activity. The Ashcroft guidelines also allowed FBI agents to "visit any place and attend any event that is open to the public, on the same terms and conditions

as members of the public generally." The FBI later claimed this authority did not require the FBI agents attending public meetings to identify themselves as government officials. Abuse quickly followed. In 2005 the IG audited the FBI's compliance with AG Guidelines and found significant deficiencies: 53 % of the audited preliminary inquiries that extended beyond the initial 180-day authorization period did not contain necessary documentation authorizing the extension, and 77% of those that extended past the first 90-day extension period lacked the required authorizations. The IG audit was unable to determine whether or how frequently agents attended public events, however, because the FBI failed to keep records of such activity.

One illustration of the excess of the Ashcroft guidelines is that all of the investigative activity known to have taken place during the MSP spying operations targeting peaceful advocacy organizations would arguably have been authorized in preliminary inquiries conducted under the Ashcroft guidelines. There is no evidence the MSP opened mail or engaged in non-consensual electronic monitoring during their investigations, which were the only prohibited investigative techniques in preliminary inquiries. The only constraint in the Ashcroft guidelines that could have prevented a spying operation like the one the MSP conducted was the requirement of "information or an allegation which indicates the possibility of criminal activity." This slight factual prerequisite was the only limitation protecting innocent Americans from a year or more of intense FBI scrutiny.

Unfortunately, the FBI was not content with such excessive power and in December 2008, Attorney General Michael Mukasey instituted new guidelines that authorized the FBI to conduct intrusive "assessments" without requiring any factual predicate to justify an investigation. The Mukasey guidelines allow the FBI to utilize a number of intrusive investigative techniques during assessments, including physical surveillance, retrieving data from commercial databases, recruiting and tasking informants to attend meetings under false pretenses, and engaging in "pretext" interviews in which FBI agents misrepresent their identities in order to elicit information. These "assessments" can even be conducted against an individual simply to determine if he or she would be a suitable FBI informant. Nothing in the new Guidelines protects entirely innocent Americans from being thoroughly investigated by the FBI. The new Guidelines explicitly authorize the surveillance and infiltration of peaceful advocacy groups in advance of demonstrations, and they do not clearly prohibit using race, religion, or national origin as factors in initiating assessments.

C. TURNING STATE AND LOCAL POLICE INTO INTELLIGENCE AGENTS

State and local law enforcement also moved away from traditional law enforcement during this period and embraced a concept called intelligence-led policing (ILP). ILP focuses on the gathering and analysis of "intelligence" in the pursuit of proactive strategies "geared toward crime control *and quality of life issues* (emphasis added)."[40] One law enforcement official described ILP as policing that is "robust enough" to resist "terrorism as well as crime *and disorder* (emphasis added)."[41] If this language is eerily reminiscent of the rhetoric FBI agents used to defend COINTELPRO, it should not be surprising. Just last month at a hearing on Homeland Security Intelligence in the House of Representatives, Commerce, Georgia Chief of Police John Gaissert testified: "The street cop isn't looking for the normal. He's looking for the

abnormal."[42] The tendency for law enforcement to see the outsider as a potential threat has not diminished with the passage of time.

This new theory of criminal intelligence 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.[43]

In case the implications for civil liberties were not obvious enough, the Chief of the Lexana, Kansas Police Department described how she uses ILP programs to improve community awareness:

> Here in Lexana we have incorporated this element into our Crime Resistant Community Policing Program. We conduct regular trainings with the maintenance and rental staffs of apartment complexes, motels, and storage facilities. We show them how to spot and identify things *like printed terrorist materials and propaganda* and unique weapons of mass destruction like suicide bomb vests and briefcases (emphasis added).[44]

ILP did more than just train motel maids in Kansas to identify terrorist propaganda; it introduced a new institution into American life: the intelligence fusion center. Fusion centers are a direct institutional outgrowth of ILP, which promotes information collection and sharing as a strategy for preventative law enforcement, emphasizing the use of data mining technology in order to find patterns of potential criminal or terrorist behavior in a community. Intelligence fusion centers grew in popularity among state and local law enforcement officers as they sought to establish a role in defending homeland security by developing their own intelligence capabilities. These centers evolved largely independently of one another, beginning in about 2003, and were originally tailored to meet local and regional needs.

This growth took place in the absence of any legal framework for regulating fusion centers' activities. This lack of regulation quickly led to "mission creep," in which fusion centers originally justified as anti-terrorism initiatives rapidly drifted toward an "all-crimes, all-hazards" policy "flexible enough for use in all emergencies."[45] The leadership at some fusion centers has admitted that they switched to an "all-hazards" approach so they could apply for a broader range of grants, and because there was far too little terrorism-related information to analyze:

> [I]t was impossible to create 'buy in' amongst local law enforcement agencies and other public sectors if a fusion center was solely focused on counterterrorism, as the center's partners often didn't feel threatened by terrorism, nor did they think that their community would produce would-be terrorists.[46]

An intelligence capability without a well-defined mission is an unnecessary risk to liberty.

As fusion centers proliferated, national efforts at bolstering, defining and standardizing these institutions on the part of governors and the federal government began to intensify.[47] The federal government began providing facilities, manpower and financial resources to fuel the growth of these state and local intelligence centers. In 2006, the Departments of Justice and Homeland Security produced a report, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," (the FC Guidelines) which outlined the federal government's vision for the centers, and sought to encourage and systematize their growth. "Intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center uses a common set of guidelines," the agencies proclaimed.[48] The FC Guidelines defined a fusion center as a "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[49] These goals are laudable and appropriate for any law enforcement intelligence operation, as we all want the police to protect us from criminals and terrorists. But the voluntary federal guidelines then go on to encourage fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[50]

The FC Guidelines envision fusion centers doing more than simply sharing legitimately acquired law enforcement information across different levels of government. They encourage fusion centers to compile data "from nontraditional sources, such as public safety entities and private sector organizations" and combine it with federal intelligence produced by the federal intelligence community "to anticipate, identify, prevent, and/or monitor criminal and terrorist activity."[51] At a fusion center, threat assessments and information related to public safety, law enforcement, public health, social services and public works could be 'fused' with federal data containing personally identifiable information whenever a "threat, criminal predicate, or public safety need is identified."[52] The FC Guidelines also encourage fusion centers to invite a wide range of public safety, public works, social services, and private sector entities to participate, and some fusion centers include National Guardsmen as well as active duty military personnel.

D. FAILURE TO ENFORCE EXISTING REGULATIONS

Such broad information collection and dissemination would obviously exceed the limitations imposed by 28 C.F.R. Part 23. Yet the federal government actively encourages the violation of the regulation. The FCG encourage fusion centers to broaden their sources of data "beyond criminal intelligence, to include federal intelligence as well as public and private sector data."[53] Rather than being constrained by the law regarding what they can collect, Delaware State Police Captain Bill Harris, head of the Delaware Information Analysis Center (DIAC), appeared to feel constrained only by resources: "I don't want to say it's unlimited, but the ceiling is very high... When we have the money, we'll start going to those other agencies and say, 'Are you willing to share that database and what would it cost.'"[54] The federal official in charge of the High Intensity Drug Trafficking Area Task Force that controlled the database in which the MSP placed erroneous information about the peaceful activists they spied on later said it was up

to the participating state and local agencies to monitor their own compliance with the federal regulation.[55]

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.[56] 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.[57] 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 federal regulations. 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 secret intelligence operations.

And unfortunately, rather than cooperate with one another, the various federal intelligence agencies still seem to compete. Though the Intelligence Reform and Terrorism Prevention Act of 2004 established the ODNI ISE as the primary mechanism for the sharing of terrorism information, homeland security information, and law enforcement information among federal departments and agencies, state, local, and tribal governments, and private sector entities, the FBI recently introduced its own network for sharing suspicious activity reports from state and local law enforcement, eGuardian.[58] As it stands now there are several avenues 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 now eGuardian systems, and the Homeland Secure Information Network (HSIN) to name just a few. 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 of the privacy and liberties of ordinary Americans. Indeed, the FBI appears to want to bend the rules in order to collect more information than the other systems. FBI documents distributed at the 2009 National Fusion Center Conference misstate federal regulations by asserting "[i]nformation that is deemed inconclusive will be maintained in eGuardian for a maximum of five years in accordance with 28 Code of Federal Regulations (CFR) Part 23." Of course the regulation does not allow for the collection or retention of "inconclusive" information for any period of time. This Subcommittee should examine all these information sharing programs closely, assess whether they demonstrably improve security, and ensure that they operate in a manner that complies with the law and protects individual rights before authorizing federal resources to support them.

IV. EVIDENCE OF ABUSE

The erosion of reasonable limits on police powers has set the stage for a return of the abusive practices of the past. In recent years the ACLU has uncovered substantial evidence that domestic intelligence powers are being misused at all levels of government to target non-violent political activists. In addition to the abusive MSP investigations discovered by the ACLU of Maryland, the ACLU of Colorado uncovered illegal surveillance of peaceful protestors and environmental activists by the Denver Police and the FBI,[59] and the ACLU of Northern California produced a report of widespread illegal spying activities by federal, state and local officials.[60] ACLU Freedom of Information Act litigation revealed JTTF investigations targeting peace activists in Pennsylvania and Georgia, and Department of Defense intelligence operations targeting anti-military protestors from around the country.[61]

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,[62] particularly because DHS representatives had previously denied that DHS had any information regarding the MSP investigations targeting these protesters.[63] 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 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."[64]

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."[65] 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.

The MSP case wasn't the only evidence of abuse in DHS programs. An assessment published by DHS this month warned that right-wing extremists might recruit and radicalize "disgruntled military veterans,"[66] and an 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."[67] 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 our limited security resources to generate such intelligence products – and yet these events continue to occur.

The ACLU has also produced two reports detailing problems at intelligence fusion centers.[68] Since these reports were published 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.[69] The same month, but on the other side of the political spectrum, a Missouri Fusion Center released a report on "the modern militia movement" that claimed militia members are "usually supporters" of presidential candidates Ron Paul and Bob Barr.[70] In March 2008 the Virginia Fusion Center issued a terrorism threat assessment that described the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats. These bulletins, which are widely distributed, would be laughable except that they come with the imprimatur of a federally-backed intelligence operation, and they encourage law enforcement officers to monitor the activities of political activists and racial and religious minorities.

What is clear is that these abusive intelligence reports do nothing to improve security. Sharing misleading information about the ideologies and activities of non-violent groups only undermines public support for law enforcement. FBI tactics targeting Arab and Muslim-Americans have so alienated the community that advocacy organizations that once teamed with the FBI threatened to end their cooperation with outreach efforts.[71]

## V. RECOMMENDATIONS

1. Congress must intensify its oversight of all government information collection and sharing practices that implicate the rights of Americans. The collection and sharing of personally identifiable information about Americans pose serious risks to liberty and democracy, and the evidence of abuse is overwhelming. Past 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.[72] It turns out, not surprisingly, that spying on innocent people is not useful to uncovering true threats to security. Unfortunately these lessons were ignored and we are increasingly seeing a return to abusive intelligence operations that target protest groups

and religious and racial minorities. Congress should examine and evaluate all information collection and sharing practices and bring an end to any government activities that are illegal, ineffective or prone to abuse. Three Patriot Act-related surveillance provisions expire at the end of this year, which gives Congress the opportunity to conduct a comprehensive review of all expanded post-9/11 intelligence authorities.[73]

2. Congress should not implement or fund new intelligence programs without empirical evidence that they effectively improve security. We should not sacrifice our liberty for the illusion of security. Fusion centers, in particular, should be audited to determine whether they can effectively serve a legitimate law enforcement function without violating the rights of innocent Americans. Any new effort to expand information sharing among law enforcement agencies must be accompanied by independent oversight mechanisms and a rigorous set of standards to ensure the use of proper methods, to preserve the privacy of innocent individuals, and to maintain the accuracy and usefulness of the shared information. Congress should review the National Research Council findings regarding the ineffectiveness of data mining as a counterterrorism tool, and should ban information collection programs that rely on data mining technology.

3. Congress should codify relevant portions of 28 C.F.R. Part 23 to establish a reasonable suspicion standard for all criminal intelligence information collection programs and to limit dissemination absent a legitimate law enforcement need. Reforms instituted after the exposure of abusive law enforcement intelligence programs were designed not only to protect the rights of innocent Americans, but also to help our law enforcement and intelligence agencies become more effective by focusing their resources on people they reasonably suspected of wrongdoing. Dissemination of criminal intelligence information to non-law enforcement entities should be prohibited unless necessary to avoid imminent danger to life or property. Congress should also provide a remedy for individuals who are harmed by intelligence activities conducted in violation of the regulatory standards.

4. Congress should ban racial profiling in all government intelligence and law enforcement programs and enact a legislative charter delineating the FBI's investigative authority. The statute should require a factual predicate establishing a reasonable suspicion that a person or organization is or will engage in illegal activity before the FBI may employ investigative techniques that implicate the privacy and civil rights of U.S. persons.

VI. CONCLUSION

While effective and efficient information sharing among law enforcement agencies is an important goal, we must remember that 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. Establishing new information collection and sharing authorities for the federal, state and local law enforcement poses significant risks to our individual liberties, our democratic principles and, ironically, even our security, particularly when fulfilling a broad and unfocused "all crimes, all hazards"[74] mandate. 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.[75] Congress should examine and evaluate all government intelligence and information sharing programs regularly and withhold funding from any activities that are unnecessary, ineffective or prone to abuse.

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 the abuse of these law enforcement authorities to spy on peaceful advocacy organizations. As the Supreme Court warned, "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power."[76]

---

[1] The Government Accountability Office defined the term "personally identifiable information" as "any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual." *See* GOVERNMENT ACCOUNTABILITY OFFICE, GAO 08-343, REPORT TO CONGRESSIONAL REQUESTERS: INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, 5, n. 9, (Jan. 2008), *available at* http://www.gao.gov/new.items/d08343.pdf.

[2] *See,* ACLU of Maryland "Stop Spying" info page, http://www.aclu-md.org/Index%20content/NoSpying/NoSpying.html (last visited Apr. 15, 2009).

[3] MSP submitted the information to the Washington-Baltimore High Intensity Drug Trafficking Area Task Force (HIDTA) database. HIDTA is a federal program that provides funding and support to participating law enforcement agencies to support regional counter-drug and counter-terrorism efforts. *See*, 21 U.S.C. §1706 (2006).

[4] 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.

[5] 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, at 10 (1976).

[6] *Id.*, at 7.

[7] *Id.,* at 7.

[8] *Id.*, at 27.

[9] 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 II), S. Rep. No. 94-755, at 5, (1976).

[10] *Id.*, at 2-3.

[11] *Id.*, at 6-7.

[12] *See*, FRANK DONNER, PROTECTORS OF PRIVILEGE: RED SQUADS AND POLICE REPRESSION IN URBAN AMERICA (1990).

[13] *See*, Arthur N. Eisenberg, New York Civil Liberties Union, Testimony Before The New York Advisory Committee To The U.S. Commission On Civil Rights: Police Surveillance of Political Activity -- The History and Current State of the *Handschu* Decree (May 21, 2003), *available at* http://www.nyclu.org/node/731.

[14] FBI Statutory Charter: Hearings Before the Senate Committee on the Judiciary, 95th Cong. Pt. 1, at 22, (Apr. 20 and 25, 1978).

[15] FBI Domestic Security Guidelines: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 98th Cong. 67-85 (1983).

[16] 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).

[17] *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.

[18] 392 U.S. 1 (1968).

[19] Institute for Intergovernmental Research, Frequently Asked Questions, http://www.iir.com/28cfr/FAQ.htm.

[20] Letter from Russell M. Porter, General Chairman, Association of Law Enforcement Intelligence Units to Michael Dever, Department of Justice Office of Justice Programs, Comments on proposed amendments to 28 Code of Federal Regulations Part 23, OJP Docket No. 1473, (Sept. 1, 2008), (on file with author).

[21] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act) of 2001, Section 505, Pub. L. No. 107-56, 115 Stat. 272 (2001). The four NSL authorizing statutes include the Electronic Communications Privacy Act, 18 U.S.C. § 2709 (2000), the Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2000), and the National Security Act of 1947, 50 U.S.C. § 436(a)(1)(2000).

[22] DEP'T 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 [hereinafter 2007 NSL Report].

[23] 2007 NSL Report, *supra* note 22, at 84.

[24] 2007 NSL Report, *supra* note 22, at 86-99.

[25] DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (Mar. 2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf [hereinafter 2008 NSL Report].

[26] 2008 NSL Report, *supra* note 25, at 9.

[27] 2008 NSL Report, *supra* note 25, at 127, 129 n.116.

[28] 2008 NSL Report, *supra* note 25, at 127.

[29] 2008 NSL Report, *supra* note 25, at 127.

[30] James Risen and Eric Lichtblau, *Bush lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200.

[31] Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USATODAY, May 11, 2006, at 1A, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[32] Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 15, 2009, at A1, *available at http://www.nytimes.com/2009/04/16/us/16nsa.html*.

[33] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta, Jr., Spy *Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1, *available at* http://www.nytimes.com/2006/01/17/politics/17spy.html?ei=5090&en=f3247cd88fa84898&ex=1295154000&pagewanted=print.

[34] *See*, TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, NATIONAL PROFILE AND ENFORCEMENT: TRENDS OVER TIME (2006), http://trac.syr.edu/tracfbi/newfindings/current/ (last visited Apr. 15, 2009); Todd Lochner, *Sound and Fury: Perpetual Prosecution and Department of Justice Antiterrorism Efforts*, 30 LAW & POLICY 168, 179 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109250.

[35] *See*, TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, NATIONAL PROFILE AND ENFORCEMENT: TRENDS OVER TIME (2006), http://trac.syr.edu/tracfbi/newfindings/current/ (last visited Apr. 15, 2009); Todd Lochner, *Sound and Fury: Perpetual Prosecution and Department of Justice Antiterrorism Efforts*, 30 LAW & POLICY 168, 179 (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109250.

[36] 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.

[37] 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.

[38] For a detailed analysis of the changes to the AGG over time, *See*, DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, THE FEDERAL BUREAU OF INVESTIGATION'S COMPLIANCE WITH ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES (2005), *available at* http://www.usdoj.gov/oig/special/0509/final.pdf.
[39] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations, (May 30, 2002), available at: http://www.ignet.gov/pande/standards/prgexhibitg.pdf
[40] DEMOCRATIC STAFF OF THE H.R. COMM. ON HOMELAND SECURITY, 110TH CONG., LEAP: A LAW ENFORCEMENT ASSISTANCE AND PARTNERSHIP STRATEGY, PREPARED AT THE REQUEST OF CONGRESSMAN BENNIE G. THOMPSON, RANKING MEMBER 5 (2006), http://hsc-democrats.house.gov/SiteDocuments/20060927193035-23713.pdf.
[41] *Id.* at 5 (quoting Michael Downing, Commander, Los Angeles Police Department Counterterrorism/Criminal Intelligence Bureau).
[42] *Homeland Security Intelligence: Its Relevance and Limitations: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. 8 (March 18, 2009) (Testimony of John Gaissert, Chief of Police, Commerce Police Department, Commerce, Georgia).
[43] 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.
[44] *Id.*, at 6 (quoting Chief Ellen Hanson of the City of Lexana, Kansas Police Department).
[45] TODD MASSE, SIOBHAN O'NEIL AND JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT FOR CONGRESS: FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS at 22 n.60, (July 6, 2007) [hereinafter CRS Fusion Center Report].
[46] CRS Fusion Center Report, *supra*, note 45, at 21.
[47] CRS Fusion Center Report, supra note 45, at 18-19.
[48] BUREAU OF JUSTICE ASSISTANCE, OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T. OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA, at iii, (Aug. 2006) [hereinafter Guidelines].
[49] Guidelines, *supra* note 48, at 2.
[50] CRS Fusion Center Report, *supra* note 45, at 1.
[51] Guidelines, *supra* note 48, at 13.
[52] Guidelines, *supra* note 48, at 13.
[53] CRS Fusion Center Report, *supra* note 45, at 1.
[54] Mike Chalmers and Lee Williams, *Intelligence Facility Casts a Wide Net*, THE NEWS JOURNAL, May 7, 2007, http://www.delawareonline.com/apps/pbcs.dll/article?AID=/20070507/NEWS/705070333.
[55] Shaun Waterman, *Analysis: Md. Spy Charges Prompt Review, United Press International*, MIDDLE EAST TIMES (July 24, 2008), http://www.metimes.com/Security/2008/07/24/analysis_md_spy_charges_prompt_review/4743/.
[56] Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0, ISE-FS-200, (Jan. 25, 2008) (on file with authors).
[57] *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.
[58] IRTPA, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[59] The Denver Police Spy Files, ACLU of Colorado, http://www.aclu-co.org/spyfiles/fbifiles.htm (last visited Apr. 15, 2009).
[60] MARK SCHLOSBERG, STATE OF SURVEILLANCE: GOVERNMENT MONITORING OF POLITICAL ACTIVITY IN NORTHERN AND CENTRAL CALIFORNIA, ACLU OF NORTHERN CALIFORNIA (July 2006), *available at* http://www.aclunc.org/issues/government_surveillance/asset_upload_file714_3255.pdf.
[61] Faces of Surveillance: Targets of Illegal Spying, ACLU Website, http://www.aclu.org/safefree/general/24287res20060227.html (last visited Apr. 15, 2009).
[62] 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.
[63] 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).
[64] Maryland State Police Intelligence File on the D.C. Anti-War Network (DAWN), 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).

[65] 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.
[66] *See,* U.S. Dep't of Homeland Security, Assessment: Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment (Apr. 7, 2009), *available at* http://wnd.com/images/dhs-rightwing-extremism.pdf.
[67] 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.
[68] MICHAEL GERMAN AND JAY STANLEY, WHAT'S WRONG WITH FUSION CENTERS? AMERICAN CIVIL LIBERTIES UNION (Dec. 2007), http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf; 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.
[69] 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.
[70] T.J. Greaney, *'Fusion Center' Data Draws Fire over Assertions*, COLOMBIA DAILY TRIBUNE, (March 14, 2009), *available at* http://www.columbiatribune.com/news/2009/mar/14/fusion-center-data-draws-fire-over-assertions/.
[71] Alexandra Marks, *FBI and American Muslims at Odds*, CHRISTIAN SCIENCE MONITOR, March 25, 2009, *available at* http://www.csmonitor.com/2009/0325/p02s01-ussc.html.
[72] 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).
[73] *See*, MIKE GERMAN AND MICHELLE RICHARDSON, RECLAIMING PATRIOTISM: A CALL TO RECONSIDER THE PATRIOT ACT, AMERICAN CIVIL LIBERTIES UNION (MARCH 2009), *available at* http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf.
[74] 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.
[75] *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.
[76] United States v. United States Dist. Court *(Keith)*, 407 U.S. 297, 314 (1972).

**Testimony**
**Slade Gorton**[1]
**Subcommittee on Terrorism and Homeland Security of the Senate Judiciary Committee**
April 21, 2009

I would like to thank Chairman Cardin and Ranking Member Kyl for holding this hearing and taking the initiative to improve information sharing by dedicating their time and energy to this critical issue. Making information sharing a top priority is essential to safeguard our national and homeland security. Improved information sharing can provide decision makers at all levels of government better information in order to protect the country. Whether the question is Iran's nuclear activities, biosecurity or a potential cyber attack on vital computer networks, federal, state and local government personnel across agencies must collaborate and share information to identify, understand, and respond to evolving security threats.

The 9/11 Commission, of which I was a member, identified ten lost "operational opportunities" to derail the 9/11 attacks—and each involved a failure to share information. If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have connected the dots.

The Congress and the President should reaffirm information sharing as a top priority by providing sustained leadership from the top and ensuring accountability throughout the government. This Subcommittee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing and that urgency does not wane. Otherwise, the United States will not be prepared to confront the threats of the 21st century.

[1] Senator Gorton served in the United States Senate for 18 years representing Washington state and currently practices law at K&L Gates LLP.

The Markle Foundation Task Force on National Security in the Information Age, on which I have had the privilege of serving since its inception, recently released a report[2] that found that, over seven years after the September 11th attacks, the United States remains at risk. Policy makers, from the President to local police chiefs, still need better information to defend our homeland. Such information should be available in time-critical situations and in ways that are tailored to facilitate decision-making and action at all levels of federal, state, and local government.

Building an information sharing framework that can provide better information to decision-makers requires the new administration and Congress to follow through with the hard work of implementation and to overcome the turf wars that stymie progress. The 111th Congress and President Obama should ensure accountability, sweep away bureaucratic resistance to information sharing, and foster an open debate about how best to achieve the twin goals of national security and protection of civil liberties.

Unfortunately, the sense of urgency on information sharing has diminished in the seven years since the 9/11 attacks. Each new problem our country confronts pushes information sharing further down the priority list.

The good news, to date, is that the required laws have been passed, and the Members of this Subcommittee deserve special recognition for the role they have played in those reforms. Specifically:

- The Congress and President Bush have acted on many of the recommendations of the 9/11 Commission, the WMD Commission, and the Markle Task Force, which informed both Commission reports.

[2] *Nation at Risk: Policy Makers Need Better Information to Protect the Country* (2009). All of the Markle Task Force's reports are available at http://www.markle.org/.

- Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 and the 9/11 Commission Recommendations Implementation Act of 2007, which required transformation of the intelligence community to achieve information sharing.
- Pursuant to the 2004 law, President Bush, the Program Manager for the Information Sharing Environment (PM-ISE), the Director of National Intelligence (DNI), and others have issued initial policy guidance reflecting the new "need to share" or "responsibility to provide" principle.

The Information Sharing Environment (ISE) created by Congress was intended to change the way government conducts the business of policy making based on information gathered. The legislation intended a "virtual reorganization of government" allowing communities of interest to work on common problems across agency boundaries and between federal, state and local governments, and the private sector—wherever important information could be found.

As a former Attorney General of Washington, I understand the important role state and local law enforcement play. A cop on the beat in Seattle may have information that can stop the next attack, but he needs to know what to look for and how to report it. To keep our country safe, information must be shared effectively, not only within the intelligence community and among federal agencies, but among federal, state, and local governments and with key private sector partners.

Yet old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. Cultural, institutional, and perceived technological obstacles have slowed the implementation of laws intended to facilitate the flow of information and create new ways of collaborating.

Much more needs to be done. The Department of Homeland Security and the Federal Bureau of Investigation have engaged state and local law enforcement through fusion centers, but both the role and future of these centers are uncertain and the sharing of information with them has been uneven. While the National Counter Terrorism Center (NCTC) and the

Office of the Director of National Intelligence (ODNI)—and to some extent the wider Intelligence Community (IC)—have made significant progress on information sharing, their work is far from complete. A 2008 review by the Inspector General of the 500 Day ODNI Plan indicated that the IC still has a long way to go on collaboration and information sharing.[3] Information sharing outside the IC—as well as information sharing across the law enforcement, domestic intelligence, and foreign intelligence communities—remains problematic. So, too, is information sharing related to US persons.

Information-sharing practices are still a hodge-podge because too much discretion has been left to each agency. While Congress and the Executive Branch have generally set out the basic policy structure for an effective information sharing framework, the Executive Branch should give agencies government-wide policy guidance on hard issues such as privacy, identity management, discoverability, and authorization. Congress should also engage in vigorous oversight to measure progress and create accountability.

Now is the moment for breakthrough progress on information sharing. Action at the start of the new administration is required. It is much better to remodel the house right the first time rather than remodeling it later.

The Markle Task Force takes heart from recent actions:

- First, the previous DNI, Admiral McConnell, signed a new Intelligence Community Directive (ICD 501) on January 21, 2009 mandating wide-ranging actions to promote information sharing, including the ability to discover and request information from all IC elements, who now have a "responsibility to provide" such information.
- Second, the Secretary of the Department of Homeland Security issued an Action Directive on State and local information sharing on her first day in office, calling for "an evaluation

[3] See *Follow-up Report of the 500 Day Plan, Part 2*, available at http://www.dni.gov/500-day-plan/500%20Day%20Plan%20Follow%20Up%20Report%20part%202.pdf.

of which activities hold the most promise for achieving the smooth flow of information on a real-time basis."

- Third, the President has affirmed the need to establish an integrated, effective and efficient approach to address 21st century threats. In *Presidential Study Directive 1*, he has called upon the Homeland Security and Counter-Terrorism Assistant to the President to review how to strengthen interagency coordination of the full range of homeland security and counterterrorism policies, including information sharing.
- Fourth, the administration has embraced information technology—and technology is now widely available both to help solve the hard issues mentioned above and to protect civil liberties.

The President has called for a new way of doing business. In light of the current financial crisis and growing budget pressures, we need to do more with less. An effective information sharing framework is not only important to protect against terrorism; it will make the government more effective in areas like energy security, bio-defense, and healthcare as well.

It is time to reaffirm our nation's commitment to improving information sharing by accelerating implementation of the laws and policies Congress put in place to shift government from a "need to know" to a "need to share" paradigm. One example of an important step toward reaffirming information sharing as a top priority is moving the PM-ISE into the Executive Office of the President (EOP), as discussed in detail below.

Overcoming persistent barriers to information sharing requires strong, sustained leadership from the top and accountability throughout the government. Therefore, I would like to take this opportunity to discuss two key elements of the Markle Task Force's latest report: (1) reaffirming information sharing as a top priority, and (2) transforming the information sharing culture with metrics and incentives.

Reaffirming Information Sharing as a Top Priority

While initial steps by the new administration are promising, the 111th Congress, President Obama, Secretary Napolitano, Director of National Intelligence Dennis Blair, and Attorney

General Eric Holder should provide strong, sustained leadership to reaffirm information sharing as a top priority. A waning sense of urgency in the seven years since the 9/11 attacks means that old habits of withholding information are returning. Top down leadership, to reaffirm the importance of information sharing, is necessary. Congress should conduct robust oversight and the President should convene a Cabinet meeting to affirm information sharing as a top priority and to help overcome the bureaucratic resistance and turf wars that stymie progress.

**Moving the PM-ISE into the EOP**. One important way to reaffirm this issue as a top priority would be for President Obama to move the Program Manager for the Information Sharing Environment into the Executive Office of the President. The reason for such a move is clear. It will enable the PM-ISE to carry out its statutorily required government-wide authority[4] to coordinate the policies and procedures necessary for an effective information sharing framework, and give the PM-ISE White House backing to carry out its mission. Currently, the PM-ISE lacks policy clout and is seen (incorrectly) as an adjunct to the intelligence community. Elevating the PM-ISE into the EOP will ensure that the PM-ISE is able to coordinate across federal, state and local agencies effectively in order to improve the way our government shares information.

I am also sensitive to Congress' concern that the PM-ISE be responsive to congressional oversight. Congressional oversight is essential to the success of information sharing, as emphasized later in my testimony.

Regardless of where the PM-ISE is situated, the President should ensure that it is fully integrated into, and has a lead role in coordinating, all information sharing policy development

---

[4] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004), states that the PM-ISE is "responsible for information sharing across the Federal Government" and that he "shall have and exercise government wide authority."

and implementation across the government, including the intelligence, law enforcement, and homeland security communities. Otherwise, wasteful duplicate efforts are inevitable as individual agencies try to address information sharing independently. This approach is a more efficient and effective way of governing, consistent with President Obama's efforts to change the way government does business.

**Ordering a High-Level Review**. The President should also order an initial 60-day high-level review of the current policy and privacy guidelines and processes for the ISE. The Markle Task Force's discussions with senior officials revealed that departments and agencies have widely differing priorities and perspectives with respect to information sharing. President Obama should also demand an assessment of the state of the ISE on an annual basis thereafter, in order to ensure government-wide focus and coordination. The administration should release public reports on the results of its 60-day review, the status of implementation, and each annual review. Congress should hold hearings on the 60-day review and on each annual report to assure that information sharing remains a high national priority.

As part of this 60-day review, the new administration should apply ISE best practices to areas of national and homeland security concern in addition to terrorism, such as cybersecurity, nuclear proliferation, energy security, and climate change. To date, the ISE has been used primarily to facilitate the flow of terrorism-related information.

Congress and the new administration should also focus directly on the overlapping worlds of law enforcement and domestic intelligence, because the sharing of information between the law enforcement community and the intelligence community—a major lapse on 9/11—remains a critical challenge. Tension persists between the intelligence and law enforcement communities and concern exists on both sides that "the wall" may be creeping up

again. The Markle Task Force encourages continued work on robust pilots that test concepts that could improve the way the two communities work together. Such pilots have reportedly been very successful in resolving information sharing disputes, and some are still underway. The Obama administration should establish a review process to transfer best practices from successful pilots to the broader intelligence and law enforcement communities.

Congress has a vital leadership role to play that can help ensure that improving information sharing remains a top priority. This Subcommittee should keep the pressure on the administration to implement the information sharing reforms in recent legislation. The oversight process can help ensure that the individuals charged with making information sharing a reality are held accountable for producing measurable progress toward a safer country.

Transforming the Information Sharing Culture with Metrics and Incentives

Sustained leadership from the top is essential, but the President and Congress cannot implement an effective information sharing framework alone. The Congress and President Obama should ensure accountability throughout the government in order to follow through with the hard work of implementation and overcoming bureaucratic resistance to information sharing.

The Markle Task Force's recent report recommends specific metrics that help Congress measure progress so it can perform its oversight function and the report puts forth a series of practical incentives that will help the Obama administration transform the culture and reduce resistance to information sharing.

**Improved Metrics**. Mission-oriented metrics are necessary to change the "need to know" culture that persists in many agencies. Past Markle Task Force reports discussed the need to establish performance metrics and self-enforcing milestones for the information sharing

framework. In our second report,[5] for instance, we provided a detailed set of questions Congress and others could use to evaluate progress made on information sharing and analysis. These 24 questions focused on whether:

- Roles, responsibilities and authorities were clarified.
- Progress was made to remove roadblocks to sharing information within the federal government.
- Intelligence was produced for a set of new customers.
- Communications and sharing was being promoted with state and local governments and the private sector.
- Overall analysis was improved.
- The capabilities of state, local and private sector entities were being improved.

Congress should develop key questions in order to evaluate and measure agencies' performance in meeting essential information sharing and analysis objectives. Once established, these metrics should be incorporated as part of the regular annual review of information sharing.

One of the first metrics should focus on discoverability (the ability of users to discover data that exists elsewhere) because data indices are necessary to enable an effective information access framework. This metric should measure what percentage of an agency's data holdings have been registered in the data indices directory. If you think of data indices as a card catalog at a library where every aisle of the library is the equivalent of an isolated information silo, this metric would measure how many of the library books have a card in the card catalog. This could be accompanied by ongoing tests across organizations on how the ISE scores according to certain critical system requirements (akin to the Quality Assurance scenarios used in the private sector).

---

[5] Markle Task Force report *Creating a Trusted Network for Homeland Security* (2003), page 26, Exhibit F.

**Accountability and Transparency**. Once improved metrics are in place, agencies should be held accountable for reaching certain benchmarks or milestones. Congress and the administration should couple program funding with how well that program increases discoverability. Programs that do not make their information discoverable by putting their data in the index should get less funding. This type of financial accountability is logical because data held by a system that is not discoverable to other federal, state, and local agencies is less useful and less valuable. This system of discovery metrics and accountability would significantly reduce the voluntary aspect of exposing select data with data indices, and can help Congress carryout effective oversight by providing clear information about who is contributing the most to the shared library and whose data is most useful.

Agency level accountability should also be accompanied by individual accountability. Penalties should be widely known, proportionate to the misuse or failure to share, and applied consistently. Field officers, mid-level analysts, and state and local actors should have a special confidential channel to call senior leadership's attention to their belief that critical information is not being shared. This channel would send a clear message of individual accountability—that information sharing is not someone else's responsibility, but critical to the mission and part of everyone's job.

**Driving Cultural Change with Performance Incentives and Training**. Individual performance incentives and training are two important tools that can change agency culture in favor of information sharing. The government has put in place some training and policies to institutionalize sharing incentives, but implementation at the agency level is lacking. For example, the PM-ISE issued a plan in 2006 requiring that agencies develop the following:

- Tailored training programs based on their unique business processes, missions, program, and policy needs.
- A core training module that will serve as the common educational baseline for the ISE.
- Incentives to adopt the ISE culture that hold personnel accountable for the improved and increased sharing of information.

Based on agency self-reporting, the PM-ISE found in June 2008 that fewer than 50 percent of agencies had adopted such training programs and personnel incentives. Moreover, there has been little assessment of the quality of any of the programs the agencies have adopted. PM-ISE guidance released on September 24, 2008 aims to make information sharing a factor in annual performance appraisals for employees of agencies that are members of the Information Sharing Council and others who handle terrorism-related information. The ODNI is still working on uniform training across the IC elements and on adding information sharing as a factor in performance evaluations throughout the IC.

Congress and the Obama administration should focus on improving incentives to share information because such incentives can accelerate cultural change where the "need to share" or "responsibility to provide" culture has not fully taken root. Many individuals still perceive risk and penalties for sharing information that might later be claimed to have been unauthorized or ill advised. They believe they are more likely to get in trouble for sharing too much information than too little.

Three specific examples of incentives and training that could drive cultural change are:

- Integrating information sharing into performance reviews and budget and personnel resource allocations for all agencies that have a national security mission.

- Creating an information sharing award. This award should be given to the federal, state or local agency or unit within an agency that has been most successful at making its data discoverable. This award would highlight the overall value of information sharing to national and homeland security, and help facilitate the necessary culture shift.

- Increasing joint duty in the IC, in order to build a sense of trust and community. As in the military, the IC is instituting the practice that promotion to senior levels requires a tour of duty at another agency. A broader concept of joint duty, especially among mid-level employees, will foster a sense of community that is not narrowly focused on each agency's separate mission.

The heart of the matter is for employees at every level to understand why information sharing is valuable to *them*. Information sharing works well in Iraq and Afghanistan because the sense of shared mission is great. The Obama administration should take these lessons learned in the field and make them work back home.

***

In conclusion, Mr. Chairman, Senator Kyl, thank you for the opportunity to appear before this Subcommittee today. I hope my comments have helped give you a clearer idea of steps that can be taken to reaffirm information sharing as a top priority and to ensure accountability throughout the government. Congress' oversight role in this area is crucial.

I commend this Subcommittee for its leadership on these issues. Sustained leadership is vital because a waning sense of urgency in the seven years since the 9/11 attacks means that old habits of withholding information are returning. The United States must not become complacent about improving information sharing in the face of the current financial crisis and in the absence of a new attack. Your leadership on this issue can ensure accountability, sweep away bureaucratic resistance, and foster an open debate.

I applaud the Subcommittee for having this hearing today. I am happy to answer any questions you may have.

**STATEMENT OF SENATOR JON KYL**
**HEARING BEFORE THE JUDICIARY SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY**
**"PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES:**
**STRATEGIES FOR TERRORISM INFORMATION SHARING"**
**21 APRIL 2009**

## Introduction

At the outset, I would like to congratulate Senator Cardin on becoming the chairman of the Subcommittee on Terrorism and Homeland Security. Senator Feinstein and I worked together for a dozen years on the subcommittee. During that time, we switched positions as chair and ranking member a number of times; but, as we often said, it was a relatively seamless transition because we worked together so closely, forging a bipartisan approach to a variety of issues within the subcommittee's jurisdiction.[1] I look forward to having an equally productive working relationship with Senator Cardin.

I would like to thank Senator Cardin for convening today's hearing on information sharing and for planning an upcoming hearing on passport fraud.

## Information Sharing

As I mentioned, the subcommittee has convened today to investigate the current state of information sharing among federal, state, and local intelligence and law enforcement agencies. This is an important issue because it directly affects our nation's ability to respond to ongoing threats, such as radical Islamists and the drug trafficking organizations that operate along our southern border.

---

[1] *See, e.g., Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (Mar. 21, 2007) (S. Hrg. 110-62, Serial No. J-110-22), at 1 (statement of Dianne Feinstein) ("He has been Chair more than I have, but, of course, I hope to change that record. But we have been able to work very well together over these many years, and I appreciate that so much."); *Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 110th Cong., 1st Sess. (May 2, 2007) (S. Hrg. 110-103, Serial No. J-110-32), at 4 (statement of Jon Kyl) ("Madam Chairman, thank you, and let me begin by thanking you for holding this hearing. First let me say that I agree with everything you have said. This is a bipartisan issue. We have worked in this Subcommittee in a very constructive and bipartisan way now for over 12 years, and it is a pleasure always to work with you, now to be your wing man now that the political tables are slightly turned here. It does not make any difference in this Subcommittee.").

The need for improved communication among our nation's intelligence and law enforcement agencies was highlighted by the 9/11 Commission, which "identified a breakdown in information sharing as a key factor contributing to the failure to prevent the September 11, 2001 attacks."[2] In response, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, thereby establishing an Information Sharing Environment (ISE) to serve as a "trusted partnership among all levels of government in the United States, the private sector, and our foreign partners" in order to prevent further attacks through "the effective and efficient sharing of terrorism and homeland security information."[3]

On July 23, 2008, the Government Accountability Office provided testimony before the Senate Homeland Security and Governmental Affairs Committee about improvements to our nation's terrorism-related information sharing capability since the establishment of the Information Sharing Environment. According to GAO, "in the wake of 9/11 . . . agencies at the federal, state, and local levels are taking steps to better share information about possible terrorist threats."[4] The GAO further stated, however, that "there is still important and critical work left to do," which includes integrating various information sharing "changes and initiatives into a set of functioning policies, processes, and procedures for sharing; continuing to break down agency stovepipes and cultures that promoted protection over sharing; monitoring and measuring progress; and maintaining momentum."[5]

**Conclusion**

I look forward to hearing from today's witnesses. I would like to extend a special welcome to Senator Slade Gorton, a former colleague respected by people on both sides

[2] http://www.ise.gov/pages/vision.html.
[3] http://www.ise.gov/pages/vision.html.
[4] http://www.gao.gov/new.items/d08637t.pdf, at 1.
[5] http://www.gao.gov/new.items/d08637t.pdf, at 1.

of the aisle for his thoughtfulness and expertise. He has testified before this subcommittee in the past,[6] and we are always pleased to hear his views.

In conclusion, I would like to work with Chairman Cardin and interested parties to improve our nation's information sharing capability, which will in turn assist our intelligence and law enforcement agencies in responding to ongoing threat posed by terrorist and criminal organizations.

[6] *Terrorism: Emergency Preparedness: Hearing before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 109th Cong., 1st Sess. (Oct. 26, 2005) (S. Hrg. 109-222, Serial No. J-109-46).

THOMAS MANGER TESTIMONY:

Chairman Cardin, Ranking member Kyl, distinguished members of the Committee ...

I appreciate the invitation to be here this afternoon speaking on behalf of the Major Cities Chiefs of Police, representing the 56 largest police departments in the United States.

I am pleased to report that the relationships and information-sharing between and among federal, state local and tribal police has never been better. But the rest of the story remains that there is still a great deal more to do to fully engage the more than 18,000 law enforcement agencies in this country as full partners in the quest for homeland security.

Federal agencies, despite their ever-improving efforts, have still yet to completely leverage the vast resources of our nation's police and sheriffs.

Since 9/11, the FBI and the Department of Homeland Security—and all other agencies included in the intelligence community—have made tremendous progress in incorporating state, local and tribal LENF into the national effort to protect our homeland.

But as with any effort so monumental ... any effort that has achieved progress so quickly, we need to take a good, long look at what has been created and make certain that what we have is what we intended. Keep what is working and build on it. Eliminate duplicative efforts and fix what is not working as it should.

The areas of oversight for this subcommittee are far-reaching and critical. But because my time here is limited, I want to focus on just a limited number of topic areas. I will focus on the role of local (1) law enforcement in homeland security; (2) several systems in place to facilitate the exchange of information; (3) establishing and maintaining safeguard of everyone's privacy and civil liberties; and (4) finally some shortcomings from the perspective of local law enforcement.

Law enforcement's role in uncovering and disrupting terrorist activities is well documented. Sergeant Robert Fromme from the Iredell County (North Carolina) Sheriff's Office saw two men enter a discount tobacco shop with over $20,000 cash in a plastic grocery bag. These men came into the shop almost daily buying many cartons of cigarettes. Fast-forward several years and the ATF and FBI indicted 26 individuals who were using proceeds from criminal

activity to fund a terrorist group based in Lebanon. A suspicious activity noted by local LENF, appropriately documented and legally investigated, results in a terrorist operation being shut down.

This type of story is repeated over and over again because of the relationships and information-sharing mechanisms in place within this nation's LENF community.

I think everyone would agree that the key lesson that 9/11 taught us is that law enforcement is more effective when relationships, protocols, and information-exchange systems are established and in place ***before*** a crisis strikes.

The national Suspicious Activity Report System (or SARS) is an effort still in its infancy that needs to be invested in and allowed to grow.

The SARS process has directly enhanced the ability of local police to protect our communities from violent crime including terrorism. And most important, the SARS process can and will be done in a manner that protects the privacy, civil liberties and civil rights of all.

The two greatest values of SARS are:

(1) the ability to connect events that in the past would never have been connected;

(2) it is a nationwide initiative that for the first time is providing consistent criteria and consistent training to all law enforcement personnel.

We are training our first responders how to identify behaviors associated with terrorism-related crime, and providing them training they need to distinguish between behaviors that are reasonably associated with criminal activity and those that are not.

No police chief wants his officers involved in confrontational interactions with people engaged in innocent, constitutionally protected behavior.

Not every person wearing baggy pants is a gang-banger and not every person videotaping the Washington Monument is a terrorist.

Public safety is not enhanced and homeland security is not increased by filling databases with information about people, organizations and activities that have no nexus to criminal activity or terrorism.

I firmly believe that the SARS system can operate with strong protections for privacy and civil liberties while it provides the nation's best practice for information-sharing among LENF agencies. JTTFs and fusion centers can also operate effectively with these protections. From a local perspective, involvement in JTTFs and fusion centers remains the most effective way to stay on top of the latest terrorist-threat information.

Unfortunately, one of the harshest realities remains that unless a police agency is capable of assigning someone to the local JTTF, or a state or local fusion center, that agency is likely to get its most timely threat information from the media. The days when CNN had information before most police chiefs are still all too common.

The Montgomery County Police Department, like many large agencies, has the resources to assign our own personnel to FBI's JTTF and two fusion centers. We have personnel assigned to the Maryland Coordination and Analysis Center (MCAC) and the Washington, D.C., Regional Threat and Analysis Center.

While there is some overlap in the intelligence and threat information we receive from these three operations, at any given time one center will have information that is of interest to

Montgomery County that no one else has. By virtue of our proximity to the nation's capital, it is best that we be plugged in to all three sources. It is staff-intensive and highlights the importance for the federal funding of intelligence analysts that work for state and local agencies.

It should also be noted that Northern Virginia has a well-established fusion center (the R.I.C.). Some might see three separate fusion centers within 20 miles of each other and wonder about duplication of effort. It is simply a reality that each fusion center puts an emphasis on different—albeit some overlapping—geographic areas. None of these fusion centers would be as effective or focused if they were combined, in my view.

The good news is that they are talking to one another and the coordination efforts taking place at the federal level continue to expand and mature. It is important to reiterate an earlier statement. Let's identify what is working and build on it.

Another area that has been a long-term issue is the need for a nationwide system for federal security clearances.

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.

Another issue involves the sharing of some information with the JTTFs. While fusion centers allow law enforcement agencies to share information generally, there is a problem when the information goes through the vetting process at the JTTF. If the FBI decides to enter the information into the Guardian system for further investigation by the JTTF, the information immediately becomes classified, thus limiting access to the information.

So if, for example, a Guardian lead is investigated involving fraudulent identifications—and it is later determined that the individuals involved have no nexus to terrorism—the lead is then closed. Local police, however, may be interested in working the case from a local-crime perspective. Unfortunately, the information gathered by the JTTF remains classified and often unavailable to local police. These issues require continued work between the FBI and local authorities.

I know I've reached the end of my time before you, so let me summarize ...

SARS is working ... let's find ways to get it fully implemented around the nation—the training, the accountability, the technology.

Fusion centers are working ... let's ensure safeguards are in place to protect our civil liberties and that all centers are equipped to combat both crime and terrorism. Done legally and done effectively, these centers have been responsible for the arrests of bank robbers, criminal street-gang members, money launderers, copper thieves, and terrorists. The cases were made because multiple jurisdictions quickly linked crimes, patterns and

individuals involved in criminal wrongdoing. The value of fusion centers is the information they put out to all stakeholders.

Every local police or sheriff's department has the particular mission of protecting neighborhoods ... protecting communities from crime and terrorism. Cops on the street are uniquely positioned to receive and document information from a variety of sources that could assist the federal government maintaining our homeland security.

We have systems in place to facilitate the sharing of that information ... let's make sure all agencies are plugged in. We have systems in place to facilitate the sharing of that information ... let's ensure effective analytic capability so that we don't go down the wrong road.

We have systems in place to facilitate the sharing of that information ... let's establish safeguards so that information is used appropriately and hold people accountable.

We have systems in place to facilitate the sharing of that information ... fund these systems and allow them to mature and improve.

It will make our neighborhoods safer and homeland more secure. God bless the United States of America.

# # #

JTM:mam