RECOMMENDATIONS OF THE 9/11 COMMISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

AUGUST 23, 2004

Serial No. 115

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

95–499 PDF WASHINGTON : 2004

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

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

TOM FEENEY, Florida
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
MARK GREEN, Wisconsin
RIC KELLER, Florida
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia

ROBERT C. SCOTT, Virginia
ADAM B. SCHIFF, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts

JAY APPERSON, *Chief Counsel*
ELIZABETH SOKUL, *Counsel*
KATY CROOKS, *Counsel*
JASON CERVENAK, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

AUGUST 23, 2004

OPENING STATEMENT

	Page
The Honorable Howard Coble, a Representative in Congress From the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	1
The Honorable Robert C. Scott, a Representative in Congress From the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security	2

WITNESSES

Mr. Christopher Kojm, Deputy Executive Director, National Commission on Terrorist Attacks Upon the United States ("9/11 Commission")	
Oral Testimony	5
Prepared Statement	7
Mr. John S. Pistole, Executive Assistant Director, Counterterrorism/Counterintelligence, Federal Bureau of Investigation	
Oral Testimony	13
Prepared Statement	15
Mr. John O. Brennan, Director, Terrorist Threat Integration Center	
Oral Testimony	19
Prepared Statement	20
Mr. Gregory T. Nojeim, Associate Director and Chief Legislative Counsel, American Civil Liberties Union	
Oral Testimony	21
Prepared Statement	23

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement by the Honorable Steve Chabot, a Representative in Congress From the State of Ohio	69
News Article: "Terror No-Fly Lists: Tough to Get Off"	70
News Article: "Science Seen As Slipping"	72
Prepared Statement from the Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas	77
Letter from Gregory T. Nojeim, along with Report by the Electronic Privacy Information Center	87
Questions and Responses for the Record from Mr. Chris Kojm	106
Questions and Responses for the Record from Mr. John S. Pistole	107
Questions and Repsonses for the Record from Mr. John O. Brennan	111

RECOMMENDATIONS OF THE 9/11 COMMISSION

MONDAY, AUGUST 23, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:02 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. Today the Subcommittee on the Judiciary of Crime, Terrorism, and Homeland Security convenes a very important hearing on the report released last month by the National Commission on terrorist attacks upon the United States, the 9/11 Commission.

Considerable time has been spent already by this Subcommittee as well as other Committees of the House of Representatives, and by our colleagues in the Senate as well, on attempting to conclude or figure out what went wrong and why the attacks of September 11, 2001, were able to be carried out with such apparent ease. Today's hearing will focus on some of the specific recommendations that were offered by the Commission and upon where we are in terms of implementing these recommendations.

To assist us in our examination, we have a distinguished panel of witnesses today from the 9/11 Commission itself and from some of the agencies that play a major role in the war on terror and that are directly impacted by some of the proposed recommendations.

I am pleased to say that some of the much needed change, reform, and restructuring has already begun, and in fact substantial measures have been undertaken within some of these agencies long before the 9/11 Commission concluded its work. Before we go any further, I would be remiss if I did not thank the members of the Commission for their tedious, thorough, and quite extraordinary work.

I would also like to thank our witnesses and the agencies they represent for embracing the work of the Commission as the incredible—at the incredible opportunity that it is, an opportunity to take a learned input from outside experts and implement or supplement meaningful change. As the Commission found, our Government intelligence apparatus was of Cold War vintage in desperate need of an upgrade. Our numerous intelligence and law enforcement agencies were not communicating with each other the way they should

and perhaps we as a Government were not as focused on the things we should have been—upon which we should have been focused.

With the release of their report and the knowledge that we as legislators have gained from the many hearings and briefings that the Congress has had on the topics of terrorism and intelligence since the events of September 11, 2001, we must look forward. We must ensure that consistent with our oversight responsibilities of the Department of Justice and the Department of Homeland Security, we do everything possible to define an old axiom: We must do everything possible to ensure that history does not repeat itself.

As this will most certainly not be the last visit that we pay to these witnesses or to this topic, today's hearing will focus primarily on the 9/11 Commission's recommendations regarding the creation of a national intelligence director, the need for more secure borders, the need to prevent identity theft and fraud, the need to target the networks that provide material support for terrorists, and the need to create a specialized and integrated national security workforce at the FBI.

Additionally we will hear about the recommendations that have already been implemented or are about to be implemented by the entities represented here today.

Before I introduce our distinguished Ranking Member let me depart from the opening statement just a minute. It is my belief, gentlemen and ladies, that when these people came on 9/11, they wanted to destroy us. But failing to do that, I think one of their asides was to frustrate our day-to-day living. And they have succeeded in spades. One of our salient features as a society since its inception has been Americans' eager willingness to embrace strangers, for example. Now we're very tentative about that, very guarded. I recall, as do you all, the anticipation with which families would examine rail or train ride or fly across the country. Now it's tentatively guarded. So that's where we are now.

I am pleased to have the gentlelady from Texas and the gentleman from Florida with us today. I am going to confine opening statements to the Chairman and the Ranking Member and all other Members will be permitted to have their statements included in the record.

I am now pleased to recognize the distinguished gentleman from Virginia, the Ranking Member of this Subcommittee, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. And thank you for holding the hearing on the 9/11 Commission report recommendations which fall under the jurisdiction of this Subcommittee. The Commission's report represents a reasonable blueprint for what must be done to better secure our Nation against terrorist attack. I am pleased to see that the Commission strongly reaffirmed that securing America does not and must not require sacrificing our civil liberties. Indeed, the Commission confirmed that we can be safe and free. Otherwise we run the risk of doing to ourselves what the terrorists were seeking to do, destroying or eroding our freedoms upon which this country was founded.

I believe that we can implement the substance of all of the recommendations of the Commission, although we should develop them in a planner which maximizes the threat of all of our agen-

cies to contribute their best in the fight against terrorism. But as those agencies address the threat of terrorism, we must not diminish their ability to fulfill their traditional missions and we must not sacrifice our civil liberties. And this is especially true with law enforcement agencies.

We should also be mindful that the investigation of the 9/11 attacks reveal that we had gathered plenty of information on the hijackers which, if used properly, could have stopped most of them, if not all of them. Accordingly, it appears that our intelligence gathering system may have worked reasonably well. It is the analysis and use function that failed us. And while we consider new ways of analyzing, collecting, and sharing intelligence across the Intelligence Community, we have to consider all those techniques affect constitutionally-based standards of domestic law enforcement. This is particularly important when we consider that the report calls for a further relaxation of the traditional wall of separation between foreign and domestic intelligence gathering. The standards for foreign intelligence are significantly lower than the standards for domestic intelligence. Although we must permit the appropriate sharing of intelligence across the intelligence spectrum, we must not allow foreign intelligence gathering techniques and uses to be applied against Americans at home.

Now, it is important to note, Mr. Chairman, that at last week's hearing with the Constitution Subcommittee and the Administrative Law Subcommittee, one of the commissioners indicated that the recommendations on new powers were intended to apply to terrorism cases, and not just generally. I think that's important, because when we passed the USA PATRIOT Act, the new powers were not restricted to terrorism cases.

The report recommends that Congress better organize its oversight and intelligence and counterintelligence functions by consolidating the oversight into a single entity in each Chamber. Now, coordination of oversight functions by various Committees with jurisdiction over homeland security is vitally important. We must avoid, however, weakening or watering down the oversight function. The different Committees in Congress have different areas of expertise. One oversight Committee could not possibly be expected to have the expertise in constitutional law and international relations, and health issues covered by the Centers for Disease Control. We need to take advantage of the expertise on all of our Committees and Subcommittees.

So I look forward to the testimony of our witnesses on how we might best proceed with implementing the recommendations of the 9/11 Commission to ensure that we are putting forth our best effort to prevent and address terrorist threats against this country. I look forward to working with you, Mr. Chairman, as we implement the recommendations which fall under the jurisdiction of this sub-Committee. I yield back.

Mr. COBLE. Thank you Mr. Scott.

Mr. COBLE. And we have been joined by the gentleman from Ohio, Mr. Chabot. Mr. Chabot, you may present your opening statement in the record.

[The information referred to follows in the Appendix]

Mr. Coble. I am now pleased to introduce our distinguished panel. And before I do that, let me say this. It serves no good purpose, I think, to point accusatory fingers, because many people were to blame. Mistakes occurred in the Clinton administration, mistakes have occurred during the Bush administration. Mistakes have occurred in the Intelligence Community. I think what we need to learn is try to see to it that they don't recur. And hopefully we will have some input from you all today.

Our first witness today is Mr. Christopher Kojm, the Deputy Executive Director of the 9/11 Commission. Mr. Kojm served on the staff of the House Committee on International Relations from 1984 to 1998 as director of the Democratic staff that is coordinator for regional issues. In addition, prior to joining the Commission, he served for 5 years as Deputy Assistant Secretary for Intelligence Policy and Coordination at the State Department. Mr. Kojm received a master's in public affairs from Princeton University and an A.B. from Harvard College.

Mr. Kojm, I notice your first alma mater has been recognized as the top university in the country. I think they shared that with Harvard—I guess both your alma maters were at the top of the heap. So congratulations to you. If you will, Mr. Kojm, convey our good wishes to Governor Kean and to former Congressman Lee Hamilton. I think they did a good job in guiding this 9/11 Commission through what at times I am sure must have appeared to have been shoals and rocks and reefs.

Our second witness is Mr. John Pistole who serves as the Executive Assistant Director of Counterterrorism and Counterintelligence at the FBI. Mr. Pistole commenced his career with the FBI as a special agent in 1983. Subsequently he served in various posts in Minneapolis, New York, Indianapolis, Boston, and the FBI headquarters. Prior to assuming his current position in December 2003, he served as Assistant Director at the Counterterrorism Division.

We also have with us today Mr. John Brennan, the Director of the Terrorist Threat Integration Center. Mr. Brennan commenced his career as an intelligence officer with the CIA in 1980. He served in many capacities within the CIA, including as daily intelligence briefer at the White House in 1994 and 95, and as chief of station in the Middle East from 1996 to 1999. He served as DCI Tenet's chief of staff for 2 years, prior to having been appointed Deputy Executive Director in March of 2001. Mr. Brennan earned his B.A. from Fordham University and his M.A. in government from the University of Texas at Austin.

Our final witness today, Mr. Gregory Nojeim, the Associate Director and Chief Legislative Counsel of the American Civil Liberties Union. Mr. Nojeim joined the ACLU in 1995 and has been responsible for analyzing the civil liberties and implications of Federal legislation regarding terrorism, national security, immigration and informational privacy. Prior to joining the ACLU, he was director of legal services of the American Arab Anti-discrimination Committee for 4 years, and as an attorney for Kirkpatrick and Lockhart for 5 year. Mr. Nojeim received his undergraduate degree from the University of Rochester and his J.D. from the University of Virginia.

I apologize to you all for having singled out Mr. Kojm's alma maters, but I don't believe your alma maters nor mine made that final cut.

So, Mr. Kojm, we're glad to have you kick it off. Gentleman, traditionally we operate under the 5-minute rule. When you see that red light on the panel before you, that means that you are skating on eternally thin ice. And we will not buggy-whip you, but that's the time to wind down. And we impose the 5-minute rule against ourselves as well when we're questioning you. So if you could keep your answers terse, we would appreciate that.

Mr. COBLE. Mr. Kojm.

TESTIMONY OF CHRISTOPHER KOJM, DEPUTY EXECUTIVE DIRECTOR, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Mr. KOJM. Mr. Chairman——

Mr. COBLE. I stand corrected. Our Chairman—traditionally we swear in all of our witnesses appearing before us. So if you all would please stand and raise your right hand.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative. Please be seated. Mr. Kojm, you will start.

Mr. KOJM. Mr. Chairman, Ranking Member Scott, distinguished Members of the Judiciary Committee, it is an honor to appear before you today. I want to thank the Chairman for his insightful comments and I certainly do thank the Chair and Ranking Member for their expertise and their statements of support for the Commission's work. I appreciate it.

The 9/11 Commission is grateful to you and to the leadership of the House for your prompt consideration of the report and recommendations of the Commission. As you know, the Commission's findings and recommendations were strongly endorsed by all commissioners, five Republicans and five Democrats who have been active in the public life of our Nation. In these difficult times and in an election year, this unanimity, we believe, is remarkable and important. It reflects a unity of purpose to make our country safer and more secure in the face of the threat posed by international terrorism. The Commission calls upon the Congress and the Administration to respond to our report in the same spirit of bipartisanship.

Mr. Chairman, you have asked the Commission to present its recommendations related to the Federal Bureau of Investigation on the topic of border security and the creation of a center for counterterrorism and the national intelligence director. All topics are treated in the written statement and I will confine my opening remarks to the FBI.

The FBI for the past several decades performed two important but related functions. First, it serves as our premier Federal law enforcement agency investigating possible violations of Federal criminal statutes and working with Federal prosecutors to develop and bring cases against violators of those laws.

Second, it is an important member of the Intelligence Community, collecting information on foreign intelligence or terrorist ac-

tivities within the United States. That information can be used either for additional counterintelligence or counterterrorism investigations or to bring criminal prosecutions.

We focused on the FBI's performance as an intelligence agency combating the al Qaeda threat within the United States before 9/11. Like the Joint Inquiry of the Senate and House Intelligence Committees before us, we found that performance seriously deficient. Director Freeh did make counterterrorism a priority in the 1990's. And Dale Watson, his counterterrorism chief, made valiant and substantial efforts to communicate that priority to agents in the field, but that priority did not effectively find its way into the daily work of the FBI's field offices, nor did it result in the creation of a corps of intelligence officers and analysts with the professional qualifications and skills needed for an effective intelligence counterterrorism operation.

Finally, when FBI agents did develop important information about possible terrorist-related activities, that information often did not get effectively communicated either within the FBI itself or in the Intelligence Community as a whole. Within the FBI itself, communication of important information was hampered by the traditional case-oriented approach of the Agency and the possessive case-file mentality of FBI agents. This Committee is only too familiar with the information technology problems that have long hampered the FBI's ability to know what it knows.

Even when information was communicated from the field to headquarters, it did not always come to the attention of the director or other top officials who should have seen it. This was the case in the now famous incidents in the summer of 2001 of the Phoenix electronic communication about Middle Eastern immigrants in flight schools and the Minneapolis field office's report to headquarters about the arrest of Zacarias Moussaoui.

The other internal barrier to communication of intelligence information between FBI intelligence officials and FBI criminal agents and the Federal prosecutors was the wall between intelligence and law enforcement that developed in the 1980's and was reinforced in the 1990's. Through a combination of court decisions, pronouncements from the Department of Justice and its Office of Intelligence Policy and Review, and risk-averse interpretations of those pronouncements by the FBI, the flow of information between the intelligence and criminal sides of the FBI and the Justice Department was significantly restricted.

This phenomenon continued until after 9/11 when the Congress enacted the USA PATRIOT Act and when the Justice Department successfully appealed a FISA court decision that had effectively reinstated the wall. These failures in internal communications were exacerbated by a reluctance of the FBI to share information with sister agencies in the Intelligence Community, with the National Security Council, and with State and local law enforcement agencies. This culture of nonsharing was by no means unique to the FBI, but the FBI was surely one of the worst offenders in this regard.

The FBI under the leadership of its current director, Robert Mueller, has undertaken significant reforms to try to deal with these deficiencies and build a strong capability in intelligence and

counterterrorism. It's certainly our distinct analysis and impression that Director Mueller has made very important reforms. We believe they are all in the right direction. But he and the Agency certainly have a long way to go.

And let me conclude, Mr. Chairman, by saying that what the Commission recommends is that further steps be taken by the President, the Justice Department, and the FBI itself to build upon Director Mueller's reforms that have been undertaken and to institutionalize these reforms so that the FBI is transformed into an effective intelligence and counterterrorism agency. The goal, as our report states, is to create within the FBI a specialized and integrated national security workforce of agents, analysts, linguists, and surveillance specialists who create a new FBI culture of expertise and national security and intelligence.

In closing, Mr. Chairman, this Committee will have a vital oversight role in monitoring the progress by the FBI and ensuring that this new capacity, so critical to our Nation, is created and maintained. Thank you.

Mr. COBLE. Thank you Mr. Kojm.

[The prepared statement of Mr. Kojm follows:]

PREPARED STATEMENT OF CHRISTOPHER A. KOJM

Chairman Coble, Ranking Member Scott, distinguished Members of the Judiciary Committee: it is an honor to appear before you today. The 9/11 Commission is grateful to you, and to the Leadership of the House, for your prompt consideration of the Report and recommendations of the Commission.

As you know, the Commission's findings and recommendations were strongly endorsed by all Commissioners—five Republicans and five Democrats who have been active in the public life of our nation. In these difficult times, and in an election year, this unanimity is remarkable, and important. It reflects a unity of purpose to make our country safer and more secure in the face of the novel threat posed by transnational terrorism. The Commission calls upon the Congress and the Administration to respond to our Report in the same spirit of bipartisanship.

You have asked the Commission to present its recommendations related to the Federal Bureau of Investigation, border security, and the creation of a Center for Counterterrorism and the National Intelligence Director. Our recommendations follow.

THE FBI

The FBI has for the past several decades performed two important but related functions.

First, it serves as our premier federal law enforcement agency, investigating possible violations of federal criminal statutes and working with federal prosecutors to develop and bring cases against violators of those laws.

Second, it is an important member of the Intelligence Community, collecting information on foreign intelligence or terrorist activities within the United States. That information can be used either for additional counterintelligence or counterterrorism investigations, or to bring criminal prosecutions.

We focused on the FBI's performance as an intelligence agency combating the al Qaeda threat within the United States before 9/11. Like the Joint Inquiry of the Senate and House Intelligence Committees before us, we found that performance seriously deficient.

Director Freeh did make counterterrorism a priority in the 1990s, and Dale Watson, his Counterterrorism chief, made valiant efforts to communicate that priority to agents in the field. But that priority did not effectively find its way into the daily work of the FBI's field offices. Nor did it result in the creation of a corps of intelligence officers and analysts with the professional qualifications and skills needed for an effective intelligence/counterterrorism operation.

Finally, when FBI agents did develop important information about possible terrorist-related activities, that information often did not get effectively communicated—either within the FBI itself or in the Intelligence Community as a whole.

Within the FBI itself, communication of important information was hampered by the traditional case-oriented approach of the agency and the possessive case-file mentality of FBI agents. This Committee is only too familiar with the information technology problems that have long hampered the FBI's ability to "know what it knows."

Even when information was communicated from the field to headquarters, it did not always come to the attention of the Director or other top officials who should have seen it. This was the case in the now-famous incidents, in the summer of 2001, of the Phoenix electronic communication about Middle Eastern immigrants in flight schools, and the Minneapolis Field Office's report to headquarters about the arrest of Zacarias Moussaoui.

The other internal barrier to communication of intelligence information between FBI intelligence officials and FBI criminal agents and federal prosecutors was the "wall" between intelligence and law enforcement that developed in the 1980s and was reinforced in the 1990s. Through a combination of court decisions, pronouncements from the Department of Justice and its Office of Intelligence Policy and Review, and risk-averse interpretations of those pronouncements by the FBI, the flow of information between the intelligence and criminal sides of the FBI and the Justice Department was significantly restricted. This phenomenon continued until after 9/11, when the Congress enacted the USA PATRIOT Act, and when the Justice Department successfully appealed a FISA Court decision that had effectively reinstated the wall.

These failures in internal communications were exacerbated by a reluctance of the FBI to share information with sister agencies in the Intelligence Community, with the National Security Council at the White House, and with state and local law enforcement agencies. This culture of non-sharing was by no means unique to the FBI, but the FBI was surely one of the worst offenders.

The FBI, under the leadership of its current Director, Robert Mueller, has undertaken significant reforms to try to deal with these deficiencies and build a strong capability in intelligence and counterterrorism. These include the establishment of an Office of Intelligence, headed by an Associate Director, Maureen Baginski, who is an experienced manager of intelligence systems. The FBI has embarked on an ambitious program to recruit qualified analysts, to train all agents in counterterrorism, and to develop career tracks for agents who want to specialize in counterterrorism or intelligence. The agency is also making progress, albeit slowly, in upgrading its internal information technology system. But, as Director Mueller himself has recognized, much more remains to be done before the FBI reaches its full potential as an intelligence agency.

Because of the history of serious deficiencies, and because of lingering doubts about whether the FBI can overcome its deep-seated law-enforcement culture, the Commission gave serious consideration to proposals to move the FBI's intelligence operations to a new agency devoted exclusively to intelligence collection inside the United States—a variant of the British Security Service, popularly known as MI-5.

We decided not to make such a recommendation for several reasons, set forth in our Report. Chief among them were the disadvantages of separating domestic intelligence from law enforcement and losing the collection resources of FBI field offices around the country, supplemented by relationships with state and local law enforcement agencies. Another major reason was civil liberties concerns that would arise from creating outside the Justice Department an agency whose focus is on collecting information from and about American citizens, residents, and visitors. The rights and liberties of Americans will be better safeguarded, we believe, if this sensitive function remains in an agency trained and experienced in following the law and the Constitution, and subject to the supervision of the Attorney General.

We also believe that while the jury is still out on the ultimate success of the reforms initiated by Director Mueller, the process he has started is a promising one. And many of the benefits that might be realized by creating a new agency will be achieved, we are convinced, if our important recommendations on restructuring of the Intelligence Community—creation of a National Counterterrorism Center and a National Intelligence Director with real authority to coordinate and direct the activities of our intelligence agencies—are implemented. An FBI that is an integral part of the NCTC and is responsive to the leadership of the National Intelligence Director will work even more effectively with the CIA and other intelligence agencies, while retaining the law enforcement tools that continue to be an essential weapon in combating terrorism.

What the Commission recommends, therefore, is that further steps be taken—by the President, the Justice Department, and the FBI itself—to build on the reforms that have been undertaken already, and to institutionalize those reforms so that the

FBI is transformed into an effective intelligence and counterterrorism agency. The goal, as our Report states, is to create within the FBI a specialized and integrated national security workforce of agents, analysts, linguists, and surveillance specialists who create a new FBI culture of expertise in national security and intelligence. This Committee will have a vital oversight role in monitoring progress by the FBI and ensuring that this new capacity so critical to our nation is created and maintained.

BORDER CONTROL

As our Report makes clear, in the decade before 9/11, border security was not seen as a national security matter. From a strategic perspective, border policy focused on counternarcotics efforts, illegal immigration, and, more recently, the smuggling of weapons of mass destruction. Our government simply did not exhibit a comparable level of concern about terrorists' ability to enter and stay in the United States.

During that same period, however, al Qaeda studied how to exploit gaps and weaknesses in the passport, visa, and entry systems of the United States and other countries. Al Qaeda actually set up its own passport office in Kandahar and developed working relationships with travel facilitators—travel agents (witting or unwitting), document forgers, and corrupt government officials.

As we know, Al Qaeda's travel tactics allowed the 9/11 hijackers to enter the United States quite easily. Yet the Commission found that many of the 19 hijackers were potentially vulnerable to detection by border authorities. Although the intelligence as to their tactics was not developed at the time, examining their passports could have allowed authorities to detect from four to 15 hijackers. More effective use of information in government databases could have allowed border authorities to intercept up to three of the hijackers had they been watchlisted.

More robust enforcement of routine immigration laws, supported by better information, could also have made a difference. Two hijackers made statements on their visa applications that could have been shown to be false by U.S. government records available to consular officers. Many of the hijackers lied about their employment or educational status. Two hijackers could have been denied admission at the port of entry based on violations of immigration rules governing terms of admission. Three hijackers violated the immigration laws after entry, one by failing to enroll in school as declared, and two by overstays of their terms of admission.

Neither the intelligence community, nor the border security agencies or the FBI, had programs in place to analyze and act upon intelligence about terrorist travel tactics—how they obtained passports, made travel arrangements, and subverted national laws and processes governing entry and stays in foreign countries.

Congress during the 1990s took some steps to provide better information to immigration officials by legislating requirements for a foreign student information system and an entry-exit system. As we know, these programs were not successfully implemented before 9/11.

Since 9/11, some important steps have been taken to strengthen our border security. The Department of Homeland Security has been established, combining the resources of the former Immigration and Naturalization Service and the Customs Bureau into new agencies to protect our borders and to enforce the immigration laws within the United States. The visa process and the terrorist watchlist system have been strengthened. DHS has begun to implement, through the US VISIT program, a biometric screening system for use at the border.

These efforts have made us safer, but not safe enough. As a nation we have not yet fully absorbed the lessons of 9/11 with respect to border security. The need to travel makes terrorists vulnerable. They must leave safe havens, travel clandestinely, and use evasive techniques, from altered travel documents to lies and cover stories. Terrorist entry often can be prevented and terrorist travel can be constrained by acting on this knowledge.

Targeting terrorist travel is at least as powerful a weapon against terrorists as targeting their finances.

The Commission therefore has recommended that we combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.

Targeting Terrorist Travel

Front line border agencies must not only obtain from the Intelligence Community—on a real-time basis information on terrorists; they must also assist in collecting it. Consular officers and immigration inspectors, after all, are the people who encounter travelers and their documents. Specialists must be developed and deployed in consulates and at the border to detect terrorists through their travel prac-

tices, including their documents. Technology has a vital role to play. The three years since 9/11 have been more than enough time for border officials to integrate into their operations terrorist travel indicators that have been developed by the intelligence community. The intelligence community and the border security community have not been close partners in the past. This must change.

We also need an operational program to target terrorist travel facilitators—forgers, human smugglers, travel agencies, and corrupt border officials. Some may be found here, but most will be found abroad. Disrupting them would seriously constrain terrorist mobility. While there have been some successes in this area, intelligence far outstrips action. This should be rectified by providing the interagency mandate and the necessary resources to Homeland Security's enforcement arm, Immigration and Customs Enforcement (ICE), and other relevant agencies, including the FBI.

This problem illustrates the need for a National Counterterrorism Center. Investigations of travel facilitators raise complicated questions: Should a particular travel facilitator be arrested or should he be the subject of continued intelligence operations? In which country should he be arrested? The NCTC could bring the relevant intelligence agencies to the table to coordinate and plan the best course of action.

Screening Systems

To provide better information to our consular officers and immigration inspectors, the government must accelerate its efforts to build a biometric entry and exit screening system. This is an area in which Congress has been active since the mid-1990's. It has been a frustrating journey. Congress first legislated an entry-exit system in 1996, to increase compliance with our immigration laws. It was neither associated with counterterrorism, nor with biometric identification. As a practical matter, the entry-exit effort was not seriously funded until the end of 2002. By that time, aspects of a system were governed by four separate laws. The establishment of the Department of Homeland Security then changed the organizational context for implementing those laws.

The new Department is emerging from its difficult start-up period and is, we believe, poised to move forward to implement Congress's mandates in this area. We would like to stress four principles that we believe must guide our efforts in this arena.

First, the U.S. border security system must be an effective part of a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The Department of Homeland Security should lead an effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind.

Second, a biometric entry and exit screening system is fundamental to intercepting terrorists and its development should be accelerated. Each element of the system is important. The biometric identifier makes it difficult to defeat a watchlist by an alteration in spelling of a name, a technique relied upon by terrorists. The screening system enables border officials access to all relevant information about a traveler, in order to assess the risk they may pose. Exit information allows authorities to know if a suspect individual has left the country and to establish compliance with immigration laws.

Third, United States citizens should not be exempt from carrying biometric passports or otherwise enabling their identities to be securely verified. Nor should Canadians or Mexicans.

Fourth, there should be a unified program to speed known travelers, so inspectors can focus on those travelers who might present greater risks. This is especially important for border communities.

We believe that the schedule for completion of this biometric entry-exit screening system should be accelerated to the extent feasible. This will require additional annual funding, and a mandate to a central organizational authority, such as the US VISIT office, to manage the effort.

International Collaboration

We need to dedicate a much greater effort to collaboration with foreign governments with respect to border security. This means more exchange of information about terrorists and passports, and improved global passport design standards. Implicit in this recommendation is continued close cooperation with Mexico and Canada. One particularly important effort is to improve screening efforts prior to departure from foreign airports, especially in countries participating in the visa waiver program.

Immigration Law and Enforcement

We must be able to monitor and respond to entries along our long borders with Canada and Mexico, working with those countries as much as possible. Our law enforcement system ought to send a message of welcome, tolerance, and justice to members of the immigrant communities in the United States, while also fostering the respect for the rule of law. Good immigration services are one way to reach out that is valuable, including for intelligence. State and local law enforcement agencies need more training and partnerships with federal agencies so they can cooperate more effectively with those federal authorities in identifying terrorist suspects.

Finally, secure identification should begin in the United States. We believe that the federal government should set standards for the issuance of birth certificates and sources of identification such as drivers' licenses.

The agenda on immigration and border control, then, is multi-faceted and vital to our national security. The bottom line is that our visa and border control systems must become an integral part of our counterterrorism intelligence system. We must steer a course that remains true to our commitment to an open society that welcomes legitimate immigrants and refugees while concentrating our resources on identification of potential of potential terrorists and prevention of their entry into the United States.

THE NATIONAL INTELLIGENCE DIRECTOR

As part of the 9/11 story, we spent a very considerable time looking at the performance of the Intelligence Community. We identified at least six major problems confronting the Intelligence Community that became apparent in 9/11 and still continue today.

First, there are major structural barriers to the performance of joint intelligence work. National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots."

Second, there is a lack of common standards and practices across the foreign-domestic divide for the collection, processing, reporting, analyzing, and sharing of intelligence.

Third, there is divided management of national intelligence capabilities, between the Director of Central Intelligence and the Defense Department

Fourth, the Director of Central Intelligence has a weak capacity to set priorities and move funds and other resources;

Fifth, the Director of Central Intelligence now has at least three jobs—running the CIA, running the Intelligence Community, and serving as the President's Chief Intelligence Adviser. No one person can perform all three.

Finally, the Intelligence Community is too complex, and too secret. Its 15 agencies are governed by arcane rules, and all of its money and most of its work is shielded from public scrutiny.

We come to the recommendation of a National Intelligence Director not because we want to create some new "czar" or new layer of bureaucracy to sit atop the existing bureaucracy. We come to this recommendation because we see it as the only way to effect what we believe is necessary: a complete transformation of the way the Intelligence Community does business.

We believe that the Intelligence Community needs a wholesale Goldwater-Nichols reform of the way it does business. The collection agencies should have the same mission as the Armed Services do: they should organize, train and equip their personnel. Those intelligence professionals, in turn, should be assigned to unified joint commands, or in the language of the Intelligence Community, "Joint Mission Centers." A joint mission center on WMD and proliferation, for example, would bring together the imagery, signals, and HUMINT specialists, both collectors and analysts, who would work together jointly on behalf of the mission. All the resources of the community would be brought to bear on the key intelligence issues as identified by the National Intelligence Director.

We believe you cannot get the necessary transformation of the Intelligence Community—smashing the stovepipes and creating joint mission centers—unless you have a National Intelligence Director.

The National Intelligence Director needs authority over all intelligence community elements, including authority over personnel, information technology and security. Appropriations for intelligence should come to him, and he should have the authority to reprogram funds within and between intelligence agencies.

The National Intelligence Director would create, and then oversee the joint work done by the intelligence centers. He should have a small staff—about the size of the current Community Management Staff.

He would not be like other "czars" who get the title but have no meaningful authority. The National Intelligence Director would have real authority. He will control National Intelligence Program purse strings. He will have hire and fire authority over agency heads in the Intelligence Community. He will control the IT. He will have real "troops," as the National Counterterrorism Center and all the Joint Mission Centers would report to him.

We concluded that the Intelligence Community just isn't going to get its job done unless somebody is in charge. That is just not the case now, and we paid the price: information wasn't shared, agencies didn't work together. We have to—and can—do better as a government.

To underscore again, we support a National Intelligence Director not for the purpose of naming another Chief to sit on top of all the other Chiefs. We support the creation of this position because it is the only way to catalyze transformation in the Intelligence Community, and manage a transformed Community afterward.

THE NATIONAL COUNTERTERRORISM CENTER

Our report details many unexploited opportunities to disrupt the 9/11 plot: failures to watchlist, failures to share information, failure to connect the dots. The story of Hazmi and Mihdhar in Kuala Lumpur in January 2000 is a telling example. We caught a glimpse of the future hijackers, but we lost their trail in Bangkok. Domestic officials were not informed until August, 2001 that Hazmi and Mihdhar had entered the United States. Late leads were pursued, but time ran out.

In this and in other examples, we find that no one was firmly in charge of managing the case. No one was able to draw relevant intelligence from anywhere within the government, assign responsibilities across the agencies (foreign or domestic), track progress and quickly bring obstacles up to a level where they could be resolved. No one was the quarterback. No one was calling the play. No one was assigning roles so that government agencies could execute as a team.

We believe the solution to this problem rests with the creation of a new institution, the National Counterterrorism Center. We believe, as Secretary Rumsfeld told us, that each of the agencies need to "give up some of their existing turf and authority in exchange for a stronger, faster, more efficient government wide joint effort." We therefore propose a civilian-led unified joint command for counterterrorism. It would combine intelligence (what the military calls the J-2 function) with operational planning (what the military calls the J-3 function) in one agency, keeping overall policy direction where it belongs, in the hands of the President and the National Security Council.

Again, we consciously and deliberately draw on the military model, the Goldwater-Nichols model. We can and should learn from the successful reforms in the military two decades ago. We want all the government agencies which play a role in counterterrorism to work together in a unified command. We want them to work together as one team, in one fight against transnational terrorism.

The National Counterterrorism Center would build on the existing Terrorist Threat Integration Center, and replace it and other terrorism "fusion centers" within the government with one, unified center.

The NCTC would have tasking authority on counterterrorism for all collection and analysis across the government, across the foreign-domestic divide. It would be in charge of warning.

The NCTC would coordinate anti-terrorist operations across the government, but individual agencies would execute operations within their competences.

The NCTC's chief would have control over the personnel assigned to the Center, and must have the right to concur in the choices of personnel to lead the operating entities of the departments and agencies focused on counterterrorism, specifically the top counterterrorism officials at the CIA, FBI, Defense and State Departments. The NCTC chief would report to the National Intelligence Director.

We appreciate that this is a new and difficult idea for those of us schooled in government of the 20th century. We won the Second World War and the Cold War because of the great departments of government—the State Department, the Defense Department, the CIA, the FBI—organized against clear nation-state adversaries. Today, we face a transnational threat. It respects no boundaries, and makes no distinction between foreign and domestic. The enemy is resourceful, flexible and disciplined. We need a system of management that is as flexible and resourceful as is the enemy, a system that can bring all the resources of government to bear on the problem—and that can change and respond as the threat changes. We need a model of government that meets the needs of the 21st century. We believe the National Counterterrorist Center meets that test.

REFORMS AS A COMPLETE PACKAGE

Taken together, we believe these reforms within the structure of the Executive branch, together with reforms in Congress, and the many recommendations we have proposed for foreign policy, public diplomacy, border and transportation security, and national preparedness—can make a significant difference in making America safer and more secure.

We believe that reforms of executive branch structures, in the absence of implementing the other reforms and recommendations in our report, will have significantly less value than the value of these reforms as a complete package. In short, while we welcome each step toward implementation of our recommendations, no one should be mistaken in believing that solving structural problems in the executive branch addresses completely, or even satisfactorily, the current terrorist threat we face.

THE ADMINISTRATION'S RESPONSE

We are gratified by the rapid response of the White House to our recommendations. President Bush has acknowledged the need for a National Intelligence Director separate from the head of the CIA. Senator Kerry shares this judgment. It is our firm belief that the National Intelligence Director must have budgetary appropriation authority over the agencies of the intelligence community. Moreover, he should have hire and fire authority for significant positions within the community. A National Intelligence Director without these authorities would be, in our view, a mere figurehead, and there would be no significant advance over the current arrangement, which we have found to be inadequate to protect the nation.

CONCLUSION

The most important responsibility of government is to protect the people.

We have made specific proposals. We believe they can make our country safer and more secure. We invite the American public to join the debate.

We are gratified by the rapid response of the White House to our recommendations. We welcome the President's support for a National Intelligence Director, and a National Counterterrorism Center. We welcome the support of Senator Kerry.

We look forward to working with you on our recommendations.

We should seize this historic opportunity and move expeditiously. With your counsel and direction, we believe that the nation can, and will, make wise choices.

We would be pleased to respond to your questions.

Mr. COBLE. Mr. Pistol.

TESTIMONY OF JOHN S. PISTOLE, EXECUTIVE ASSISTANT DIRECTOR, COUNTERTERRORISM/COUNTERINTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION

Mr. PISTOLE. Good morning, Chairman Coble, Ranking Member Scott, Members of the Subcommittee. Thank you for the invitation to speak here this morning.

The FBI has worked closely with the 9/11 Commission staff and we commend it for its extraordinary efforts. Throughout this process we have approached the Commission's inquiry as an opportunity to gain further input from outside experts. We took its critique seriously, adapted our ongoing reform efforts, and have already taken substantial steps to address its remaining concerns.

First, on the transformation of the FBI under Director Mueller's leadership, we have moved aggressively to implement a comprehensive plan that has fundamentally transformed the FBI with one goal in mind: establishing the prevention of terrorism as the Bureau's number one priority.

Director Mueller has focused on four areas. One is centralized our counterterrorism operations; two, expanded our intelligence capabilities; three, modernized our business practices and technology; and four, improved coordination with our partners.

A number of steps have been taken to—have taken place to enhance operational and analytic capabilities and to ensure continued sharing of information with our partners at the Federal, State, local, tribal and international levels. As a result, we have more than doubled the number of counterterrorism agents, intelligence analysts, and linguists. We have created and expanded the terrorism financing operation section. We have become active participants in the Terrorist Threat Integration Center and the Terrorist Screening Center. We've integrated our intelligence operations with CIA at virtually every level. This cooperation will be further enhanced as our counterterrorism division continues to colocate with the CIA's Counterterrorist Center and the TTIC.

We have also expanded the number of joint terrorism task forces from 34 prior to 9/11, to currently 100 nationwide. We have created and refined new information sharing systems and centralized the management of our CT program to ensure consistency of CT priorities and strategy, integrated CT operations domestically and overseas, improved coordination with other agencies and governments and to make senior managers accountable for the overall development and success of our CT efforts.

In our intelligence program we've recognized that a strong enterprise-wide intelligence program is critical to our success across all investigations. And we have worked to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the U.S. and across the FBI.

Along those lines we have stood up the Offices of intelligence with Maureen Baginski, my colleague, as Executive Director for Intelligence.

We have established a formal analyst training program.

We have developed and are in the process of executing concepts of operations governing all aspects of the intelligence process.

We have established a Requirements and Collection Management Unit to identify intelligence gaps and developed collection strategies to fill those gaps.

We have established Reports Officers positions and Field Intelligence Groups in each of our field offices.

The FBI's Joint Terrorism Task Force program continues to be the U.S. Government's primary operational arm for preventing and investigating terrorist attacks in the United States. As I mentioned, we now have 100 nationwide.

Details on our efforts in counterproliferation and the new workforce are included in my written statement. I won't go into details at this time in my oral statement.

On August 2nd, the President announced his intention to establish a national intelligence director to take on the responsibility of principal intelligence advisor and head of the Intelligence Community at a national counterterrorism center. While the details of these two new entities are still being worked out, the FBI does agree that operations and intelligence need to be intertwined and complementary to each other. We believe that concerns regarding civil liberties must be appropriately addressed in all that is proposed. This will require paying particular attention to legal and historical differences regarding the question of information in the United States and overseas.

We look forward to working with you and your Subcommittee on the functions of both the NID and NCTC. The 9/11 Commission's recommendations will enhance the FBI's capability by providing more robust intelligence-focused organizational structure, workforce, and infrastructure.

The FBI looks forward to an ongoing public discussion of ways to support the Intelligence Community's CT capabilities, collection mission, and collection support mission, and to further enhance information sharing and collaboration with the intelligence and law enforcement communities.

Again, the FBI would like to thank the 9/11 Commission for its public service. And I thank you for inviting me here today to testify before the Subcommittee. Thank you, Mr. Chairman.

Mr. COBLE. Thank you, Mr. Pistole.

[The prepared statement of Mr. Pistole follows:]

PREPARED STATEMENT OF JOHN S. PISTOLE

Good afternoon Chairman Coble, Ranking Member Scott and members of the Subcommittee. Thank you for inviting me to speak to you today regarding the 9/11 Commission's Recommendations, specifically those recommendations that focus on the creation of a National Intelligence Director, creating a specialized and integrated national security workforce at the FBI, and targeting the networks that provide material support to terrorism. The FBI has worked closely with the 9/11 Commission and its staff and we commend it for an extraordinary effort. Throughout this process, we have approached the Commission's inquiry as an opportunity to gain further input from outside experts. We took its critiques seriously, adapted our ongoing reform efforts, and have already taken substantial steps to address its remaining concerns. We are gratified and encouraged that the Commission has embraced our vision for change and recognized the progress that the men and women of the FBI have made to implement that vision. We agree with the Commission that much work remains to be done, and will consider its findings and recommendations as we refine our continuing transformation efforts.

TRANSFORMATION OF THE FBI

Under the leadership of Director Mueller, the FBI has moved aggressively forward to implement a comprehensive plan that has fundamentally transformed the FBI with one goal in mind: establishing the prevention of terrorism as the Bureau's number one priority. No longer are we content to concentrate on investigating terrorist crimes after they occur; the FBI now is dedicated to disrupting terrorists before they are able to strike. Director Mueller has overhauled our counterterrorism operations, expanded our intelligence capabilities, modernized our business practices and technology, and improved coordination with our partners.

At the FBI we are taking full advantage of our dual role as both a law enforcement and an intelligence agency. As we continue to transform the FBI to address the priorities articulated by the Director, a number of steps have taken place to enhance operational and analytical capabilities and to ensure continued sharing of information with our partners at the federal, state, local, tribal, and international levels. As a result:

- We have more than doubled the number of counterterrorism Agents, intelligence analysts, and linguists.
- We created and expanded the Terrorism Financing Operations Section which is dedicated to identifying, tracking, and cutting off terrorist funds.
- We are active participants in the Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC), which provide a new line of defense against terrorism by making information about known or suspected terrorists available to the national security, homeland security, and law enforcement communities.
- We have worked hard to break down the walls that have sometimes hampered our coordination with our partners in federal, state and local law enforcement. Today, the FBI and CIA are integrated at virtually every level of our intelligence operations. This cooperation will be further enhanced as our

Counterterrorism Division continues to co-locate with the DCI's Counter Terrorist Center and the multi-agency Terrorist Threat Integration Center.

- We expanded the number of Joint Terrorism Task Forces (JTTF) from 34 to 100 nationwide.
- We created and refined new information sharing systems, such as the FBI National Alert System and the interagency Alert System that electronically link us with our domestic partners.
- We have sent approximately 275 FBI executives to the Kellogg School of Management at Northwestern University to receive training on executive leadership and strategic change.

We centralized management of our Counterterrorism Program at Headquarters to limit "stove-piping" of information, to ensure consistency of counterterrorism priorities and strategy across the organization, to integrate counterterrorism operations domestically and overseas, to improve coordination with other agencies and governments, and to make senior managers accountable for the overall development and success of our counterterrorism efforts.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked relentlessly to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI:

- We stood up the Office of Intelligence, under the direction of a new Executive Assistant Director for Intelligence. The Office of Intelligence sets unified standards, policies, and training for analysts, who examine intelligence and ensure it is shared with our law enforcement and intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President and members of the Intelligence Community.
- We established a formal analyst training program. We are accelerating the hiring and training of analytical personnel, and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.
- We developed and are in the process of executing Concepts of Operations governing all aspects of the intelligence process—from the identification of intelligence requirements to the methodology for intelligence assessment to the drafting and formatting of intelligence products.
- We established a Requirements and Collection Management Unit to identify intelligence gaps and develop collection strategies to fill those gaps.
- We established Reports Officers positions and Field Intelligence Groups in the field offices, whose members review investigative information—not only for use in investigations in that field office—but to disseminate it throughout the FBI and among our law enforcement and Intelligence Community partners.

PREVENTING TERRORISM AT HOME AND AGAINST U.S. INTERESTS ABROAD

The FBI's JTTF Program continues to have primary operational responsibility for terrorism investigations that are not related to ongoing prosecutions. Since September 11th, the FBI has increased the number of JTTFs nationwide from 34 to 100. The JTTFs are comprised of FBI Special Agents and personnel from other federal, state, local and tribal government and law enforcement agencies. We also established the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters, staffed by representatives from 38 federal, state, and local agencies. The mission of the NJTTF is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of counterterrorism operations.

In addition, we continue to grow the Field Intelligence Groups (FIGs) established in every FBI field office and are on track to add some 300 Intelligence Analysts to the FIGs in FY 2004. The FIGs conduct analysis, direct the collection of information to fill identified intelligence gaps, and ensure that intelligence is disseminated horizontally and vertically to internal and external customers, including our State, local and tribal law enforcement partners.

We have also improved our relationships with foreign governments by building on the overseas expansion of our Legat Program; by offering investigative and forensic support and training, and by working together on task forces and joint operations. Finally, the FBI has expanded outreach to minority communities, and improved coordination with private businesses involved in critical infrastructure and finance.

INTELLIGENCE PROGRAM

At the FBI, we recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that both appropriately protect the privacy of information and allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence both within the FBI and outside it. This has occurred under the umbrella of the FBI(s Intelligence Program.

The mission of the FBI(s Intelligence Program is to optimally position the FBI to meet current and emerging national security and criminal threats by (1) aiming core investigative work proactively against threats to US interests, (2) building and sustaining enterprise-wide intelligence policies and human and technical capabilities, and (3) providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities.

We built the FBI Intelligence Program on the following core principles:

- *Independent Requirements and Collection Management:* While intelligence collection, operations, analysis, and reporting are integrated at headquarters divisions and in the field, the Office of Intelligence manages the requirements and collection management process. This ensures that we focus intelligence collection and production on priority intelligence requirements and on filling key gaps in our knowledge.
- *Centralized Management and Distributed Execution:* The power of the FBI intelligence capability is in its 56 field offices, 400 resident agencies and 56 legal attaché offices around the world. The Office of Intelligence must provide those entities with sufficient guidance to drive intelligence production effectively and efficiently, but not micro-manage field intelligence operations.
- *Focused Strategic Analysis:* The Office of Intelligence sets strategic analysis priorities and ensures they are carried out both at headquarters and in the field.
- *Integration of Analysis with Operations:* Intelligence analysis is best when collectors and analysts work side-by-side in integrated operations.

Concepts of Operations (CONOPs) guide FBI intelligence processes and detailed implementation plans drive specific actions to implement them. Our CONOPs describe the Intelligence Requirements and Collection Management system and are supported by lower-level collection and collection support processes and procedures defined in our *Intelligence Requirements and Collection Management Handbook.* These concepts and processes complement FBI operations and are enhanced by the Commission's recommendations.

What follows are some of our key accomplishments:

- We have issued our first ever FBI collection tasking for international threats, including international terrorism. We based those requirements on the National Intelligence Priorities Framework and, in cooperation with the Intelligence Community, issued an unclassified version for our partners in state and local law enforcement.
- We have inventoried our collection capability. We created an on-line inventory of all our collection sources. This tells us what we could know about all threats.
- We are now comparing the intelligence requirements to our capabilities and identifying gaps in our ability to produce information described in our requirements. Dedicated targeting analysts at headquarters and the field then analyze how we could fill those gaps by developing new sources. Source development tasks are given to each Field Intelligence Group (FIG) to execute.
- As a result of this process, we then produce information—both raw intelligence reports and finished assessments—in response to requirements. Each intelligence report requests customer feedback. Based on what we learn, we adjust collection and production.

COUNTER PROLIFERATION

In the area of counter-proliferation, our Counterintelligence Division is currently in the process of creating a counter-proliferation unit in each of its region and issue-oriented operational Headquarters sections. While we currently work diligently on proliferation matters, this will further the emphasis our fifty six field divisions place on counter-proliferation investigations through a more robust Bureau-wide orienta-

tion. These new units will also form the basis for the future creation of a new Counter-proliferation Section at FBI Headquarters. This enhanced organizational architecture will enable the FBI to meet the growing challenges of world-wide WMD proliferation and to continue to protect our national security.

THE NEW WORKFORCE

The FBI is actively working to build a workforce with expertise in intelligence. While much remains to be done, we have already taken steps to ensure this transformation.

On March 22, 2004, Director Mueller adopted a proposal to establish a career path in which new Special Agents are initially assigned to a small field office and exposed to a wide range of field experiences. After approximately three years, agents will be transferred to a large field office where they will specialize in one of four program areas: Intelligence, Counterterrorism/ Counterintelligence, Cyber, or Criminal, and will receive advanced training tailored to their area of specialization. We are working to implement this new career track.

Director Mueller has also approved a proposal to establish a formal Intelligence Officer Certification that can be earned through a combination of intelligence assignments and training. Once established, this certification will be a prerequisite for promotion to the level of Section Chief at FBIHQ, or Assistant Special Agent in Charge (ASAC) at the field level, thus ensuring that all members of the FBI's highest management levels will be staffed by fully trained and experienced intelligence officers.

We have implemented a strategic plan to recruit, hire, and retain Intelligence Analysts. The Bureau has selected veteran analysts to attend events at colleges and universities, as well as designated career fairs throughout the country. We executed an aggressive marketing plan, and for the first time in FBI history, we are offering hiring bonuses for FBI analysts.

In our Special Agent hiring program, we have updated the list of "critical skills" we are seeking in candidates to include intelligence experience and expertise, foreign languages, and technology.

The FBI's Executive Assistant Director for Intelligence has been given personal responsibility for developing and ensuring the health of the FBI intelligence personnel resources. It is important to note that the FBI's intelligence cadre is not limited to intelligence analysts, but also includes agents, language analysts, surveillance specialists, and others. It takes all of these specialists to perform quality intelligence production at the FBI. The FBI's plan to create a cradle-to-grave career path for intelligence professionals at the FBI parallels the one that has existed and functioned so well for our agents and has been codified in our Concept of Operations (CONOP) for Human Talent for Intelligence Production.

NATIONAL INTELLIGENCE DIRECTOR AND NATIONAL COUNTERTERRORISM CENTER

On August 2nd, the President announced his intention to establish a National Intelligence Director (NID), to take on the responsibility of principle intelligence advisor and head of the Intelligence Community, and a National Counter Terrorism Center (NCTC). While the details of these two new entities still need to be fleshed out and discussed, the FBI does agree that operations and intelligence need to be intertwined and complementary to each other. We believe that concerns regarding civil liberties must be appropriately addressed in all that is proposed. This will require paying particular attention to legal and historical differences regarding the collection of information in the United States and overseas. We look forward to working with you on the functions of both the NID and the NCTC.

As the Commission points out, we have much work still to do, but we have made great progress and continue to move forward in accordance with a clear plan. With the support and understanding of lawmakers and the American people, I am confident that we will successfully complete our transformation and ultimately prevail against terrorists and all adversaries who would do harm to our Nation.

The FBI looks forward to an ongoing public discussion of ways to support the Intelligence Community's counterterrorism mission and capabilities and to further enhance information sharing and collaboration within the Intelligence and Law Enforcement Communities. The Commission's recommendations will enhance the FBI's capabilities by providing a more robust, intelligence-focused organizational structure, work force and infrastructure.

The FBI thanks the 9/11 Commission for its public service and I thank you for inviting me here today to testify before the Committee. It will be my pleasure to answer any questions you may have at the appropriate time.

Mr. COBLE. Mr. Brennan.

TESTIMONY OF JOHN O. BRENNAN, DIRECTOR, TERRORIST THREAT INTEGRATION CENTER

Mr. BRENNAN. Good morning, Mr. Chairman, and distinguished Subcommittee Members. It's an honor and privilege to be before you today to talk about the Terrorist Threat Integration Center, or TTIC, and the recommendations of the 9/11 Commission.

In his State of the Union speech in January 2003, the President called for the creation of an integrated center to merge and analyze all threat information in a single location. On 1 May of last year that vision became a reality with the stand up of the TTIC. For the first time in our history a multiagency entity has access to information systems and databases spanning the intelligence, law enforcement, homeland security, diplomatic and military communities that contain information related to the threats of international terrorism. In fact, TTIC has direct access connectivity to 26 separate U.S. Government networks, with more networks coming online, enabling information sharing as never before in the U.S. Government.

This unprecedented access to information allows comprehensive insight to information related to terrorist threats to U.S. interests at home and abroad. Most importantly, it enhances the Government's ability to provide this information and related analysis to those responsible for detecting, disrupting, deterring and defending against terrorist attacks.

There currently exists within the TTIC joint venture real-time collaboration among analysts from a broad array of agencies and departments who sit side by side sharing information and piecing together the scattered pieces of the terrorism puzzle. These partners include not only the FBI, CIA, and the Departments of State, Defense, and Homeland Security, but also other Federal agencies and departments such as the Nuclear Regulatory Commission, the Department of Health and Human Services, and the Department of Energy.

This integration of perspectives from multiple agencies and departments represented in TTIC is serving as a force multiplier in the fight against terrorism. On a strategic level TTIC works with the community to provide the President and key officials a daily analytic product on the most serious terrorist threats and related terrorism information that serves as a common foundation for decision-making regarding the actions necessary to disrupt terrorist plans.

Rather than multiple threat assessments and disparate information flows on the same subject matter being forwarded separately to senior policymakers, information and finished analysis are now fused in a multiagency environment so that an integrated and comprehensive threat picture is provided. If there are analytic differences, they are incorporated into analysis.

The Terrorist Threat Integration Center embodies several of the characteristics envisioned by the 9/11 Commission report for the proposed national counterterrorism center. TTIC is an existing joint intelligence center, staffed by personnel from various agencies and well positioned to integrate all sources of terrorism information. It is likely for those reasons that the Commission recommends

that TTIC serve as the foundation of a new national counterterrorism center. As a long time proponent of structural reform of the Intelligence Community, I fully and personally support the integration concept and the establishment of a national counterterrorist center.

In the weeks and months ahead I look forward to working with TTIC's partner agencies, the Congress, and the White House to build upon TTIC's strong foundation and create a national counterterrorism center. The potential benefits of a national counterterrorism center are enormous. So too, however, are the challenges associated with Government transformation. I have experienced those challenges firsthand over the past 15 months in the establishment and development of TTIC. Together we will need to determine how to implement the national counterterrorism center in a thoughtful and evolutionary manner so that we do not adversely affect ongoing activities in the global war on terrorism which is so ably led by the different departments and agencies throughout the U.S. Government.

Thank you, Mr. Chairman. I look forward to taking your questions.

Mr. COBLE. Thank you, Mr. Brennan.

[The prepared statement of Mr. Brennan follows:]

PREPARED STATEMENT OF JOHN O. BRENNAN

Good afternoon, Chairman Coble, Congressman Scott, and Subcommittee members.

It is an honor to appear before you today to talk about the Terrorist Threat Integration Center, TTIC, and discuss the recommendations of the 9/11 Commission, specifically the creation of the National Counterterrorism Center as announced by the President.

As this Committee knows, the President has embraced the Commission's recommendation for the creation of a centralized organization to integrate terrorist threat information. The President's formal announcement to establish a National Counterterrorism Center is a natural extension of the work and successes the administration has already achieved through the establishment of TTIC.

In his State of the Union speech, in January 2003, the President called for the creation of an integrated center to merge and analyze all threat information in a single location. On May of last year, that vision became a reality with the stand-up of TTIC. Over the past 15 months, TTIC has endeavored to optimize the U.S. Government's knowledge and formidable capabilities in the fight against terrorism.

For the first time in our history, a multi-agency entity has access to information systems and databases spanning the intelligence, law enforcement, homeland security, diplomatic, and military communities that contain information related to the threat of international terrorism. In fact, TTIC has direct-access connectivity with 26 separate U.S. Government networks—with more networks coming on-line—enabling information sharing as never before in the U.S. Government.

This unprecedented access to information allows us to gain comprehensive insight to information related to terrorist threats to U.S. interests at home and abroad. Most importantly, it enhances the Government's ability to provide this information and related analysis to those responsible for detecting, disrupting, deterring, and defending against terrorist attacks.

In addition, there currently exists within the TTIC joint venture, real-time collaboration among analysts from a broad array of agencies and departments who sit side-by-side, sharing information and piecing together the scattered pieces of the terrorism puzzle. These partners include not only the FBI, CIA and the Departments of State, Defense and Homeland Security, but also other federal agencies and departments such as the Nuclear Regulatory Commission, the Department of Health and Human Services, and the Department of Energy.

- As envisioned by the President, this physical integration of expertise and sharing of information enables and empowers the key organizations involved in the fight against terrorism. Collectively, they are fulfilling their shared re-

sponsibilities in a fused environment, "doing business" jointly as TTIC. This fusion and synergy will be further enhanced when CIA's Counterterrorist Center and FBI's Counterterrorism Division collocate with TTIC in the coming months.

- This integrated business model not only capitalizes on our respective and cumulative expertise, but it also optimizes analytic resources in a manner that allows us to cover more effectively and comprehensively the vast expanse of terrorist threats that will face the Homeland and U.S. interests worldwide for the foreseeable future.

This integration of perspectives from multiple agencies and departments represented in TTIC is serving as a force multiplier in the fight against terrorism. On a strategic level, TTIC works with the Community to provide the President and key officials a daily analytic product on the most serious terrorist threats and related terrorism information that serves as a common foundation for decision making regarding the actions necessary to disrupt terrorist plans. Rather than multiple threat assessments and disparate information flows on the same subject matter being forwarded separately to senior policymakers, information and finished analysis are now fused in a multi-agency environment so that an integrated and comprehensive threat picture is provided. If there are analytic differences on the nature or seriousness of a particular threat, they are incorporated into the analysis.

As is evident, the Terrorist Threat Integration Center embodies several of the characteristics envisioned by the 9/11 Commission report for the proposed "National Counterterrorism Center." TTIC is an existing center for "joint intelligence, staffed by personnel from the various agencies" and well positioned to "integrate all sources of information to see the enemy as a whole." It is likely for those reasons that the Commission recommends that TTIC serve as the foundation of a new National Counterterrorism Center. As a long-time proponent of structural reform of the Intelligence Community, I fully support the integration concept and the establishment of a National Counterterrorism Center.

In the weeks and months ahead, I look forward to working with TTIC's partner agencies, the Congress, and the White House to build upon TTIC's strong foundation and create a National Counterterrorism Center. The potential benefits of a National Counterterrorism Center are enormous. So too, however, are the challenges associated with Government transformation. I have experienced those challenges firsthand over the past 15 months in the establishment and development of TTIC. Together, we will need to determine how to implement the National Counterterrorism Center in a thoughtful and evolutionary manner so that we do not adversely affect ongoing activities in the global war on terrorism which are so ably led by my colleagues on this panel.

In conclusion, I believe the benefits to be gained from this integration concept, as envisioned by the President and called for by the 9/11 Commission, strongly support the creation of a National Counterterrorism Center, and I look forward to working with you to implement a national counterterrorism system that maximizes the security and safety of all Americans wherever they live or work.

Thank you Mister Chairman. I look forward to taking your questions.

Mr. COBLE. Mr. Nojeim.

TESTIMONY OF GREGORY T. NOJEIM, ASSOCIATE DIRECTOR AND CHIEF LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. NOJEIM. Thank you, Chairman Coble, Ranking Member Scott, Members of the Subcommittee. Thanks for the opportunity to testify before you today on behalf of the ACLU about the recommendations of the 9/11 Commission. The ACLU is a nationwide, non-partisan organization of 400,000 members dedicated to protecting the principles of freedom and equality set forth in our Nation's Constitution and our civil rights laws.

The ACLU supports intelligence and other reforms that are calculated to make us both more secure and to secure liberty. We recognize the real continuing threat that terrorism poses. We also recognize that securing the Nation means securing the freedoms that make our Nation great.

The Commission's report proposes major structural changes to address intelligence failures. It is to be commended for its work and for recognizing that many of its recommendations call for the Government to increase its presence in the lives of Americans. This, and the proposed consolidation of intelligence powers, pose challenges to civil liberties that must be addressed.

My written testimony includes 19 recommendations calculated to protect civil liberties. I will focus on four of them.

First, the Judiciary Committees in the House and Senate should retain jurisdiction to conduct oversight over domestic intelligence and criminal surveillance and over governmental actions to fight terrorism that affect legal and constitutional rights. This may seem an unusual position for the ACLU. After all, more civil liberties lawsuits challenge the constitutionality of statutes that come out of the Judiciary Committee than from any other.

At the same time, though, the Judiciary Committee conducts vigorous oversight openly and it takes significant statutory steps to preserve civil liberties. The Committee's determination to report to the full House H.R. 338, the Federal Agency Protection of Privacy Act, is a good example. It would require Federal agencies to consider the privacy impact of the regulations they propose and adopt. Limiting the number of congressional Committees with oversight duties may frustrate, rather than enhance, congressional oversight.

Second, we support the Commission's call for a civil liberties oversight board that would become the office that looks at actions taken government-wide to protect America. It would ensure that liberty concerns are appropriately considered. As Commission Vice Chair Hamilton recognized, the civil liberties board must have enough clout to make Federal agencies respond to it. And that means it must have subpoena power. It should be independent, nonpartisan, and open. It should be both a proactive voice for civil liberties while policies are being formulated, and it should be able to look retrospectively at patterns of civil liberties abuses. It would supplement, not supplant, the Inspectors General.

By helping focus security measures on truly dangerous people and not on everyone else, a civil liberties board serves both the causes of liberty and security. Remember, a security system that spends 20 hours treating Senator Ted Kennedy and Representative John Lewis as potential terrorists has 20 fewer hours to identify the next Mohammad Atta.

Third, should Congress create a national intelligence director, it should not put it in the Executive Office of the President. The President himself shares this view, as does the Ranking Member of the House Intelligence Committee, Representative Harman, and the Ranking Member of the Senate Armed Services Committee, Senator Levin. To locate this function in the President's Office could complicate congressional oversight with claims of executive privilege and would risk politicizing the use of intelligence power.

Finally, we urge you to reject the federalization of identity documents issued by the States, a back door to a national identification card. Once the Federal Government tells the States what can and cannot go on the card and what data will be behind the card, the card will be required to clear and track all manner of transactions now conducted freely and privately. Businesses will want to see

and swipe the card and they will use the identifiers on the card to track customer purchases and activities.

We urge you, finally, to act with care as you consider the Commission's recommendations. Changes to the structure of the Intelligence Community will last generations. Mistakes could be very costly. Any such changes should be accompanied by measures to ensure that America remains not only safe but free. Thank you.

Mr. COBLE. Thank you Mr. Nojeim.

[The prepared statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM

Chairman Coble, Ranking Member Scott and Members of the Subcommittee:

I am pleased to appear before you today on behalf of the American Civil Liberties Union and its more than 400,000 members, dedicated to preserving the principles of the Constitution and Bill of Rights, to explain the ACLU's views on the recommendations in the Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission report").

The 9/11 Commission report exhaustively details significant failures of the intelligence agencies, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), and proposes major structural changes to address those failures. The report contains helpful suggestions on privacy and civil liberties, proposing a Civil Liberties Protection Board and a framework for judging anti-terrorism powers including the USA PATRIOT Act. The report also endorses more effective oversight of the intelligence community, and real reform of excessive secrecy.

The report also contains detailed discussion of border and transportation security issues, including airline screening, the "no fly" list that has stranded many innocent travelers, and passenger profiling. By endorsing an expansion of intrusive border screening to domestic travel, the report's recommendations could—if implemented without change—result in a "checkpoint society" in which a federally-standardized drivers license serves as a "national ID" and internal passport.

As the 9/11 Commission itself acknowledges, "many of our recommendations call for the government to increase its presence in our lives. . . ." (p. 395). In fact, as outlined, a number of specific proposals could have serious unintended consequences that would be highly detrimental for basic civil liberties. Legislation must include significant changes to some recommendations to protect civil liberties. The Commission's proposals to advance civil liberties—including increased oversight, reduced secrecy and a Civil Liberties Protection Board—must be implemented to ensure that, as the government centralizes some powers, it provides stronger checks and balances.

No one doubts the necessity of reorienting an intelligence community built to fight the Cold War to focus on the national security threats of the 21st Century. The ACLU strongly favors reforming the intelligence community in a way that enhances national security, encourages openness, and protects civil liberties.

This testimony outlines specific recommendations for how to implement the reforms proposed by the Commission without eroding basic freedoms.

THE NATIONAL INTELLIGENCE DIRECTOR AND NATIONAL COUNTER-TERRORISM CENTER

Recommendation #1: The National Intelligence Director (NID) should not be a Cabinet or White House official and the National Counter-Terrorism Center (NCTC) should not placed in the Executive Office of the President, nor should stronger community-wide powers be given to an official who continues to head the CIA. A new head of the intelligence community, if one is created, should instead head an independent Office of the Director of National Intelligence.

In a democratic society, domestic surveillance must serve the goals of preventing terrorism, espionage and other serious crime, not the political goals of the party in power. As we have learned from past mistakes, the temptation to use the intelligence community to further a political agenda is ever-present.

Misuse of both foreign and domestic intelligence powers for political ends can occur under any Administration. Direct White House control of intelligence powers and access to sensitive intelligence files have been responsible for serious mistakes that undermine civil liberties and accountability, and have lessened the confidence of Americans in their government. For example, the worst spying abuses of the Nixon Administration were directed by White House staff with intelligence backgrounds and included warrentless secret searches to obtain medical records, covert

wiretaps of journalists, and the Watergate break-in itself. Under President Reagan, a covert operation conducted by National Security Council staff member Lt. Col. Oliver North led to the most serious crisis of Reagan's presidency when it was revealed that the operation involved trading arms for hostages and using the proceeds to provide assistance to Nicaraguan rebels. Under President Clinton, White House political staff obtained hundreds of confidential FBI files on prominent Republicans that had been created from extensive background checks designed to protect national security.

In spite of these lessons, the 9/11 Commission's recommendations place effective control over the intelligence community—including parts of the FBI, Department of Homeland Security, and other agencies that exercise domestic surveillance powers—in the Executive Office of the President (the White House) and fail to include any mechanism (such as a fixed term) to ensure the National Intelligence Director's autonomy. The proposal seriously increases the risk of spying for political ends.

The proposed structure centralizes too much power over both foreign and domestic intelligence in the White House, and risks a re-run of the mistakes that led to Watergate, Iran-*contra*, "Filegate," and other significant abuses of Presidential power.

The placement of the National Intelligence Director in the White House could also frustrate Congressional oversight. White House officials have long received, on separation of powers grounds, far less scrutiny from Congress than agency heads and other Executive Branch officials. White House officials are not usually subject to Senate confirmation and do not usually testify before Congress on matters of policy. Executive privilege may be claimed as a shield for conversations between the President and his advisors from both Congressional and judicial inquiries.

President Bush announced on Monday, August 2, a proposal for a national intelligence director that is not a White House or Cabinet official, but instead heads an independent office. Likewise, bills proposed by leading Democratic members of the House and Senate intelligence committees do not make that person a White House official.

Rep. Jane Harman, the ranking member of the House Permanent Select Committee on Intelligence, has introduced legislation to create a "Director of National Intelligence." Like President Bush's proposal, H.R. 4140, the "Intelligence Transformation Act," places the new intelligence director in an independent office, not the White House. The leading Senate legislation takes the same approach. Senate bills include S. 190, the "Intelligence Community Leadership Act of 2003," sponsored by Senator Feinstein (D-CA) and S. 1520, the "9/11 Memorial Intelligence Reform Act," sponsored by Senators Graham (D-FL), Feinstein (D-CA) and Rockefeller (D-WV).

The ACLU supports placing a new intelligence director in an independent office. The National Intelligence Director and the National Counter-Terrorism Center, if they are established, should be accountable to the President, but they should not be servants of the President's political or ideological agenda.

Pitfalls of greater power for head of the CIA. Rep. Porter Goss (R-FL), President Bush's nominee for Director of Central Intelligence (DCI), has introduced a different intelligence reorganization bill, H.R. 4584, the "Directing Community Integration Act." The Goss bill rejects a new intelligence director and instead enhances the powers of the DCI over community-wide responsibilities, including domestic collection of intelligence, while leaving the DCI as the head of the CIA.

The Goss bill is, in some respects, even worse than the Commission's proposal for a White House NID, because it contemplates much greater involvement of the DCI—the head of a foreign intelligence agency—in domestic intelligence matters. The Goss bill would even go so far as to render toothless the current prohibition on CIA involvement in domestic activities by amending it to bar "police, subpoena, or law enforcement powers within the United States, *except as otherwise permitted by law or as directed by the President.*" [1]

The proposed amendment would erase a fundamental limitation on CIA authority that prevents the use of CIA-style covert operations and intelligence techniques—including warrantless surveillance, break-ins, and infiltration and manipulation of political groups—from being used in the United States against Americans.

Recommendation #2: The National Intelligence Director must be subject to Senate confirmation and Congressional oversight, and should, like the Director of the CIA, have a fixed term that does not coincide with that of the President.

Congress must ensure that the National Intelligence Director is appointed by and with the advise and consent of the Senate, and that the NID will regularly testify before Congress. The Office of the NID and the NCTC must also be answerable to

[1] H.R. 4584 § 102(a) (amending 50 U.S.C. § 401–1(c) and repealing § 403–3(d) (emphasis added)).

Congress. Congress must make clear that key officials will be asked to testify and that the NID and the NCTC are expected to provide answers to questions, relevant documents, and cooperate with Congressional inquiries.

The Commission recommends that the Director of the CIA should serve a fixed term, like the Director of the FBI, that does not coincide with the President's term. Insulating the CIA further from political pressure is a welcome step.

Ensuring the intelligence community works well together is an extremely important responsibility that must remain above partisan politics or the appearance of serving an ideological agenda. The President should, of course, appoint the National Intelligence Director, with Senate approval, and should retain the power to fire the director for poor performance. As with the head of the FBI or the Chairman of the Federal Reserve Board, however, the director should serve a fixed term that does not coincide with the President's term.

Recommendation #3: To ensure the FBI retains control of domestic surveillance operations, the head of the FBI's intelligence operations must report to the FBI Director and the Attorney General, not to the National Intelligence Director or another intelligence official.

The United States has—historically and to the present day—entrusted the domestic collection of information about spies, terrorists, and other national security threats to federal and state law enforcement, with the FBI playing the most important role. The reason is simple: Americans do not believe the government should investigate you if you are not involved in a crime—if your activities, however unpopular, are not illegal.

For this reason, the CIA—a pure spy agency with no law enforcement functions—has been barred from domestic surveillance ever since it was created by the National Security Act in 1947. President Truman—a strong opponent of Communism and a hawk on security—shared the concerns of many Americans about the CIA's establishment as a peacetime agency. Truman believed that a permanent secret spy agency could, if allowed to operate on American soil, use espionage techniques—including blackmail, extortion and disinformation—against American citizens who were critical of government policy or the incumbent administration, but had broken no law. With Truman's support, the National Security Act, sometimes described as the CIA's "charter," contains a prohibition—which stands today—on the CIA's exercising any "police, subpoena, or law enforcement powers or internal security functions."[2]

Truman's concerns were not just with bureaucratic turf—whether the FBI or the CIA was the lead agency in collecting information about national security threats within the United States. Truman believed that the domestic collection of information about national security threats should generally be handled as a law enforcement matter. Indeed, Truman often clashed with FBI Director Hoover over whether the FBI had any business using break-ins, illegal wiretaps, and other spy techniques, at one point saying Hoover's advocacy of such methods risked transforming the FBI into the equivalent of the Gestapo.[3] Truman did not just want to prevent the CIA itself from operating on American soil—he wanted to ensure that a CIA-style agency did not become dominant in domestic collection of intelligence about national security threats.

The 9/11 Commission proposes that the NID hires both the FBI's Director of Intelligence and the intelligence chief of the Department of Homeland Security, either of whom may serve as the deputy NID for homeland intelligence. This proposal is very problematic. The Commission proposal puts the FBI's intelligence capabilities in the hands of a super-spy who could involve in domestic spying officials of the CIA and other agencies that use the methods of agencies that operate overseas—such as break-ins, warrantless surveillance, or covert operations.

While a NID could play a role in coordinating the activities of the Intelligence Community, the NID should not be given, as the Commission's proposal currently contemplates, what amounts to control over targets of intelligence collection within the United States. That should remain the responsibility of the FBI Director, under the supervision of the Attorney General.

Recommendation #4: The FBI Director and the Attorney General should have the responsibility to ensure that the guidelines and rules that govern domestic surveillance in both criminal and national security investigations are followed. The guidelines must be strengthened. While they may continue to allow "enterprise investigations" of criminal organizations including foreign and domestic terrorist organizations, they should clearly prohibit domestic spying on First Amendment-protected activity.

---

[2] 50 U.S.C. § 403–3(d)(1).

[3] *See Curt Gentry, J. Edgar Hoover: The Man and the Secrets* (2001).

The FBI's own mistakes and missteps show the dangers of a powerful government agency that uses its investigating authority without regard to whether the subjects of its investigations are involved in criminal activities. To a large degree, these abuses were the result of the FBI's unique lack of accountability to the courts, Congress and even the Attorney General under the direction of FBI Director J. Edgar Hoover.

Today, as a result of the Church Committee reforms, the FBI operates under both internal and external controls that constrain its criminal and national security investigations. These controls are designed to ensure that its intrusive intelligence-gathering and criminal surveillance powers are directed at organizations involved in criminal activities and at the investigation of foreign agents and not at lawful political, religious and other First Amendment activities. Controls that protect civil liberties include guidelines for FBI investigations, constitutional limits enforced by the exclusionary rule, and the "case-oriented" focus of the FBI. Putting a spy chief in charge of parts of the FBI could seriously erode each of these controls.

Domestic terrorism guidelines. For criminal investigations of organized crime or domestic terrorism, Attorney General guidelines restrict the use of most surveillance techniques—such as tracking mail, following suspects, and interviewing witnesses—to situations where there is at least some indication of criminal activity. These guidelines were weakened, following September 11, to allow FBI agents to visit, on a clandestine basis, political and religious meetings that are "open to the public" without any such indication. The ACLU and many members of the House and Senate judiciary committees opposed this change. Most other investigative techniques still do require at least some indication of crime.

International Terrorism Guidelines. National security investigations of international terrorist groups are governed by separate guidelines, important parts of which are secret. The guidelines do not require probable cause of crime but are, in theory, designed to restrict national security investigations to circumstances in which there is some indication of hostile activity by an agent of a foreign power. The most intrusive national security investigations—those that involve physical searches or electronic eavesdropping—must also at least "involve" some possible criminal activity when the subject of the investigation is a United States citizen or permanent resident, although this falls far short of the constitutional standard of criminal probable cause.

Investigative guidelines are vitally important to preserving civil liberties. The government argues that a number of highly intrusive intelligence gathering techniques—including collecting files on individuals and groups, physical surveillance in public places, and tracking the sender and recipient of mail, telephone and Internet communications—are not constitutional "searches" subject to the Fourth Amendment's probable cause standards. As a result, for investigations using such techniques, it is only the guidelines and case-oriented structure of the investigating agency that protects against widespread spying on lawful political and religious activities.

The Constitution and the exclusionary rule. For those intrusive techniques that the government concedes are searches—including electronic eavesdropping of the content of communications and searches of a person's home or office—the Fourth Amendment and federal statutes plainly require court approval based on probable cause. However, the Fourth Amendment's principal remedy, the exclusionary rule that provides illegally-obtained evidence may not be used in court, does nothing to hinder illegal searches and wiretaps if the government does not plan to use the information in a prosecution.

The danger is certainly exacerbated by putting the FBI's intelligence operations in the hands of the government's "top spy" instead of its "top cop." The FBI Director could, of course, direct abuses on the theory that the information is to be used for intelligence purposes rather than criminal prosecution and so need not be gathered legally. The danger would be far greater, however, if the FBI's national security operations are under the effective control of intelligence officials who are used to operating entirely outside the constraints of the exclusionary rule.

The FBI's case-oriented approach. The FBI's focus on both criminal and intelligence "cases" helps prevent highly intrusive and sensitive investigations that may involve religious and political activities that are protected by the First Amendment from losing all focus on crime and terrorism. This focus is vitally important to civil liberties, and could be lost if a spy chief is placed in charge of parts of the FBI.

Critics of placing the FBI in charge of domestic national security surveillance argue that the case-oriented mindset of a law enforcement agency cannot be reconciled with quality intelligence analysis. While the FBI concerns itself with gathering information of relevance to particular cases, they argue, intelligence analysts

must be looking more broadly to see how specific data fits into the "big picture" of a national security threat.

This critique sweeps too broadly because it fails to recognize the difference between two very different kinds of cases. The FBI not only investigates particular crimes—generally, crimes that have already occurred and must be "solved"—it also opens "enterprise" investigations of organized crime and terrorism. For example, in investigating a domestic funding network for Al Qaeda as a possible criminal enterprise, the FBI is not limited to investigating whether the organization was involved in funding specific terrorist bombings or other attacks, such as the 1998 embassy bombings in Africa, the 1999 bombing of the U.S.S. Cole, or the September 11 attacks. Rather, the FBI has authority to investigate the organization as an enterprise, and to fit together bits of information that help prevent future terrorist attacks, not just gather information about past crimes. The FBI's failures in analyzing information about Al Qaeda's domestic activities are not a result of flaws in the basic concept of an enterprise investigation; rather, they appear to be the result of a combination of other failures that must be addressed on their own terms.

Recommendation #5: The powers of the NID and the National Counter-Terrorism Center should be specified by a statutory charter that prohibits powers not authorized and requires the NID to observe guidelines to protect against domestic spying on First Amendment activity. Explicit, enforceable statutory language should make clear that the NID does not have what amounts to operational control of targets of domestic surveillance, whether directly or through the NCTC.

The Commission proposes a powerful new National Counter-Terrorism Center under the authority of the NID. The Center, while not itself a domestic collection agency, would go beyond the analysis of intelligence collected in the United States and abroad that is the function of the existing Terrorism Threat Integration Center (TTIC). If the Center's powers are not specified, and if it is not barred from monitoring First Amendment activities within the United States, the Center could task domestic collection efforts that seriously erode the limits the collection agencies themselves are bound to respect.

The Center would be structured like the CIA. The Center would have separate divisions for "intelligence" and "operations." It would have the authority to "task collection requirements" and to "assign operational responsibilities" for all intelligence agencies—including the FBI—and to follow-up to ensure its mandates are implemented.

The Center's power over both intelligence collection and operations throughout the intelligence community could pose grave risks of encouraging espionage and covert operations techniques on American soil. The Center's tasking and strategic planning functions would extend not only to the FBI's national security investigations, but also to other domestic agencies, including the Department of Homeland Security, with immigration, border control and transportation security functions.

Likewise, some of the powers of the NID and the Center over the intelligence agencies of the Department of Defense—the largest agencies, consuming the large majority of the intelligence community's budget—could have domestic implications. The Department of Defense, after September 11, established a powerful regional Northern Command (NORTHCOM), led by a four-star general, with responsibility for the domestic United States (together with Mexico and Canada).

NORTHCOM already has a military intelligence unit, which raises serious questions under the Posse Comitatus Act—the law that limits military involvement in domestic affairs. Under the proposed structure, the NID and the Center could have what amounts to control of the domestic intelligence operations of civilian federal law enforcement and of the NORTHCOM intelligence unit, creating a real risk of blurring the military and civilian functions.

Recommendation #6: The National Intelligence Director and the National Counter-Terrorism Center should not be permitted to direct or plan intelligence "operations" that include "dirty tricks" or other extra-legal methods within the United States. Domestic use of intelligence information must remain bound by the legal system.

Perhaps the most far reaching power of the National Counter-Terrorism Center is its authority to plan and direct intelligence "operations" throughout the intelligence community. If the NID and the NCTC are created, it must be made clear that information derived from domestic surveillance is only to be used within the bounds of the legal system, and cannot be used for domestic "operations" outside that system.

The FBI's COINTELPRO operations—"counterintelligence" programs under FBI Director J. Edgar Hoover that both gathered intelligence and used that intelligence to disrupt perceived national security threats—led to extremely serious abuses of

power. These abuses included the illegal wiretapping of Martin Luther King, Jr. and the infiltration of scores of social, political and religious groups that opposed government policy, as well as "dirty tricks" campaigns to exploit damaging information without exposing the FBI's sources and methods in a criminal prosecution.

The COINTELPRO programs were initially rationalized as attempts to counter what Hoover perceived as the influence, or possible influence, of the Soviet Union on the civil rights and anti-war movements. However, a lack of internal or external controls led to the continuation of these highly intrusive operations without any real evidence of involvement of a genuine agent of a foreign government or organization and without an indication of criminal activity. In other words, the FBI's most serious abuses of civil liberties occurred precisely when its top leadership forgot it was a law enforcement agency operating to enforce and uphold the law—not a freestanding security or spy agency designed to counter those individuals and groups whose views seemed, to the government officials, to be dangerous or un-American.

If the powers of the National Counter-Terrorism Center are not properly limited, the result could be the establishment of what amounts to just such a freestanding spy agency in all but name. For civil liberties reasons, the 9/11 Commission soundly rejected the idea of moving the FBI's counter-intelligence and intelligence gathering functions to a separate agency patterned on the UK's Security Service or MI-5. The FBI, because of its mission and culture, can serve the intelligence gathering mission that the CIA serves overseas, but the FBI must operate under the U.S. Constitution and "quite different laws and rules." The Commission was also sensitive to the dangers of negative public reaction to civil liberties abuses that would result from creating an agency unconstrained by those rules. A "backlash," it says, could "impair the collection of needed intelligence."

It also objects to the MI-5 idea for these reasons:

- The creation of a new agency, and the appearance of another big kid on the intelligence block, would distract the officials most involved in counter-terrorism at a time when the threat of attack remains high.
- The new agency would need to acquire, train and deploy a vast amount of new assets and personnel, which the FBI already has at its disposal.
- Counter-terrorism very easily ropes in matters involving criminal investigation. With the removal of the pre-9/11 "wall," it makes logical sense, the commission says, to have one agency utilize the entire range of intelligence and criminal investigative tools against terrorist targets.
- In the field, the cooperation between counter-terrorism investigators and the criminal side of the FBI has many benefits.

The Commission was right to reject the model of a domestic intelligence agency. For much the same reason, however, its proposals for intelligence reform must be modified and clarified. 1Reducing Excessive Secrecy and Strengthening Oversight of the Intelligence Community

As the 9/11 Commission observes, structural reform of the intelligence community will not by itself solve basic intelligence deficiencies that contributed to recent intelligence failures. Substantive reforms—including strong internal watchdogs and a civil liberties board, a reduction in excessive secrecy, an increase in real public and Congressional oversight, and stronger efforts to incorporate dissenting views into analysis—must be adopted to prevent future intelligence breakdowns.

Recommendation #7: The Commission recognized its recommendations could increase government intrusion on civil liberties and urged strong oversight. Congress should not act to reorganize the intelligence community without also implementing the Commission's proposals for strong internal watchdogs and an effective civil liberties protection board.

Strong internal watchdogs. Proposals to reform the intelligence community have included the creation of an Inspector General for the intelligence community. The Inspector General would have significant investigative powers, including subpoena power, that would aid internal investigations. An Inspector General for the intelligence community would report directly to the National Intelligence Director and, as a result, could be a more powerful, and more independent, watchdog than the inspectors general that currently have jurisdiction over each of the fifteen intelligence agencies.

Civil liberties protection board. The 9/11 Commission should be commended for recognizing the need to protect civil liberties and endorsing an independent watchdog board to strengthen oversight throughout the government. While various entities and offices within the Executive Branch, such as inspectors general, officers for civil rights and privacy, and oversight boards, are charged with policing certain de-

partments, agencies or programs, no one board has the responsibility for ensuring that civil liberties are not compromised by the need for enhanced security.

The need for such an independent, nonpartisan voice is clear. The Commission recommends putting the burden of proof on the government to show the need for new security powers, such as those enacted by the USA PATRIOT Act, but there is no reliable, independent agency that performs this function. The Commission did not, however, set forth any specific proposals with respect to what a civil liberties board could do.

The 9/11 Commission observed:

> "[D]uring the course of our inquiry, we were told that there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered. If, as we recommend, there is substantial change in the way we collect and share intelligence, there should be a voice within the executive branch for those concerns."

The Commission proposes a board that would "oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."

The recommendation implicitly recognizes that that there is a need for two functions, one proactive and one retrospective. First, a board should be a proactive voice for civil liberties during the development of counter-terrorism policies. For example, during the development of the government's "no fly" list, the board should be asked to study and address civil liberties concerns. How are persons who are mistakenly put on such a list to get off the list? How will the government ensure that innocent travelers who have the same or similar name to a person on the "no fly" list are not harassed?

Second, a board must be able to look retrospectively at patterns of civil liberties abuse, or at significant new programs or laws that intrude on civil liberties. The board could, for example, examine the treatment of terrorism suspects detained on immigration violations or as "material witnesses," but not charged with terrorism. The board could also look at the effectiveness, and impact on civil liberties, of new powers, such as the USA PATRIOT Act, and issue a report prior to the expiration of such powers.

This investigative function should build on the work of others, including the inspectors general of the agencies involved. Because those offices do not have government-wide authority, a board must be able to have the discretion to review and assess the work of inspectors general and other existing investigators, and to go further where necessary.

To complete its objectives, the board must have substantial clout, authority, and powers. It should be bipartisan. Ideally, appointments should be shared between the President and Congressional leaders, if such an appointment process can be reconciled with separation-of-powers concerns. Board members should have independence and should serve a fixed term, and they should be prominent citizens with experience in civil liberties, government investigations, and security. The board should hire an full-time executive director and a staff that permits it to carry out its functions.

The board should have the power to hold public hearings and issue both annual reports assessing the state of civil liberties and special reports that detail the results of investigations. Agencies should be required to respond to their recommendations, and the board should also make recommendations, where appropriate, for legislation. The board should have the power to subpoena documents and witnesses, and should enjoy the cooperation of all departments. Members and staff should have high-level security clearances to enable the examination of even the most sensitive national security secrets.

Recommendation #8: A presumption against classification without good reason was contained in Executive Order 12958 but has been rescinded. As a first step in reforming an outmoded system of secrecy designed for the Cold War, the presumption should be reinstated.

As the 9/11 Commission report recognized, excessive classification—not civil liberties protections—almost certainly represents the greatest barrier to effective information sharing. As the report states, too often the attitude has been that "[n]o one has to pay the long-term costs of over-classifying information, though these costs . . . are substantial." The report laments an outdated, Cold War-era "need to know" paradigm that presumes it is possible to know, in advance, who requires access to critical information. Instead, it recommends a "'need-to-share' culture of integration."

"Groupthink" led to some in the government discounting the possibility that Al Qaeda terrorism was directed at the United States, rather than overseas. According to the Senate Select Committee on Intelligence, groupthink was also the major culprit behind the intelligence failures regarding Iraq's WMD programs. Groupthink cannot be challenged in secret. Public pressure—including the media and public interest groups—can challenge government agencies to reassess their assumptions.

Unfortunately, the Bush Administration has moved in the opposite direction—towards greater secrecy. President Bush's executive order on classification, issued after September 11, not only extended a deadline for automatic declassification of old documents, it actually reversed a presumption against classification without good reason that was put into place by President Clinton in 1995 as a signal to agencies that their classification decisions should have stronger justification.[4]

Recommendation #9: The Freedom of Information Act should be amended to require courts to balance the public's need to have access to information that is critical for oversight of government—such as serious security flaws, or civil liberties abuses such as the mistreatment of detainees—against government claims that the information is exempt from disclosure.

"Need-to-share" cannot be limited to agencies within the government or defense and homeland security contractors, but also must include, to the greatest extent possible, sharing relevant information with the public. Congress and the Administration have created, through the Homeland Security Act, an entirely new category of information that is withheld from public view—sensitive but unclassified (SBU) information. While the 9/11 Commission criticizes excessive secrecy, it also endorses establishing a "trusted information network" for sharing of unclassified, but still nonpublic, homeland security information.

The Commission's calls for greater openness and sharing of information will not be effective if it succeeds only in adding another set of complex secrecy rules designed to limit public access to "homeland security information" on top of the existing classification regime. New categories of secret information—including "sensitive but unclassified," homeland security information, or information in a new "trusted information network"—may succeed only in replacing one unwieldy secrecy regime with another. The need for government and industry to keep critical infrastructure information from the public must be balanced against the public interest in access to critical oversight information. The Freedom of Information Act should be amended to require this.

Recommendation #10: Congress should enact H.R. 2429, the Surveillance Oversight and Disclosure Act, sponsored by Rep. Hoeffel (D-PA), or its Senate counterpart, S. 436, the Domestic Surveillance Oversight Act, as a first step towards making more information about the use of FISA available to the public.

The Commission calls for a debate on the USA PATRIOT Act, putting the burden on the government to show why a given power is needed. However, the government still takes the position that its use of surveillance authorities under the Foreign Intelligence Surveillance Act (FISA) is classified, and that the public's right to know only extends to the total number of surveillance applications made and the total number of orders granted. There can be no meaningful debate on the government's use of the USA PATRIOT Act, which expanded FISA surveillance powers, without any publicly-available objective data on such basic matters as how many surveillance orders are directed at United States persons, how many orders are for electronic surveillance, how many are for secret searches of personal records, and so on.

Rep. Hoeffel has introduced legislation (H.R. 2429) that would provide more public information about the use of FISA, and Senators Leahy, Specter and Grassley have introduced a similar measure (S.436).

Recommendation #11: Congress should enact H.R. 4855, sponsored by Rep. Bud Cramer (D-AL), which establishes a bipartisan classification review board, or its Senate counterpart, S. 2672, the Lott-Wyden bill. Congress should consider enhancing the board's power to release improperly classified documents. The Senate Select Committee on Intelligence should also make clear it will wield its existing power under the Senate rules as an effective check against intransigence by the President in releasing classified information that the board recommends to be released.

The Congress should enact H.R. 4855, sponsored by Rep. Bud Cramer, the "Independent National Security Classification Board Act of 2004." An identical bill, S. 2672, has been introduced in the Senate by Senators Trent Lott (R-MS) and Ron Wyden (D-WA).

---

[4] Further Amendment to E.O. 12958 (March 25, 2003); See Adam Clymer, *U.S. Ready to Rescind Clinton Order on Government Secrets*, N.Y. Times, March 21, 2003.

The bill would create a bipartisan board, appointed by the President and members of Congress, to review and reform classification rules. The board should consider whether a complex system of government secrets that has grown to include layers upon layers of bureaucratic rules is the best way to safeguard the national security, and recommend real reforms.

Recommendation #12: The intelligence committees should hold far more open hearings. The annual hearings on legislation authorizing the intelligence community—as well as other legislative hearings—should be open to the public.

The 9/11 Commission called for Congressional oversight to be greatly improved, calling the current structure "dysfunctional." As the Commission made clear, the establishment of a Senate and House committee devoted to intelligence matters does not provide effective oversight when hearings—even hearings on legislative matters—are almost always closed to the public

Recommendation #13: The intelligence budget should be made public as the Commission recommends.

Perhaps the most inexplicable example of excessive secrecy that frustrates real accountability is the continued insistence by the intelligence community on keeping basic information—even information that is widely known or guessed—classified. Even the overall amount of money budgeted for intelligence activities, which is widely reported as being approximately $40 billion, is classified as is the amount of money budgeted for components of the intelligence community. At least these numbers, and other information that would help the public know how its dollars are being spent, should be made available.

Recommendation #14: While Congress should consider ways to consolidate and strengthen oversight of the intelligence community, the intelligence community should not be shielded from the oversight of relevant committees. Most importantly, the House and Senate judiciary committees must retain jurisdiction that is concurrent with the intelligence and homeland security committees over domestic surveillance, access to the courts and other government actions that affect legal and constitutional rights.

The Commission's other recommendations include investing the intelligence committees, or a joint committee of both Houses of Congress, with authorizing and appropriations powers over the intelligence communities. This proposal should be approached with caution. Limiting the number of committees with jurisdiction over the intelligence community may frustrate oversight instead of enhancing it. If the single committee with jurisdiction over intelligence does not ask probing questions concerning a given program or policy, there will no longer be the potential for another committee to fill the void.

Most importantly, the judiciary committees of the House and Senate must retain concurrent jurisdiction over intelligence matters affecting legal and constitutional rights. A more powerful intelligence committee should *not* have the exclusive or final say on amendments to the Foreign Intelligence Surveillance Act or other sensitive surveillance statutes, for example. The same need for some concurrent jurisdiction in the judiciary committees arises if Congress adopts the Commission's proposal for permanent committees to oversee the Department of Homeland Security.

Recommendation #15: Congress should enact H.R. 3281, the Platts bill, or its Senate counterpart, S. 2628, the Akaka-Grassley bill, providing special protections for national security whistleblowers.

Finally, a thorough and comprehensive review of the treatment of national security whistleblowers must be part of any reform of the intelligence community. The role of whistleblowers in assisting our understanding of pre 9/11 intelligence failures has been essential.

National security whistleblowers face unique obstacles. Many intelligence and national security jobs are exempt from the civil service protections, including whistleblower protections, enjoyed by most government employees. National security whistleblowers also face additional hurdles, such as the loss of a security clearance or possible criminal charges for allegedly disclosing classified information, that are not faced by most government whistleblowers.

The 9/11 Commission's calls for reform of the intelligence community that would challenge conventional wisdom should include specific procedures that would encourage whistleblowers. Additional safeguards, consistent with national security, must be enacted to encourage employees who see distorted and sloppy analysis or other serious shortcomings to come forward without fear of losing their jobs, security clearances, or going to prison.

THE USA PATRIOT ACT

Recommendation #16: Congress should adopt the 9/11 Commission's framework for determining whether to extend controversial provisions of the USA PATRIOT Act when they expire next year, which puts the burden on the government to show why powers are needed *before* examining the impact on civil liberties. In particular, Congress should wait until next year to decide whether to re-authorize the sections of the law that sunset so as to preserve an adequate opportunity for the debate for which the Commission called.

During the rush to enact the USA PATRIOT Act after September 11, the White House and Attorney General implied that if changes to the law did not pass quickly, and there was another terrorist attack, the blame would rest on Congress. Not surprisingly, the law passed by wide margins: 96 to 1 in the Senate, 357 to 66 in the House. Since then, however, numerous lawmakers have expressed reservations, and many, including members of the Subcommittee, are actively seeking to refine the law to better protect civil liberties.

Congress wisely included a series of "sunset" provisions in the law, which would require Congress to reauthorize certain provisions or let them expire by December 31, 2005. The Administration has asked Congress to act this year to remove the sunset provisions, which would make the entire law permanent.

The 9/11 Commission report unequivocally said that the government has the responsibility for defending the expansions of government power that are the hallmark of the USA PATRIOT Act. The Commission could have, but did not, endorse the PATRIOT Act and call for its renewal. Instead, the Commission called for a "full and fair debate" over the need for these new powers, with the burden of proof resting on the government to show why a power is needed. In our view, the Department of Justice has not to date met this burden—particularly with respect to the most controversial parts of the USA PATRIOT Act. These sections relate to secret searches and access to library and other records, either under a minimal level of judicial review under Section 215, or with no review at all in the case of National Security Letters in Section 505.

The 9/11 Commission also recommended that expansions of government power must come only with adequate supervision of the executive's use of the powers to ensure protection of civil liberties. This is a very important recommendation. We believe that enacting the Security and Freedom Ensured Act ("SAFE" Act), H.R. 3352 (and S. 1709 in the Senate) is an important step that Congress could take to increase judicial, Congressional and public supervision.

A NATIONAL ID CARD

Recommendation #17: Congress should reject any proposal to (1) make state-issued driver's licenses into a common license that is federally-designed, but issued by the states, (2) require licenses to contain an embedded computer chip bearing the holder's biometric identification information (i.e. a fingerprint or retina scan and digital picture), or (3) link the ability to obtain a drivers license to immigration status.

While the 9/11 Commission did not endorse a national identification card *per se*, its recommendations for federal standards for drivers licenses would almost certainly amount to a back-door way of accomplishing the same objective. Rep. Cannon (R-Utah) pointed this out at a hearing on August 20.

Even during periods of national threat, most notably the Cold War and World War II, the country has never thought it necessary to require citizens to carry "papers" with them at all times. If Congress did so now, it would endanger both security and civil liberties.

Once federalized, drivers licenses would be demanded for all manner of personal transactions that do not now require one. Moreover, federalized licenses would be the key that accesses personal information about the holder that would be inevitably linked to the license. Today, that information would include obvious identifiers such as Social Security Number and address. But tomorrow, it would include less obvious identifiers, and not just fingerprints and retina scans. Many businesses—from landlords to retailers—would themselves, or through the government, seek to tie personal information to the federalized drivers license, and they would not allow routine transactions unless a person produced their federalized drivers license.

Some states have decided that drivers licenses should be issued to those who can prove that they can drive, as opposed to those who can also prove that they are in the country lawfully. They have decided that it serves their public safety needs to ensure that all drivers are licensed regardless of immigration status. Congress should not step in to upset this determination.

Moreover, the same people who produce fraudulent state identification documents today would produce fraudulent federalized identification documents tomorrow. The fraudulent federalized documents would be used not only by those seeking to commit fraud, but by those intending to do much more serious harm.

Finally, Congress has considered, and ultimately rejected, this proposal before. This proposal is very similar to Section 656(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. The regulation the Department of Transportation proposed to implement Section 656(b) was roundly criticized as a system of national identification, and was never implemented. The regulation that the DOT proposed drew literally thousands of negative comments from members of the public. Congress wisely repealed the provision in a subsequent transportation appropriations bill.

A much better approach would be for Congress to fund state efforts to make drivers licenses more secure.

AIRLINE PASSENGER PROFILING AND "NO FLY" LISTS

Recommendation #18: Before the TSA begins administering no-fly lists, Congress should ensure that there is some independent review, subject to appropriate security measures, of how someone gets on the no-fly list. For travelers who find themselves wrongfully included in the no-fly list, there must be some process for them to clear their names, and the TSA should be required to track the number and cost (both to effectiveness and civil liberties) of "false positives."

The 9/11 Commission took no position on whether the passenger profiling system known as CAPPS II should go forward. Moreover, its factual findings suggest that the approach taken by the proposed CAPPS II—to subject every commercial air passenger to an invasive background check against business and intelligence databases—is not necessary to ensure airport security.

However, the Commission did endorse broad expansions of "no-fly" and "automatic selectee" lists, and that screening against these lists should be performed by the Transportation Security Administration, instead of by the airlines, as is now the case.

The ACLU has long-standing concerns about the use of federal watchlists. While it does not oppose the concept of a watchlist per se, the practical use of such tools is fraught with peril for civil liberties. As currently administered, the no-fly list has spawned stigmatization, interrogation, delay, enhanced searches, detention and/or other travel impediments for innocent passengers. These innocent passengers can include prominent Americans such as Senator Ted Kennedy, who recently revealed that he was on the "no-fly" list for weeks, and people with the same name as terrorist suspects, such as the four innocent "David Nelsons" who were repeatedly stopped in the airport because their name was on such a list. ACLU has filed a lawsuit seeking to vindicate the due process rights of people on the list. *(www.aclu.org/nofly).*

Expansion of the "no-fly" and "automatic selectee" lists, as proposed by the 9/11 Commission, should not go forward unless the TSA establishes adequate policies and procedures to ensure that the right people are on the list, people who are wrongly identified as terrorist suspects have a way of getting off of the list, and there is an independent review of the criteria used to put a person on one of the lists. The ombudsman process that the TSA has established has not to date proven adequate to accomplish these ends.

There is also some ambiguity in the report, which could result in parts of CAPPS II making their way into a reformed passenger screening system. Most notably, the commission's recommendations that the air carriers turn over all necessary information about their passengers to implement any new screening system could open the door to the same kinds of problems with the CAPPS II proposal. The TSA must not use this as an opening to engage in the dragnet screening of every air traveler. Suspicion must still be individualized, and based on reliable indicators of threat, not whimsy, bias or unproven profiling schemes.

BORDER SECURITY AND IMMIGRATION

Recommendation #19: While improved border security is important for national security, the report's "integrated approach" recommendation should not be implemented in a manner that creates what amounts to an "checkpoint society" or internal passport system. Discriminatory profiling should be rejected.

The 9/11 Commission recommended that the U.S. border security system be integrated into a larger network of screening points that includes our transportation

system and access to vital facilities, such as nuclear reactors. While border security screening needs to be improved, it should not be converted into a system of internal checkpoints at all major transportation systems.

Major transportation systems include trains, light rail, inter-city bus systems, intra-city bus systems, and subway systems such as the Metro system here in Washington, D.C. The process for boarding a Metro train should not be integrated into the system designed for those crossing the border. To do so would not only bring internal transportation to a crawl, but would fundamentally change the character of American society by creating a system of internal checkpoints. One should not have to scan a passport—or a federalized drivers license—to board a bus or hop on a subway train.

We do not believe that the 9/11 Commission meant to call for such a system, and we encourage members of the Commission to clarify this recommendation.

Rejection of discriminatory profiling and the "special registration" for visitors from Arab and Muslim countries. The 9/11 Commission essentially rejected any border security scheme that singles visitors out based on national origin or other categorical criteria. None of its recommendations should be construed as supportive of any such system. The report says: "We advocate a system for screening, not categorical profiling. A screening system looks for particular, identifiable suspects or indicators of risk. It does not involve guesswork about who might be dangerous." (pg. 387).

We are hopeful that the Administration will interpret this recommendation in a way that ensures that the US VISIT program does not follow the path of its predecessor, the National Security Entry-Exit Registration System, or NSEERS. NSEERS singled young men visiting the United States from certain Muslim and Arab countries out for heightened scrutiny and forced them to register with the government; Congress should ensure that US VISIT does not go down this road.

Conclusion

Increased threats of terrorism after September 11, 2001, lightening-fast technological innovation, and the erosion of key privacy protections under the law threaten to alter the American way of life in fundamental ways. Terrorism threatens—and is calculated to threaten—not only our sense of safety, but also our freedom and way of life. Terrorists intend to frighten us into changing our basic laws and values and to take actions that are not in our long-term interests.

Proposals for fundamental reforms of the intelligence community are particularly sensitive because of the fundamental tension between intelligence gathering and civil liberties. Where government is focused on gathering intelligence information not connected to specific criminal activity, there is a substantial risk of chilling lawful dissent. Such inquiries plainly have a chilling effect on constitutional rights.

The answer is not to reject all intelligence and other reforms. The answer, instead, to ensure that specific safeguards for domestic collection of intelligence information that preserve the role of the FBI while ensuring against the use of spy tactics against Americans through strengthened guidelines and other checks to bar political spying. Greater openness, real accountability to both Congress and the public, and protection of whistleblowers is vitally necessary to challenge old assumptions and ensure better analysis and performance. If watch lists are used that have real consequences to those errantly on the list, then there must be a way to ensure that innocent people are not mistaken for dangerous ones, and to ensure that they can get off the list.

The 9/11 Commission should be applauded for avoiding the easy—and wrong—scapegoating of civil liberties and human rights protections for intelligence failures. The commissioners clearly understood that in order for America to remain strong and free, any reform of our intelligence or law enforcement communities must reflect the values and the ideals of our Constitution.

While we take exception to some of the 9/11 Commission's recommendations, such as the federalization of drivers licenses, we take heart from others, such as the call on government to justify broad expansions of power.

The challenge to our intelligence community is the same as the challenge to Congress, and for the nation as a whole. Securing the nation's freedom depends not on making a choice between security and liberty, but in designing and implementing policies that allow the American people to be both safe and free.

APPENDIX

9/11 COMMISSION RECOMMENDATIONS
SUMMARY OF CIVIL LIBERTIES SAFEGUARDS

National Intelligence Director, Counter-Terrorism Center must be accountable, not political

1. Intelligence director should not be White House official, but should be independent office, counter-terrorism center should not be in White House, and head of CIA should not be given more powers over domestic surveillance.
2. Intelligence director should be subject to Senate confirmation and should have a fixed term, like FBI Director and new Director of the CIA; President can fire for cause.

Make sure a "top cop," not a "top spy" remains in charge of domestic surveillance

3. Head of FBI intelligence operations must report to FBI Director and Attorney General, not intelligence chief;
4. FBI Director and Attorney General should be required to make and enforce guidelines prohibiting spying on First Amendment protected activity;
5. Powers of intelligence director and counter-terrorism center should be specified by statute, and other activities barred. Explicit, enforceable language should make clear intelligence director does not have effective control of domestic surveillance, whether directly or through counter terrorism-center.
6. No "covert operations" on American soil—use of domestic intelligence must be bound by legal system;

Reduce excessive secrecy, improve accountability

7. Create strong Inspector General and other internal watchdogs for intelligence community; create Civil Liberties Protection Board with real power to investigate abuses and prompt corrective action;
8. Restore presumption against classification for no good reason in prior Executive Order;
9. Amend Freedom of Information Act to provide that exemptions for new categories of unclassified, but nonpublic, information must be balanced against public interest in disclosure;
10. Enact legislation (e.g., S. 436/H.R. 2429) increasing public reporting on use of Foreign Intelligence Surveillance Act (FISA) that governs FBI national security wiretaps, secret searches, and records demands within United States;
11. Enact Lott-Wyden bill (S. 2672/H.R. 4855) establishing bipartisan classification review board, and make clear Senate is prepared to release information on board's recommendation if President is intransigent;
12. Intelligence committees must hold more open hearings, and open all legislative hearings;
13. Make intelligence budget public;
14. New and stronger committees to oversee intelligence community and Department of Homeland Security must allow for oversight by other relevant committees. Judiciary committees must have concurrent jurisdiction over domestic spying and other actions affecting constitutional rights.
15. Enact legislation (e.g., S. 2628/H.R. 3281) to provide specific protections for national security whistleblowers.

The USA Patriot Act

16. Congress should adopt the 9/11 Commission's framework for evaluating the USA PATRIOT Act, which puts the burden on the government to show a power is needed.

Border and Transportation Security

17. Congress should reject proposals to federalize drivers licenses and thereby turn them into a national ID that links databases and mandates immigration restrictions.
18. Standards for "no fly" and other watchlists must be enhanced to ensure there is clarity about how a person gets on a list, how the "same name" problem can be addressed, and how a person gets off.
19. Tracking "terrorist travel" should not be accomplished by a system of internal "checkpoints" that requires Americans to carry what amounts to an internal passport. Discriminatory profiling should be rejected.

Mr. COBLE. I commend you witnesses. You complied very consistently with our request for the 5-minute rule. You know, folks, time

is a very precious element in this hectic era in which we live. There is another 9/11 hearing being conducted simultaneously, at least one more on the Hill I know of. But in view of the significance of this hearing, I believe that we will have a second round of questioning. This will permit the Members to examine you all on a second round.

Having said that, Mr. Kojm, a new report from the staff of the 9/11 Commission was released just this morning. And I don't mean to be critical—well, strike that. I guess I mean to be critical, unless there was a good reason for our not getting it prior to this morning. If we could have gotten it earlier, it would have been of great help. But in any event, this report that we just received this morning details the lax controls on immigration and customs that the hijackers exploited to carry out their plot, beginning by acquiring false visas in April 1999.

Mr. Kojm, if you could expand on these new developments and what recommendations you can make with regard to improving visa tracking and entry exit security.

Mr. KOJM. Mr. Chairman, first with respect to release of the report, this was a staff report neither endorsed by nor reviewed by the commissioners. And we needed to put it out before the Commission went out of existence, which was on Saturday. And we had a full complete process of prepublication review with the executive branch which only concluded very late on Friday. So that explains why it was released so late. And, of course, we apologize that this Committee did not have sufficient time to review it before this hearing.

Mr. COBLE. Well, that diminishes my criticism, then.

Mr. KOJM. Mr. Chairman, with respect to the recommendations of the Commission, they remain the same. The staff report essentially provides more detail on the same questions, but we believe strongly that it is critical that terrorists' travel intelligence be integrated into all agencies that have responsibility for border security.

For example, it was quite startling to us that the people in the Department of Homeland Security, who have responsibility for borders, did not even know the names of their counterparts in the Intelligence Community who work on these very issues with respect to terrorism travel. Now, that's not the kind of relationship that our Government needs to have. What we believe here is that there needs to be a very close relationship, an operational one, so that what is known by the experts in the Intelligence Community, that this information gets right to the border inspectors, to the consular officials, that they can punch numbers and buttons on their screens. This information is available to them. Otherwise, we can do all the great intelligence work we want, but if it's not available to our point people on the line every day, then it's not making a difference. And I'll just stop right there. Thank you.

Mr. COBLE. Mr. Nojeim, it has been suggested by some that the Congress immediately implement all of the 9/11 Commission recommendations for the safety of the American public. What is your response to that?

Mr. NOJEIM. We believe that the Congress ought to move very carefully and very cautiously, and that a rush to implement all of the provisions at once would probably be a mistake. It would be im-

portant for the Congress—and I think that the Commission expected this—to examine each recommendation very carefully, make an assessment, bringing in experts such as the people at this table to assess whether the recommendation makes sense, have a full debate about it, and take whatever time is necessary.

Mr. COBLE. I'm inclined to agree with that. I think a deliberate rather than an accelerated response probably is more desirable.

Mr. Pistole, according to the Commission staff report on terrorist financing that was released Saturday, the CIA is developing institutional and long-term expertise in the area of terrorist financing. How does this role complement the role of the FBI's terrorist financing operation section?

Mr. PISTOLE. Mr. Chairman, the FBI and CIA have a very close working relationship in the area of terrorism financing since 9/11. The terrorism financing operation section of the FBI is actually the largest of the 10 sections of the counterterrorism division, with over 150 people working just on terrorism financing at our headquarters. We also have terrorism financing coordinators in each of our 56 offices who work very closely with FINO from the Counterterrorist Center of the CIA on both international and domestic terrorism financing matters. It is a very proactive, operationally focused effort with a number of different private sector entities involved in that.

Mr. COBLE. I thank you. I see the red light now illuminates in my eye. I want to revisit this with you on the second round, Mr. Pistole. The gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. When we talk about reorganization there's a difference between just reorganizing things and actually improving things, especially when reorganization brings with it some inefficiencies. Just mention the fact that some people didn't know their counterparts. When you reorganize, nobody is going to know anybody.

Exactly what information was not gathered under the present system that, if you reorganize all the boxes, would have been gathered and what could have been done with it under a new organization that could not be done under the present organization if people would just do their jobs better?

Mr. KOJM. Mr. Scott, let me begin—first of all, thank you for the question. We on the Commission do appreciate the changes have been made since 9/11 and that they have been important changes, largely, we believe, in the right direction. But we believe that change has not been sufficient. We still are dealing with Cold War institutions. And the national security threat we face today is fundamentally different from any we faced in the previous two generations. So we believe that the institutions of Government must reorganize. Two stories, briefly. We caught——

Mr. SCOTT. Let me stop you there. Just reorganizing—sometimes when you have a problem and you don't like the status quo, the suggestion is therefore you must agree with the proposed change. Sometimes the proposed change isn't any better than the status quo. My question is how is the proposed change going to make—what is the proposed structure going to do better necessarily than the old structure, particularly when you have people knowing each other a little bit on this side and, if you can just improve the way

they're doing their jobs, will that do a better job than reorganizing everything?

Mr. KOJM. Mr. Scott, fundamentally we believe the answer to that question is no. Good people are working together and working together better, but they are still hampered by, we believe, bad structures. We believe the risks for the Nation are greater if we do not change than the risks that always accompany periods of change and transition.

Simply one story from 9/11 that we find powerful is of Kuala Lumpur where in January of 2000 we saw two future hijackers, we caught a glimpse of them. The CIA did a very good job tracking those people. The trail was lost in Bangkok. Ultimately those two hijackers came to the United States. That information never was passed to the FBI until August of 2001. We could have made a significant difference and we believe it is certainly possible that we could have disrupted that plot had there been better——

Mr. SCOTT. What would have happened to the information under the new structure?

Mr. KOJM. Under the new structure, under the national counterterrorism center, the FBI and CIA would be living together, sharing this information on a daily basis. There would be a quarterback in charge. So when the trail was lost in Bangkok, there would be someone who knew it was lost and would give an order to make sure that the case was followed, that the case was managed and that the case was not dropped, as occurred in the 9/11 story.

Mr. SCOTT. And that means everything goes into the TTIC. Is that——

Mr. KOJM. Well, this would be the national counterterrorism center that we believe needs to built on the good foundation that was started with the creation of TTIC that Mr. Brennan heads.

Mr. SCOTT. What would happen to TTIC under this new structure?

Mr. KOJM. Well, I think Mr. Brennan's words are apt. It is a good foundation, but a foundation is not the same as the house. We believe that the head of the national counterterrorism center needs people assigned to him, not detailed to him. He needs tasking authority. He needs to conduct strategic analysis. He needs to conduct warning. He needs to have more power over the analysis of information and he needs a counterpart who plans joint intelligence operations under the leadership of the head of the national counterterrorism center.

Mr. SCOTT. Mr. Brennan, you want to comment on that?

Mr. BRENNAN. I agree with some of the things that Chris said, but I don't think that structural change would have made a difference as far as that information that he was referring to as far as Malaysia is concerned. Having a quarterback in charge of those different elements doesn't mean that that quarterback is going to know every single bit of data that resides within the terrorism arena. And there are terabytes of data.

I think what is most important is to have an information sharing architecture and system that will allow the information to get into the appropriate databases that can be then pulsed by FBI, CIA, and other offices as appropriate. And I happen to be, again, a pro-

ponent of some reform, but I don't think it would have addressed the issue that you raised, as far as—or that Chris raised there.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman. The gentleman from Florida, Mr. Feeney.

Mr. FEENEY. Thank you, Mr. Chairman. And thank all of you for your testimony. I was here on Friday when we had Mr. Hamilton and Senator—Slade and others testify on some privacy-related matters. I hope to take that up with Mr. Nojeim in a minute.

But, Mr. Kojm, I am this morning. We did get a copy of addendum of materials that add to the 9/11 report. So we haven't been able to get through that entirely. But one of the new things that is suggested appears in the report, is that in 1992 a manual produced by the CIA known as the "Red Book" which advised border and security agents in how to deal with the potential targeting and identification of terrorists or threats to security was discontinued as a training tool for those border agents in 1992.

Was the Commission able to determine why the training was discontinued? Was there any document that was used to replace training for our security or immigration or border clerks? And if not, in light of the World Trade Center bombing in 1993, what was done to try to put our people in charge of protecting our borders on notice that there were ways to try to detect potential threats?

Mr. KOJM. Mr. Feeney, thank you for the question. The question you asked about the Red Book is exactly the same one that we wrestled with. I'm not sure we got a fully satisfactory answer. Part of the reason it was discontinued in 1992, we believe, is because it was felt that it was compromised. This book we shared with counterpart foreign governments and liaison services, and they found it very useful. But we do believe it was compromised—the Commission was told this—and for this reason it was discontinued.

The maddening question, of course, though, is why wasn't this replaced with either an electronic database or some other kind of system and training? We don't have a good answer for that.

As to your second question, after the first World Trade Center bombing, there was a significant effort to modernize and update the State Department's watch list. And it was computerized, with assistance from the Intelligence Community, into what became known as the tip-off look out system, which had 60,000 terrorist names in its database at the time of 9/11. Unfortunately, the names of the hijackers, of what turned out to be three of them, were not entered until August 23, 2001.

Mr. FEENEY. Thank you. I hope to come back to that.

Mr. Nojeim, I guess this an opportunity to take up some of your testimony. By the way, I was struck by how much of it I actually agree with, at least with respect to the concerns that I have. I don't always agree with positions of the American Civil Liberties Union, but I do agree that the privacy and civil liberties is the foundation for what makes America great. Appreciate that.

Along those lines there's a wonderful book written, believe it or not, by our Chief Justice Rehnquist, called "All the Laws But One" which talks about the pendulum between civil liberties and securities. It was issued in 1987, 15 years before the September 11 at-

tacks. We're going through one of those periods where rebalancing civil liberties and new security threats is necessary.

Some of your concerns, maybe not specific recommendations I agree with, are concerns about the national ID card; the potential use of surveillance domestically to infiltrate and manipulate political organizations; the fact that the national intelligence director, if we're going to create one, ought to have some responsibility in answering to Congress, including potentially Senate confirmation; and the concern that FBI and domestic surveillance not be allowed to engage in ad hoc spying across the board; that there ought to be specific incidents or threats before we turn spies loose on citizens.

One of the things I probably disagree with the ACLU, the protection for American citizens as opposed to noncitizens. I think that there are two very distinct categories under our Constitution. But some of your positions are troubling. For example, you suggest that it's inappropriate for domestic intelligence officers to show up at public meetings and find out what people are saying. If the KKK Grand Wizard was having a discussion about what to do, legally or illegally, I think we would want people at a public meeting in that audience. Same thing, if a Nazi rally. ACLU supported the right of Nazis to march through Skokie, Illinois for example.

At the upcoming GOP Convention, the ACLU officers have expressed skepticism about some of the surveillance that the FBI is doing on Web sites and people that have actually suggested using Molotov cocktails, sling shots, bolt cutters, et cetera, people that have not only refused to renounce violence, but in the name of apparently peace are suggesting that we ought to have some violence against at least property if not persons.

Can you tell me where we draw the line about the use of American domestic officers attending public meetings and going to places where the discussion of terrorist activities or threats is actually out in the open?

Mr. NOJEIM. Yes. Yes, I think I can be helpful on that. We believe that the FBI should follow up when it has a lead; that it shouldn't be monitoring what every political group, what every religious group is saying when it's meeting and not engaging in any criminal or otherwise unlawful activity. When the FBI has a lead, it should be able to go in and watch and listen and gather information. That was the old rule. That was the rule under the FBI guidelines before they were changed in May of 2002. Now the rule is that the FBI can go to any political meeting and monitor what people are saying, even though it doesn't have any evidence that anybody is up to anything that's unlawful.

Mr. COBLE. The gentleman's time has expired. The gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much Mr. Chairman. Let me add my respect and appreciation for the Chairman and the Ranking Member for convening this hearing. I serve as a Member of the Homeland Security Select Committee, and we too had hearings along with a number of other Committees.

Allow me in my respect as well for the witnesses and, of course, the Commission to really offer my debt of gratitude, although they know that they wished that more could have come from those of

us who serve in public policy positions—that is the families of the 9/11 victims, those who lost their lives and those who suffer still today from the tragedy and the enormity of that day—and offer an apology for the failures of this Government and our systems, infrastructure.

I think more than ever as we have received the 9/11 Commission report, we should never forget that this Government failed the American people. Mr. Chairman, this is not accusatory, because you're right; it's not important to point as to who and why. I think the 9/11 Commission has appropriately thrown a large net and all can stand under it. But my great concern as we have these meetings and these hearings, although very appropriate, I think it is important to note for the Members of this body as well as the American people, that this Congress is not convened for legislative business; that those of us who have written legislation and are prepared to move and work on initiatives that I think are imperative to act on—the recommendations of the 9/11 Commission—are barred from performing our duties because our leadership has failed to convene, if you will, the legislative process that is necessary.

I hope that as we proceed that there may be an opportunity, even before the end of August, maybe in the first weeks that we return, that immediate legislative action could be included so that all the worries that have been expended both in these hearings and in the 9/11 Commission report would certainly provide us with an opportunity for action. I think, if anything, we owe this to the American people. And we certainly owe this to the many, many members of the 9/11 families who were persistent, determined, and with great passion for this Commission to exist and for its report to come in finally.

Let me add to the record my comments on the Chairman's comments about this report that came out in the last days of this past weekend, and only say that I hope that the lateness of it—and I appreciate your explanation and recognize that there is a sense of, if you will, tediousness and bureaucracy when we're trying to move paperwork, but I really would hope that this had nothing to do with political vetting. We have not had a chance to read this. And I hope that it's not the case of let's cover ourselves and not let any information get out. I would have hoped—and I have this document here—that we would have been able to read it. Maybe in the next question I would have gotten a sentence or two on it. Because our Committee that I serve on on Immigration would, I think, benefit from having the review of this document. And I think that might be an appropriate hearing for us.

Mr. Chairman, allow me to ask to submit into the record the first page of my legislation dealing with elevating or making the director of intelligence a Cabinet position. I am delighted to be joined by Senator Roberts. My legislation was written on August 11, 2004. It would have been nice to be in session so it could have been filed. I would ask to submit the first page into the record. I ask unanimous consent.

Mr. COBLE. Without objection.

[The information referred to follows:]

108TH CONGRESS
2D SESSION

H. R. _____

To establish the Director of National Intelligence as a cabinet level position in the Executive Office of the President to oversee budget, operations, and personnel of the entire intelligence community of the Federal Government.

IN THE HOUSE OF REPRESENTATIVES

Ms. JACKSON-LEE of Texas introduced the following bill; which was referred to the Committee on _____

A BILL

To establish the Director of National Intelligence as a cabinet level position in the Executive Office of the President to oversee budget, operations, and personnel of the entire intelligence community of the Federal Government.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 "Director of National Intelligence Act of 2004".

6 (b) TABLE OF CONTENTS.—The table of contents for
7 this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

Ms. JACKSON LEE. I also ask unanimous consent to submit into the record the FAIR Act of 2004, written on August 4th, 2004.

F:\M8\JACKSO\JACKSO.259 H.L.C.

[DISCUSSION DRAFT]

AUGUST 4, 2004

108TH CONGRESS
2D SESSION

H. R. _____

IN THE HOUSE OF REPRESENTATIVES

Ms. JACKSON-LEE of Texas introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Homeland Security Act of 2002 to establish a fund for purposes of providing aid to areas of exceptionally high threat level.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. FUNDS FOR AREAS OF EXCEPTIONALLY HIGH**
4 **THREAT LEVEL.**

5 (a) ESTABLISHMENT OF FUND.—Title V of the
6 Homeland Security Act of 2002 (6 U.S.C. 311 et seq.)
7 is amended by adding at the end the following new section:

F:\V5\080404\080404.027
August 4, 2004

Again because we're not in legislative session, this bill cannot be introduced. It deals with funding vulnerable areas so that if it is determined on a threat assessment basis that your area is more vulnerable than others, without any disrespect to any other areas of the United States, this legislation would be appropriate.

I do that in the name of understanding the works of local authorities. And I want to make note that the port of Houston today is opening their new communication system that deals with local authorities who are trying to follow the 9/11 Commission report and coordinate, if you will, all of the items that they have.

I see my time is out in terms of a question. I will just say this, Mr. Chairman. I understand that have you a second round of questioning.

Mr. COBLE. There will be a second round.

Ms. JACKSON LEE. If you would allow me 10 seconds to make mention of this, it will lay the groundwork for the questions in the second round, the approach that I will take on national IDs and standardized questions. Sitting in a jailhouse in Houston, Texas, very quickly I will say this is an Indian national. He has a 6-month visa. He is in fact in this country legally. He was detained as an elderly citizen at the Houston airport on the grounds of having knives. They were decorative knives that all of us know from the Indian culture and other places, brought for his daughter. He was detained by Homeland Security and Customs. They looked at the decorative knives and ultimately cleared him. What happened? District Attorney Rosenthal, our local district attorney now, has him in a Harris County jail for 30 days under the pretense of possessing illegal weapons. In the midst of that, our Homeland Security has put a hold on him. Why? Because the local authorities asked for that; not because he is here illegally, not because he has ever been an overstay, not for any other reason other than overreach and abuse. We must be fearful of a system that pretends to protect us and yet follows in a trend that undermines the Constitution of the United States of America.

Ms. JACKSON LEE. I look forward to asking questions to the witnesses in the next round

Mr. COBLE. You all may want to consider that question when it comes her time again.

The gentlewoman's time has expired. The gentleman from Ohio is recognized.

Mr. CHABOT. Thank you, Mr. Chairman. I thank you for holding this hearing.

Mr. Pistole, in the addendum report that was released just this morning by the 9/11 Commission indicates three of the September 11 hijackers were carrying Saudi passports containing "a possible extremist indicator which was present in the passports of many of the al-Qaeda members."

While it's not clear what the indicator was, the report added that it had not been analyzed by the FBI or the CIA or border authorities. Why was this the case, and has that indicator now been disseminated among the agencies charged with examining these documents, and are FBI agents now trained in how to detect such indicators?

Mr. PISTOLE. Congressman, I think you've hit on a key point of the transformation of both the Law Enforcement/Intelligence Communities post-9/11, and that is the timely sharing of information and the actions taken in response to that information.

To address your specific question, I have not read the specific details of that, so I'll have to get back with you on that, but as to the sharing of information of the indicators, I am not aware of when the FBI received that information pre-9/11. The issue that has been addressed in the post-9/11 environment is that there's a whole new paradigm of that information-sharing, and information such as that now, through a number of different media, would be exchanged on a timely basis and acted on in a way that did not exist prior to 9/11. So if that's of any consolation in terms of changes that have been made, I'll be glad to go into detail if you'd like on those changes both within the FBI and within the community that would pick that up now.

Mr. CHABOT. Thank you. Because we're so limited in time, I'd like to move on to another area now.

Would you please explain the distinction between a money remitter and a hawala? What characteristics of either of these allow criminal activity to flourish, lack of recordkeeping and oversight and that sort of thing?

Mr. PISTOLE. Sure. Both a money remitter and hawala, different names depending on how you are defining them, could be for the same entity that uses a method of exchanging finances, money, currency, without extensive recordkeeping. And by that, for example, hawala may be operating in Chicago and pre-9/11 could have money deposited with it from a person in Chicago, sent to anyplace over the world, but the money is not actually sent, and there's simply a recognition at the receiving end that a person is entitled to X amount of money, similar to a wire transfer, money order that's being sent through any number of different entities.

The change with the PATRIOT Act, these money remitters, hawalas, if they're engaged in that business, do not have to be registered in the State that they are located. And what it does is it provides a way of tracking money that was, we believe, some of the funding for the 9/11 hijackers. We did not have that system in place prior to 9/11, and it caused great difficulties in determining where the approximately $400–$500,000 the 9/11 hijackers used, where that all came from. And so that's been one of the areas that there has been a legislative fix, if you will, to help us in our law enforcement efforts.

Mr. CHABOT. Thank you. Let me continue with you, if I can.

What is the al Barakat network, and why does the FBI and the Office of Foreign Assets Control at the Treasury Department differ as to whether this network has terrorist links?

Mr. PISTOLE. In terms of al Barakat, there is a fair amount of reporting, both intelligence and evidence of its support for terrorist activities. I would be glad to go into much more detail in a closed setting if that would be appropriate, and I would be glad to provide that briefing. Suffice it to say that there is both intelligence and evidence to indicate that it has provided funding to groups such as al Qaeda and other groups.

Mr. CHABOT. Thank you, Mr. Chairman. I note the yellow light has been on some time, so I will get to my following questions in the next round. Thank you, Mr. Chairman.

Mr. COBLE. I thank the gentleman from Ohio.

We have been joined by the gentleman from Wisconsin Mr. Green, who is now recognized.

Mr. GREEN. I thank the Chairman. I apologize for being late. I have the privilege of serving on both this Committee and the Financial Services Committee, and they are simultaneously having hearings on the 9/11 Commission, so I am running back and forth a great deal.

A couple of brief questions. First off, Mr. Kojm, will the Commission be supporting legislation as we go forward? How is it going to respond to the different legislative proposals that are almost certainly going to be floating around when we return back in September?

Mr. KOJM. Thank you for the question.

Well, I'm certain that Commissioners will want to reflect upon bills as introduced and meet now as former Commissioners and assess their response. I think it's fair to say that the closer the legislation, draft legislation, is to the Commission recommendations, the more comfortable they will be in signaling their support for it.

I should add, too, that this is a learning process for Commissioners, and they have taken the view that please adopt our recommendations or something better. So by no means do the now former Commissioners exclude the ability to improve upon their work.

Mr. GREEN. Thank you.

Mr. Pistole, we have been working on legislation, I think it is fair to say a number of Members have been working on legislation, ever since 9/11, looking to provide tools for the FBI, Intelligence Community, obviously responding to changing conditions as we understand them. One piece of legislation that we've introduced is H.R. 4942 that deals with the, quote/unquote, material support for terrorism. It tries to get at the different ways in which individuals may support terrorist organizations other than the obvious supply of money, the supply of physical, tangible goods; instead, perhaps, intellectual support or where an individual, someone residing in this country, a citizen or not a citizen, becomes a recruit and actually travels and attends a terrorist training camp, whether or not that person then goes on to participate in terrorist activities.

Have you given thought to the types of tools that we should be working on? And, secondly, with the specific reference to legislation that I referred to, I don't know if you are familiar with it at all, and would you be willing to respond to that concept, whether or not you think that would be useful?

Mr. PISTOLE. Yes, Congressman. Thank you for the opportunity.

Let me just start by saying one of the very basic tools that we do not have in terrorism investigations which we do in other select investigations is the use of administrative subpoenas for counterterrorism investigations. It's something that we use in drug investigations, we use in health care fraud investigations by statute, but we do not have the authority to use administrative sub-

poenas, which are basically just a streamlined way of obtaining documentary evidence.

One example is where somebody checks into a hotel late at night. The desk clerk is suspicious because the person looks like somebody who may be wanted on charges, terrorism charges, but there's a question as to what the legal process is for obtaining that. The JTTF, Joint Terrorism Task Force, goes out to the hotel and the general manager says, no, we cannot give you the registration, the name of the person who checked in, because you don't have a subpoena.

If we had administrative subpoena authority, we could get that information right away, and given the timeliness of terrorism investigations, that's something that just seems very basic to us, which would be a beneficial tool; whereas if we have to go to an assistant U.S. Attorney to get a Federal grand jury subpoena, obviously by the time we get that, circumstances may change, and in a worst-case scenario, we could be dealing with a terrorist attack that's already happened. That's one basic thing.

I don't have the specifics of H.R. 4942, so I'll take a look at that and be glad to get back to you on that. Anything that helps us in our efforts to identify somebody who may be providing material support obviously would be welcome.

We look at several areas that terrorists have to engage in to commit an act, and along those lines, obviously, we have the operators who are the bomb-throwers, if you will; we have the facilitators, who may be unknowing and unwitting in what they're doing; but we have the financial people. And at any of those stages if we can intercept somebody using the material support statute, that is of benefit to us.

Mr. NOJEIM. Could I add to that for just a minute? I did review the legislation before I came over. I think that one of the purposes of the legislation is to respond to the Humanitarian Law Project cases. Those cases were about expert advice and assistance and the finding of specific intent for that particular crime of providing material support for expert advice and assistance. Since that case was decided, there's been additional cases decided, one in Florida involving Mr. Al-Arian, that have a much broader interpretation of the kind of intent that would be required, and also has some very helpful information about inferring intent. And we'd like to work with you on that because I think that's kind of the next generation of where the law is going, and you'll want your legislation to be responsive to it.

As for the administrative subpoenas, in the very example that Mr. Pistole used, the person who reported to the FBI that a suspicious character had come into the hotel under current law can give the record to the FBI when they show up. There's no need for a subpoena. There's no need for a grand jury subpoena. That person who said a suspicious person is here can give that information away.

Mr. GREEN. I appreciate your additional response to the question. I would appreciate your input again, in particular with H.R. 4942 as we try to move forward. Obviously, the greater clarity of detail that we can provide, I think the better for all of us in making this an effective tool.

I guess I would just say before I surrender back my time, I think it's clear that particularly in the House we will want to act in September to make sure that we do a great deal of the work that's been recommended by the 9/11 Commission, but we're also looking for opportunities, given how much time will pass between September and when we're likely to return next session, to make sure that we do a good job in providing necessary tools with this evolving threat. So I would invite all of you to help us through that process, because obviously time will be short.

With that, Mr. Chairman, I surrender back my time.

Mr. COBLE. I say to the gentleman from Wisconsin the Subcommittee appreciates your attending two hearings simultaneously today. I know that's a stretch, but we thank you for being here.

We will now commence our second round of questioning. Let me revisit terrorism financing with Mr. Pistole.

Mr. Pistole, I am firmly convinced that terrorism is heavily subsidized through illegal drug trafficking. To what extent, if any, is American organized crime or American drug trafficking involved, if you know?

Mr. PISTOLE. Mr. Chairman, the FBI has had a number of investigations which led to prosecutions where one of the underlying criminal acts that was being charged was drug trafficking. We have a number of investigations that are ongoing which involve that also, and drug trafficking being one of any number of illegal activities that we believe help support terrorist organizations overseas and perhaps also here in the U.S. We have not seen a direct link between organized crime either in the traditional sense or any of the emerging organized crime groups that are directly and knowingly supporting terrorist activity through the drug trafficking.

Mr. COBLE. If you would keep this Subcommittee current on that, Mr. Pistole, I would be appreciative.

Mr. Brennan, I have ignored you up until now. The current Terrorist Threat Integration Center is a multiagency joint effort that is tasked with the integration and analysis of terrorism through threat-related information and disseminates that information to key officials. To what degree do you attribute the success of TTIC to the fact that it is not housed in or controlled by one agency and is therefore able to minimize the effects of interagency turf battles?

Mr. BRENNAN. Thank you, Mr. Chairman. I think whatever success TTIC has enjoyed is precisely because of that, because we are not housed in one single department or agency. I think over the years there have been some issues related to one department or agency does not necessarily want to follow another one in terms of how business is conducted and how they do their work. When you have a collaborative multiagency joint venture such as TTIC, I think it allows the departments and agencies really to collaborate with one another in a way that hasn't happened before.

Mr. COBLE. I think, as we have learned today, that was one of the problems, the fact that communication lines were clogged between various entities in the Intelligence Community, and hopefully that has at least been recognized and is hopefully being resolved.

Mr. Kojm, do you believe that the PATRIOT Act has assisted in the war on terror, A; and, B, have you been provided with any evi-

dence that law enforcement has abused the new authorities and updated authorities provided in the USA PATRIOT Act?

Mr. KOJM. Mr. Chairman, on the first part of your question, we looked in detail at the question of the wall with respect to the PATRIOT Act, and the Commission is certainly of the unanimous view that taking down the wall was a very beneficial step and has significantly improved communication between law enforcement and intelligence. And more generally on the question of terrorism, we did not take any point-by-point review of the PATRIOT Act. We do appreciate that many of its aspects relate to updating current statutes to the digital age, but apart from the question of the wall, we did not take a detailed view.

Mr. COBLE. Mr. Nojeim, I think I pronounced your name several ways, but I think I finally have it down. Mr. Nojeim.

The 9/11 Commission recommended the creation of a position of a National Intelligence Director, NID, located in the Executive Office of the President. I think we have touched on this previously. The President has proposed a slightly different model which would allow the NID to oversee the NCTC and to report directly to the President, but not be a member of the Cabinet nor have the authority to circumvent the agency heads. What advantages and/or disadvantages do you see with these models?

Mr. NOJEIM. The disadvantage with the model of having the NID at the White House is that it politicizes the analysis of intelligence and the consolidation of intelligence. Under the Commission's proposal, the FBI intelligence function would report to somebody inside the White House. Now, remember a few years ago when it was a big scandal that a number of FBI files—that a number of FBI files on individuals ended up in the White House? That was called the Filegate incident. We're concerned that under the proposal, FBI files in the White House would not be so unusual. It would not be so unusual, because, at least in the case of surveillance files, that might be where the Director looks at them.

Mr. COBLE. My time has expired, but I see Mr. Kojm is antsy to respond, so let me have Mr. Kojm respond as well.

Mr. KOJM. Thank you, Mr. Chairman.

I want to be clear here, the Commission recommendations do not change in any way, shape or form the legal authorities under which the FBI operates, and that includes the restrictions on its authorities. What is crucial for us is the sharing of intelligence and the FBI participating in that, and the sharing of operational plannings. And the FBI would be involved in that process, but there would be no control by the White House, and I invite my colleague to complete my answer here.

Mr. PISTOLE. Mr. Chairman, if I could just add on that point, clearly the independence of the FBI from political process is critical to our being able to protect the civil liberties and the safety of everybody in the U.S. So it's at—the very notion that it would be politicized under this recommendation is contrary to the way we interpret that.

Mr. COBLE. I thank you, gentlemen. My time has expired.

The gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

I want to thank Mr. Nojeim for pointing out the difference in the investigation pursuant to the Levy guidelines where you have to actually be investigating some kind of a lead or a crime before you start infiltrating organizations and conducting them under the pre-Levy guidelines, where you just snoop around and infiltrate groups just to gather information on people. And that is obviously a stark difference.

One of questions I had is on a kind of flowchart where the National Counterterrorism Center is under the National Intelligence Director. It's on page 413 of the report. It seems to me that the National Counterterrorism Center really ought to be serving as a staff of the Director, otherwise things may get to the center, it would have to go back up or go back down. At some point a CIA agent who has some information has to give it to somebody and has to filter through the process so that an FBI agent can use that information.

Now, I understand that we're gathering enough information, but I kind of view this as kind of the "Where's Waldo" puzzle, where if somebody on that puzzle—if somebody shows you the picture, there he is, it's obvious, but in the whole picture, trying to find him may take you a long time.

Now, my question is, with all the information coming to one person, will they be deluged with so much information that it will be essentially useless? And, Mr. Brennan, in TTIC are you running into that where you get all the information, if somebody had just pointed out to you which of the 20,000 e-mails is actually important, it would be obvious to you what to do; but if somebody is sitting at a desk and runs 20,000 e-mails, what did you do with that information?

Mr. BRENNAN. Yes, Mr. Scott. That's why the information has to be put in some type of information system architecture and database that can be accessed and pulsed as a result of searches that are done. Right now in TTIC we have access to all FBI information coming from the field, all CIA information coming in from the field, on a real-time basis. So you have to apply the analytic tools and the computer tools in order to access that information because there's just voluminous information that comes in on a daily basis.

People keep talking about information-sharing, and it's not sufficient just for me to share information just with Mr. Pistole. In the Government you need to make sure that the special agent in New York City or the case officer over in Africa or a State Department officer in Europe has access to information as appropriate, and that requires a tremendous engineering of that process.

Mr. SCOTT. Will the new proposal make things better or worse?

Mr. BRENNAN. We are on a glide path right now to do this. In order to access the information right now within TTIC, we have 180 officers from all throughout the Government who are able to access this information. But I do not see how this, what they're calling for, is going to allow us to do that on its own.

There is a recommendation in here on information-sharing that talks about incentives for information-sharing, and that's one of the issues that I take objection to. You can't incentivize information-sharing. You have to institutionalize it, and you have to have an

enforcement mechanism and a compliance regimen in order to ensure that happens.

Mr. SCOTT. I have a lot more questions. I'm sorry. Go ahead.

Mr. KOJM. Mr. Scott, thank you for letting me just respond briefly to Mr. Brennan.

One of the incentives is precisely what Mr. Brennan outlines, a new architecture for information-sharing, and I couldn't agree with him more in the importance of a system that allows just the kind of work that analysts need to do. That's one of the incentives that needs to be built into the system.

One of the things we found in our study is that even when the FBI and the CIA put people in each other's centers and detailed them there, that alone was not enough to have information shared. We have to get the systems right, and therefore I agree with Mr. Brennan.

Mr. SCOTT. Mr. Nojeim, they're talking about taking down the wall between CIA information gathered under the casual foreign intelligence gathering systems and FBI, which has limited probable cause and other kinds of barriers. Is there any limit to the amount of information that ought to be shared between the CIA and the FBI, particularly when they're working in joint operations?

Mr. NOJEIM. I think I would look at it a little bit differently. The situation that we have now is one where if an agent has—if an agent believes that a person is involved in a crime, but they don't have probable cause of crime, they can go around the Fourth Amendment's probable cause of crime requirement and conduct the wiretap or a physical search of a home with the use of intelligence authorities. That's what happened in the PATRIOT Act in section 218.

We think that that situation needs to be fixed somehow. It's not necessary to re-erect a wall to fix it, but it is necessary to ensure that when the Government is looking for crime, and it's doing a very intrusive search, that it have probable cause of crime as found by a Federal judge.

Mr. SCOTT. Can I ask a quick follow-up question then? At the last hearing we heard that these new powers and information-sharing was aimed at terrorism and not at general law enforcement. If you are talking about general law enforcement and using foreign intelligence techniques to conduct what is essentially a criminal investigation, should we just limit it, these new powers, to terrorism so that we know what we're talking about, not just general run-of-the-mill crime?

Mr. NOJEIM. Some of the new powers in the PATRIOT Act were limited to terrorism, and some were not. For example, the secret searches, the sneak-and-peek searches, those are for all searches, not just for searches involving allegations of terrorism. We think that there should be truth in advertising; that when a bill is sold as an anti-terrorism tool, that it used as an anti-terrorism tool.

Mr. PISTOLE. Mr. Scott, if I could just comment also, sir, on the issue of the wiretaps. In any use of a wiretap, whether it's under the criminal title III laws or under the Foreign Intelligence Surveillance Court laws, the FISA Act, in each and every instance there is an application made to a court, and a court establishes

that, yes, there is justifiable probable cause, but that a wiretap should be granted——

Mr. SCOTT. Probable cause of what under FISA?

Mr. PISTOLE. Under FISA it's establishment that there's either a foreign power or a terrorist nexus in that.

Mr. SCOTT. And no allegation of crime is needed, just that you have got an agent of a foreign government, and you are curious of what is going on.

Mr. PISTOLE. No, that there is a relationship between that individual that we're trying to establish additional information about, that that person has engaged in something that is contrary to the national security of the United States. And under that——

Mr. SCOTT. Which could be a trade deal, a trade deal.

Mr. PISTOLE. Well, there are laws on certain exports of trade items, if that's what you're talking about. Obviously, the foreign intelligence collection that the FBI does transcends counterterrorism. I also have responsibility for counterintelligence, and there's a lot of issues there that involve no crimes.

Mr. SCOTT. And the question is if you can get foreign intelligence wiretaps without any allegation of a crime. And the question is, as Mr. Nojeim has suggested, that if you are actually running a criminal investigation, but do not have probable cause, you can run the investigation under the foreign intelligence gathering standard, get all the information, and then if you find something, then you can hand it over to the FBI.

Mr. PISTOLE. Well, the safeguards that are in effect on that, sir, are the Office of Intelligence Policy Review, the OIPR, the Department of Justice——

Mr. SCOTT. The precedent is the wall; you cannot get it over there. There is no incentive to do it if this wall is erect, but we are talking about taking it down.

Mr. PISTOLE. That's what the PATRIOT Act did is eliminate the wall. Just as an example, in New York if there's an agent, an FBI agent, who is investigating the blind sheikh, for example, that agent would have to open either an intelligence or criminal investigation on the blind sheikh. This is pre-9/11. There could be a separate parallel investigation, either criminal or intelligence, that would be conducted, but the two could not share that information.

What the PATRIOT Act did in a FISA court of review decision, coupled with the AG guidelines, what that did was allow that information to be shared which goes to the national security of the United States. And that's all we're trying to do is make sure that the people of the United States are free from terrorist attacks and that we're doing everything humanly possible to address that. Pursuit under criminal sanctions, that's one thing, we can lock somebody up. If they're not criminal sanctions, we can still collect on a national security matter.

Mr. SCOTT. Mr. Chairman, I do not want to belabor the point, but as Mr. Nojeim has indicated, we ought to have some truth in advertising. You have discussed a terrorism situation, but you could say the same thing if you trip over some information in an investigation that had nothing to do with the terrorism, and you trip over a crime, or you were looking for the crime, and you can use the information by gathering it under the foreign intelligence

standards, which are very casual, and give over to the FBI information they could not have gotten otherwise.

Mr. PISTOLE. With all due respect, Congressman, we could not use the FISA wiretap in that situation you just described. We would have to have the articulation of a foreign power or terrorist entity that is involved in that situation before the FISA court will ever give us the authority. Otherwise we have to have the criminal allegations, probable cause under title III of the wiretap authority. So we cannot casually collect information like that. I disagree with your assessment there, sir.

Mr. NOJEIM. If I could clarify a little bit.

Mr. COBLE. Very quickly, Mr. Nojeim.

Mr. NOJEIM. It's that the wall wasn't erected just based on the law. It was based on interpretations of the law, and the PATRIOT Act changed the law. But the wall was the result of much more than just what the law said. It was the result of the way it was interpreted.

Mr. COBLE. Well, the good news is this will probably not be the final time we visit with you all. This will be ongoing.

Mr. Feeney from Florida, I previously commended the gentleman from Wisconsin for his agility and durability in simultaneously attending two hearings today. I didn't want to omit that recognition to you. I now recognize you.

Mr. FEENEY. Thank you.

Yes, Mr. Hamilton is testifying in the Financial Services Committee, but, Mr. Chairman, this is my second round of questioning here. They have not gotten to me over there. So this shows how efficient you run your Committee, for which I am grateful.

Mr. Pistole, to go back for a second, because this is a very important matter. Mr. Nojeim would have people believe that we have a couple thousand James Bonds running around snooping in our living rooms based on the way he put the question, and that they do not needs warrants. FISA wiretaps are only done pursuant to a warrant issued by the FISA court; is that right?

Mr. PISTOLE. Absolutely, Congressman.

Mr. FEENEY. And there always has to be proof established that there is either a foreign agent involved, likely involved, probable cause, or that there is probable cause that a terrorist activity under our new definition of terrorist crimes or related crimes is involved; is that correct?

Mr. PISTOLE. That's correct, sir.

Mr. FEENEY. And not every terrorist crime involves hijacking a plane and committing suicide or using a bomb. There are a lot of crimes or activities that are necessary predicates to the ultimate crime, and they are eligible for surveillance under the new PATRIOT Act guidelines; is that right?

Mr. PISTOLE. That's exactly right, sir.

Mr. FEENEY. I think the concerns are legitimate because I do not want warrantless searches of the American people, and I do not want unreasonable search warrants being issued, but by the same token, what's reasonable, because our Founding Fathers were very wise men indeed, depends on the circumstances and threat, in my view, and unfortunately the threat is something that we have not always anticipated.

Going back to some of the problems with the wall, Mr. Pistole, the new addendum to the 9/11 report, and by the way, it's not necessarily an addendum. I'm told by Mr. Hamilton that this was issued by the staff because of the incredible research that they did, and while it is intended to complement the report, it has not been approved or authorized or voted on by the Commission. Mr. Hamilton wanted to make that clear. Mr. Kojm, do you want to confirm that?

Mr. KOJM. Mr. Hamilton is always right.

Mr. FEENEY. And he also suggests that there may be several other subsequent reports issued by staff to fill in details, and once things become appropriately clear and so forth.

Mr. KOJM. We were able to get the cooperation of the executive branch with respect to these two reports before time ran out in the Commission's life, and the executive branch was very cooperative. It is simply difficult to get these cleared, and they did. Thank you.

Mr. FEENEY. The CIA claimed this addendum is not really an addendum, but this staff report that we just got over the weekend, that they did not get to review terrorist travel documents after 1992 because the FBI decided not to share what they gathered in law enforcement investigations, some of the cross-sharing of information that we're talking about between law enforcement investigations and surveillance. Is that the case, Mr. Kojm, and has that been rectified since 1993, the World Trade Center bombings, or since 9/11?

Mr. KOJM. Our strong impression is that today very significant progress has been made with respect to information-sharing in this regard, but we still believe it can be better and must be better. I'm really not prepared to respond to the immediate aftermath of '92. I just don't have that information with me, and we can provide that for the record.

Mr. FEENEY. Mr. Kojm, some of the concerns expressed by the ACLU representative I do share as well, because out of the sunshine, allegations can be made by the executive branch of the Government. A court will issue a wiretap perhaps if probable cause is made, but it's very difficult for the American people to hold folks accountable when it's not done in the sunshine. However, in the surveillance situation it sometimes is necessary. It's one of the reasons for the privacy and civil liberties officer that the Commission has strongly suggested be set up as a national protection for civil liberties and privacy. Is that one of the reasons that you have suggested that? And as you answer that, tell me about how that privacy officer can protect the sharing of data and also people's civil liberties and privacy as we share not just between Federal agencies, but up and down with the States and localities.

For the first time since 1812, States and local Governments have got to be involved in preventing and deterring and stopping attacks on the American mainland by foreign-authorized threats. So tell me how that privacy officer can balance civil liberties and privacy up and down as well as across Federal agencies.

Mr. KOJM. Congressman, I'll start your question, and then I'll invite my colleague, the former general counsel, Dan Marcus, he may wish to join in further comment.

Your question exactly establishes why the Commission did what it did. We're quite mindful that our recommendations would increase the intrusiveness of the Federal Government in the lives of citizens, particularly with respect to border security and aviation security. Therefore, we thought it very important to create a countervailing checks and balances even within the executive branch; hence, the Civil Liberties Board, to which individuals and Government officials could bring their cases and appeal when they thought that guidelines went too far or that privacy had been intruded on.

But it's not just the Civil Liberties Board. We believe strongly that our recommendations on congressional oversight will include the quality and attention on oversight matters by the Congress, which together with the courts and the Board and the executive branch are critically important to the protection of civil liberties.

Let me just turn around for a second.

Mr. MARCUS. I don't really have anything to add unless you want to swear me in.

Mr. COBLE. That's fine. That's fine.

Mr. FEENEY. I yield back.

Mr. COBLE. The gentleman's time has expired.

The gentlewoman from Texas.

Ms. JACKSON LEE. Thank you again, Mr. Chairman.

I would like to offer two articles. I ask unanimous consent to have them included in the record. The first one is dated August 21, 2004, Terror No-Fly List Tough to Get Off. And, of course, it sites the renowned stories of Senator Edward Kennedy and Congressperson and civil rights leader, Representative John Lewis. I ask unanimous consent for that article to be submitted into the record.

Mr. COBLE. I'm sorry. I did not hear you.

Ms. JACKSON LEE. I ask for an article dealing with the terror no-fly list, Tough to Get Off.

Mr. COBLE. Without objection.

Ms. JACKSON LEE. And another article dated August 22, 2004, Science Seen as Slipping in U.S., Visa Hurdles Are Turning Away Foreign Talent, Expert Argues. And of course it is a long scenario about our failings in the visa system as it relates to innocent individuals who are attempting to come to the United States. I would add this impacts businesspersons and people in the medical profession as well.

Mr. COBLE. Without objection.

Ms. JACKSON LEE. Thank you very much.

I would like to go down a line of questioning that was framed by my colleague, Ranking Member Scott, when he mentioned that a lot of information was gathered regarding the 9/11 hijackers, but it was not used properly. It may have been the Ranking Member, it might have been one of the witnesses, so forgive me, when that language came out.

Let me also cite on page 68 in your report dealing with Immigration Border Security Evolves 1993 to 2001, and that was not the 9/11 report, but the terrorist travel report that came out over the weekend. The opening paragraph indicates that the Intelligence Community did not organize to disrupt travel except when tar-

geting individual terrorists. It also failed—and this is chronicling the infrastructure failures with respect to 9/11 terrorists—it also failed to fully use the one tool it supported to prevent terrorist entry, the terrorist watch list.

An article a couple months ago said there are currently a dozen official terrorist watch lists maintained by nine Federal agencies, and not all employees of each agency currently have access to all of those watch lists. In the aftermath of 9/11 it was discovered that at least two of the 9/11 terrorists could have been stopped from boarding their airplanes had the Government's various watch lists been unified.

So there lies a deep penetrating flaw in our system. Unfortunately, I am not comforted that we have made any inroads in making those lists unified so that we definitively can get the bad guys against the good guys.

Mr. Nojeim, would you comment first on the story that I recalled in the earlier statement that I made dealing with the elderly Indian national who I believe you find an overreach between Federal and local officials? How do we strike a balance in what will potentially happen where you have local authorities overreaching based on lack of information, lack of knowledge and lack of coordination? And what impact should a Federal system have in being able to, in essence, dictate to the local authorities, which have no Federal immigration responsibilities as I know it, or no immigration responsibilities, in the instance of an elderly Indian national now detained on the pretense of possessing illegal weapons which have been cleared by Homeland Security? How do we have a firewall on that instance?

Mr. NOJEIM. I can't comment on the particular case because I really don't know enough about it to make comments on the general case. But generally once you start melding the enforcement of immigration laws with the local officials, we run into all kinds of problems, and one of the problems that seems to be recurring is that people who have questionable immigration status don't come forward. And many of the local officials for that reason have decided for public safety reasons that they don't want to be in the business of enforcing immigration laws. So that's one piece of it. But as for the particular case, I really don't know enough about it.

Ms. JACKSON LEE. I do not want you to comment on the particular case. I have made the record for that. There is an Indian national detained for no reason whatsoever. I think the question is when someone is cleared by Federal authorities, Homeland Security, the question is do we have some kind of consistent policy so they are not caught up in a web of overzealous local authorities who really have no basis for retaining them on terrorist activities or anything else?

Mr. NOJEIM. A person who's been cleared should be released. A person who is suspected of a local crime can be held under local authorities.

Ms. JACKSON LEE. I would like to, if you would indulge me, Mr. Chairman, to pose this question to the FBI regarding the watch list, which seems to still be broken. What efforts are being made to effectively unify that list, which says that agencies are not even coordinating these disparate lists?

I also make mention of the fact that there was knowledge in the Minneapolis office of—9/11—about some strange activities dealing with the 9/11 terrorists. That information did not get to Washington. How will the CT coordination office facilitate communication between agencies when there have been problems at the interagency level?

I think this is key. So if you can answer the watch list question and the coordination of intelligence. That has been the key that we found in the problems of the 9/11 terrorists. We had the information. We just could not utilize it. We could not protect the American people.

Mr. Pistole.

Mr. PISTOLE. Thank you, Congresswoman.

On the first issue of the terrorism, the watch list, as you know, in September of last year the President announced the creation of the Terrorist Screening Center. On December 1 of last year, the FBI was tasked with the responsibility of standing that up, and its initial operating capacity was stood up as of December 1 of last year. The purpose of the Terrorism Screening Center is to integrate the various disparate watch lists across the U.S. Government into a single, consolidated watch list. It's not done yet. There's still work that needs to be done. You are absolutely right. But what has been accomplished thus far is that all of these watch lists have now been collocated, if you will, in the Terrorism Screening Center, which is headed by a senior person from the Department of Homeland Security, Donna Bucella, who reports through the FBI.

What that does is allow for each agency to query this database of combined names in a way that was not done prior, well, to December of last year. What we don't have yet is—I think you made an earlier comment about each officer or agent in various agencies, they don't have that capacity to query that database yet. That's being worked out. The technology piece of that is still being done. Hopefully by the end of this year, that will be done to allow for an easy query. But over 7,000 calls have been made into that center in terms of questions about people on watch lists. For example, people who are subject to the FBI terrorism investigations, if they get stopped someplace by a State trooper for speeding, that State trooper, when they run the check, will find out that there is something about that person that they need more information about, and so that runs through the Terrorism Screening Center. So that is one aspect.

The second part of your question dealt with lack of coordination, and you mentioned the Minneapolis situation, and, of course, that was dealing with Zacarias Moussaoui and the issue of whether there was sufficient probable cause, if you will, to do a FISA wiretap on him and do a search.

In that situation the information actually did go to FBI headquarters, but because of the challenge of getting FISA authority prior to 9/11, the cumbersome process that existed, the authority was not granted in a timely manner, because FBI supervisors looked at it and said, there's more that we need to develop here, and that was being developed. Unfortunately 9/11 happened at the time. But the coordination issue has been addressed by making the

Counterterrorism Division responsible for directing and orchestrating all the counterterrorist activities.

Ms. JACKSON LEE. Let me just say that I respect the hard-working staff of the FBI. Let me make that very clear. I am also very sensitive of discussing proprietary information, meaning how you do things in terms of this watch list. But might I just respectfully say that it is shameful that we do not have a watch list now some 3 years later.

And I beg to disagree on the interpretation that you gave on Minneapolis. What I would say is there was lack of understanding of even how to pursue what they received. I think it made it difficult then to move in a different manner.

But the real issue is it is now August—let me get my dates correct—23, 2004, and we do not have an integrated watch list in the United States of America. I hesitate to even say that publicly. And I appreciate where we are, but we do not have one.

Mr. COBLE. The gentlewoman's time has expired.

Mr. PISTOLE. If I could just clarify. We do have an integrated watch list. It's the accessibility of that by every officer and agent across the country which we don't have yet. So we do have an integrated watch list. It's the ease of accessibility, and that's an information technology fix that is still being addressed.

Ms. JACKSON LEE. And that is the holistic approach in order to make sure that we are securing America. I appreciate what you are saying. We are not where we need to be, and it is August 23, 2004.

Mr. COBLE. Even though the lady's time has expired, Mr. Brennan, this is also overflowing into your area of expertise. Do you have anything to add to this?

Ms. JACKSON LEE. I appreciate it, Mr. Chairman.

Mr. BRENNAN. I just wanted to say that the study that the Representative noted was a GAO study of April of '03, and since that time, as Mr. Pistole mentioned, the Homeland Security Presidential Directive 6 of September gave two entities the responsibility for maintaining national data bases. TTIC has the responsibility for maintaining the national database on known and suspected international terrorists, transnational terrorists, to include U.S. Persons operating on U.S. Soil here. The FBI has the responsibility for maintaining the national database on known and suspected domestic terrorists, abortion clinic bombers, animal rights activists and others.

We have the combined responsibility then feeding that information at the classified level to the Terrorist Screening Center, which is the one-stop point within the U.S. Government right now that can provide assistance to all those watch listers and screeners, whether they be at borders, whether they be at consular sections overseas.

What we want to do is maintain a single database. People keep referencing sort of one watch list. Well, you have different purposes that need to be served. So you have a no-fly list which you don't want to have people get on the plane any way, any how.

Ms. JACKSON LEE. And that is inaccurate with John Lewis' and Ted Kennedy's names on it.

Mr. BRENNAN. I think they were on the selectee list. The selectee list are those names that are suspected to be individuals involved in international terrorism.

Ms. JACKSON LEE. I do not want to besmirch their names, but go ahead, sir.

Mr. BRENNAN. There is a process under way to improve the quality of the information that has been collected over the past 20 years. We are talking about 150,000 or so names that are, in fact, part of this Terrorist Screening Center database that provides that support to Federal and non-Federal entities throughout the Government—throughout the country.

Mr. COBLE. Thank you, Mr. Brennan.

We have two gentleman that have been patiently waiting. I recognize the gentleman from Ohio Mr. Chabot.

Mr. CHABOT. Once again, thank you, Mr. Chairman.

Mr. Kojm, let me turn to you if I can. On page 367 of the 9/11 Commission report, it recommends that "the U.S. Government must identify and prioritize actual or potential terrorist sanctuaries. For each it should have a realistic strategy to keep possible terrorists insecure and on the run using all elements of national power."

This recommendation was made with regard to working with other countries. Do you believe that this recommendation should apply to providing sanctuary to terrorists in the U.S.? In other words, for example, should Congress restrict law enforcement from using court orders to receive terrorism-related information from libraries and effectively create a sanctuary for terrorists to use for research and communication?

Mr. KOJM. Congressman, we did not really look into the question of court orders with respect to libraries and terrorism. We did not look into every aspect of the PATRIOT Act. For example, we—our attention really focussed on the wall because we found that to be directly relevant to the 9/11 story.

Mr. CHABOT. Thank you.

Would any of other witnesses—I figured you would like to, Mr. Nojeim. We also would like to hear from the other folks, but go ahead.

Mr. NOJEIM. Section 215 of the PATRIOT Act set a very low standard for judicial consideration of records requests. And under section 215, if the FBI asserts that a record or an object is "sought for", that's the language of the statute, is "sought for" an intelligence or counterterrorism-type investigation, and it gets an order just based on that mere assertion. It can require you, me, any business to turn over any record or anything. That's a very low standard of proof.

What the SAFE Act would do, and that's legislation that's been introduced to fix some of the parts of the PATRIOT Act, would be to slightly raise that standard. We believe that it needs to be raised because the current standard is just too low for the kind of access that would be given and the kind of information that would be available.

Mr. CHABOT. Thank you.

Mr. Pistole or Mr. Brennan, if you would like to.

Mr. PISTOLE. Yes. I think a vigorous public discussion about these issues is appropriate. And we in the FBI welcome that from the perspective of being able to articulate with some specificity, and that may have to be in a closed hearing because of the sensitivities of it; the uses of the section 215, for example, or indications of how does the Congress and the Administration and the American people, how do they want us to investigate the possible terrorist activities here in the U.S. And we welcome that because we have very good guidelines that we work by.

And just to say on section 215, there's been a lot of discussion about that. Without giving the exact—let's just say it has been used very, very infrequently. We have not employed that as a general tool, but we do look at it as one of the tools that we have in the fight against terrorism here in the U.S. And I did not want to be the person who is in the situation where I have to tell an agent out in the field that, no, you cannot go get this record because we don't have authority. If section 215 is repealed, and Mohammed Atta was a person—or his equivalent had access to a record or used something that we could have obtained under 215, but for that we are not able to obtain that, and so we miss that keylink that we are charged with the responsibility of connecting the dots, if we cannot connect the dots, then we can't connect them.

Mr. CHABOT. Mr. Brennan, I do not know if it has been adequately covered, but before you answer, I should probably mention, your name is the same as my father-in-law. He is John Brennan also. Before I ask you any questions I was going to ask you, are you or have you ever been my father-in-law?

Mr. BRENNAN. No, but I'm pleased to be related to you if that's possible.

Mr. CHABOT. Thank you very much.

Before my time runs out, Mr. Kojm mentioned before, he was talking about the Kuala Lumpur meeting and the fact that if changes had been made, that perhaps other things could or could not have resulted. I notice that you were perhaps subtly but somewhat vigorously shaking your head. I thought I might give you the opportunity to address that.

Mr. BRENNAN. Well, there's been a lot of discussion over the past several weeks about if only the FBI and CIA shared information, if we had a culture of sharing. Well, I can tell you that my experience is, since TTIC has stood up, there is a strong culture of sharing. It's not a question of willingness, it's a question of ability. And that's where you have to have in place a national system whereby you can get information into the system so that it can be accessible to all those Government departments and agencies, both Federal and non-Federal, that need that information.

It is a tremendous, tremendous challenge, and just moving boxes around within the Government will not do that. There is tremendous engineering as far as the wiring, the plumbing that is required. So I fully subscribe to the notion that we need to have a better system in place to allow this information to be shared securely so that you can take information that is collected clandestinely overseas and move it at the speed of light so that it can be accessed by analysts at headquarters, at FBI headquarters, at the JTTF, the Joint Terrorism Task Force in Los Angeles, and even by

the local police departments and first responders. But that is a tremendous engineering challenge that requires interoperable systems that we, as a Government, as a Nation, I think, need to move forward. It is not sufficient just to say CIA and FBI need to learn to share information better. That is not it.

Mr. CHABOT. Mr. Chairman, I note that my time has expired. I would like to comment by saying I think all four witness have been extremely helpful this morning.

Mr. COBLE. I thank you, Mr. Chabot. And pardon my modesty, but I think you all will agree your Chairman has used the gavel sparingly, but I think this is a very worthwhile hearing, and I think sparing use of gavel is in order.

Mr. Kojm, I think you wanted to be heard, so let me recognize you very briefly.

Mr. KOJM. I appreciate that, Mr. Chairman, simply to join into Mr. Brennan's point. He appears to be disagreeing with the Commission recommendations, but quite the contrary, we would agree in full with what he states. Good people are trying to do their jobs, are trying to share, are cooperating, but we need fundamental reform of information systems, which is one of the main recommendations of the Commission report. I guess we are in violent agreement on that point.

Mr. COBLE. Thank the gentleman.

The gentleman from Wisconsin, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

It was actually in that tome that I think this question was posed, and I pose it primarily to Mr. Kojm. You testified at a hearing I attended last week, and I didn't get to ask this question, but in the executive report, executive summary to the 9/11 Commission report, there was a sentence that struck me in which the report states, we are safer than we were 4 years ago, but we are not safe. And I think many of us would agree with that. But I think it's very easy for us during this process, this hearing process, whether it be in this Subcommittee or other Committees or what we do going forward, we tend to focus only on what is not working or what is in obvious need of change. Can you elaborate on why the Commission believes we were safer than we were 4 years ago? I think it is useful for us to have it on the record and for the American people to hear that.

Mr. KOJM. Mr. Green, thank you for the question. Certainly since 9/11 the Government, meaning both the executive and the legislative branch, have under taken significant steps, the creation of the Department of Homeland Security, the creation of TTIC as we've just discussed here this morning, changes in border security, much more with respect to aviation security in terms of checkpoint screening.

I think our fundamental point would be that there's so much more we could do and that we could do more efficiently, and that the institutions of Government still need comprehensive reform, and that there are many reforms of policy as well that are still required. Thank you.

Mr. GREEN. I appreciate your answer. I think you can tell from the hearings that you have attended, the statements that you have seen, that we all agree, and that there will be dramatic steps

taken. But I think it is important for us to talk about what is being done, because I think people need to realize that.

I guess in that same vein, Mr. Pistole, what have you seen that has been a positive change since 9/11; and perhaps in particular with respect to the tools that the FBI has seen as a result of PATRIOT Act, what progress have you seen?

Mr. PISTOLE. Clearly Congressman, the PATRIOT Act and the FISA court of review decision and the attorney general guidelines have made it much more of a fair fight from our perspective, whereas, prior to 9/11, it was like a boxer with one hand tied behind his back trying to do the job that the American people expected to us do but we couldn't even share within the FBI between the intelligence investigation and the criminal investigation. So, clearly, that has made us more efficient in what we do and the way we conduct business.

In addition to that, by being able to share within the FBI, we then are able to share outside the FBI in a much more cohesive fashion and in a way that makes efficiency something real. And the creation of TTIC I think is one of the key things that has been done and implemented since 9/11 where we have CIA case officers, we have Department of Homeland Security, we have, clearly, FBI agents and analysts sitting there who are sharing information real time and where non-FBI employees, as Mr. Brennan noted earlier, can access FBI counterterrorism investigation on a real-time basis. That simply wasn't done prior to 9/11 on any type of meaningful scale.

Also, the integration of case officers, agents, analysts between the various agencies has significantly helped the exchange of information, and it has enabled us to share the information that, for example, if we have reporting overseas either from a foreign intelligence agency or CIA has picked up information, the bottom line is how efficiently can we get that information to the police officer on the street, whether it's in Omaha, Des Moines, Los Angeles or New York, who needs to action that information.

And we're working on the continuation of efforts to declassify or classify at the lowest possible level that information at the origin so we can pass what is needed while still protecting the sources and methods so that the action can be taken that corresponds with what the intelligence is.

Just to summarize, everything we do in the FBI is intelligence-driven now. It used to be we would collect information that would be used in the prosecution for a particular case. Everything we do now is intelligence-driven. The start-up of the Office of Intelligence, the Director of Intelligence of the FBI, what Mr. Brennan's people do and what this new NCTC and NID would do as we envision is to assist in that process of establishing collection requirements and then having us execute those requirements in a logical, cohesive fashion.

Mr. GREEN. Mr. Brennan, my time is running short. I don't know if there's anything you care to add about what you've seen in terms of improvements since 9/11.

Mr. BRENNAN. Just in addition to what has already been mentioned, I think there has been a much greater appreciation of the holistic nature of the terrorism challenge. It is not just CIA or FBI

or Department of Homeland Security. It extends beyond that. The Department of Agriculture, Health and Human Services, Department of the Interior. And it's not just at the Federal level. It's also trying to bring in the governors and mayors and first responders and others.

It's a tremendously complex and interconnected system of systems that we need to put together. It's in some respects mind numbing in terms of its complexity and comprehensiveness, but I think there is an effort to try to transform those individual departments and agencies that make up that large universe of components that are really working together now, and it is challenging to do that in as fast a fashion as possible.

I am very sympathetic to calls for these things that have not happened yet, but trying to bring it all together, that engineering that's required to make sure the policemen on the streets of Baltimore can be serviced the way he or she needs to be. It is a tremendously challenging, again, engineering problem that we have to deal with. I think there has been that appreciation.

Mr. GREEN. Thank you.

Thank you, Mr. Chairman.

Mr. COBLE. This concludes our second round, and I am scheduled to be at a luncheon meeting at 12:15. The Ranking Member has another question, and in a sense of fairness I'm going to recognize him. If Ms. Jackson Lee and Mr. Chabot have one more question, I would implore you—Ms. Lee, if you will start—I will implore you all if you can, for the sake of the old man, be brief so I can make my luncheon meeting. Ms. Jackson Lee.

Ms. JACKSON LEE. With the distinguished Chairman's graciousness, let me try to put this on acceleration.

First of all, I want to acknowledge the work of our staff on this Committee. I know, not privy to staff works in other Committees, let me thank the Chairman's staff but also the Ranking Member's staff.

Mr. COBLE. If the lady would suspend, I want to echo that. The staff on both sides, Democrat and Republican, have been extraordinary, outstanding, did an outstanding job in preparation for this hearing.

Ms. JACKSON LEE. This is an excellent document. I thank them. The reason why I thank them is because there is an important probative question that I just want to ask Mr. Kojm and Mr. Pistole.

Mr. Kojm, did the 9/11 Commission—and I made the point that we had information, but we didn't all use it correctly—make a definitive, definite recommendation of a national identification card?

Mr. KOJM. Congresswoman, the answer to that would be as follows: We discussed the topic, and I think the Commissioners appreciated at least some of the sensitivity surrounding such a recommendation, and they consciously decided not to make that recommendation. But they do believe that we need stronger standards for drivers' licenses and birth certificates because these are the essential documents that all individuals use to get other documents. And if those basic documents are not at a high standard, then successive documents will not be. But the recommendation is Federal standards, not a national ID card.

Ms. JACKSON LEE. I thank you.

I don't want to prolong it, I will just say, Mr. Chairman, I think I am hearing that we can have stronger standards in States, as opposed to Federal standards, but there is no national ID.

The only thing for Mr. Pistole is I would appreciate just a quick answer on the calls that I am getting in my office about peace activists moving into New York and the intimidation that appears to be happening which is blurring the—between activists and terrorists. I want to know what the FBI is doing to make sure that blur does not happen.

I thank the Chairman very much for a very excellent hearing. I yield to the gentleman. Thank you.

Mr. COBLE. You're indeed welcome.

Mr. PISTOLE. Yes, Congresswoman, there has been some recent press reporting about what the FBI has done in terms of interviews of potential protesters, both at the DNC and at the RNC. And that is all predicated on—first, let me say it's a very small number of people that we've interviewed. In fact, it's less than the number of people in this room right now that we've interviewed nationwide. So out of a nation of 280 million people, we've interviewed less people than are in the room currently; and each of those people were interviewed because we had specific, credible information that they either were planning to engage in criminal activity, violent activity at one of the two conventions or that they had knowledge of one of the other people that would be engaged in that activity.

Ms. JACKSON LEE. Thank you. Thank the Chairman.

Mr. COBLE. The gentleman from Ohio, Mr. Chabot.

Mr. CHABOT. Thank you, Mr. Chairman. I'll be very brief.

The Chairman of the Senate Intelligence Committee has come out with a plan very recently, and I'm sure that not everyone has had an opportunity to fully understand or read about this and digest it, but if anyone had any comments that they'd like to make very briefly—I'm sure some probably would like to comment, so I'll open it to the floor.

Mr. KOJM. Just very briefly, we very much welcome the Senate's taking up our recommendations, and we look forward to studying the details of the proposal. We appreciate the Chair of that Committee is taking the report as his base for his bill.

Mr. NOJEIM. I'd like to add we haven't seen the plan, but the things to look out for are where is the intelligence director placed? Is it going to be at the White House? And does the FBI intelligence function report to this top spy or does the FBI intelligence function report to the FBI director, as is now the case?

Mr. PISTOLE. We have, of course, great respect for Chairman Roberts. The issue for us is whether the FBI will be able to maintain its independence of investigations and collection, obviously predicated on the requirements set by whomever it is, the NID, the NCTC, but then are we able to execute that in a way that we are able to protect the civil liberties of people in the U.S. and make sure we are doing everything that we can to prevent the next terrorist attack?

Mr. BRENNAN. I would just point out that the Goldwater-Nichols legislation that totally revamped and transformed the military took about 4 years to work through the various congressional efforts

here. It is an extraordinarily complex task to transform the Intelligence Community as well as just the CIA itself.

I think any effort to do that really needs to be a thoughtful one, a careful one, after considered options and thorough discussion. But to do it quickly and to just do it at the facade level and not understanding the implications of moving things about, and my understanding of this is that it would make the agency three separate, distinct agencies, that's not moving toward integration in my mind. But I would just caution people to make sure we understand exactly what is being called for and what the implications are of such a dramatic transformation very quickly.

Mr. COBLE. I thank the gentleman.

The Ranking Member, the gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Nojeim, under section 215, after the Department of Justice has made an assertion that the information is needed for a terrorism investigation, does the judge have any discretion on issuing the warrant?

Mr. NOJEIM. Under the statute, the assertion is enough. The judge has no discretion. He is a rubber stamp.

Mr. SCOTT. I would like to pose a question for the record, Mr. Chairman. We have heard back and forth about which model is better. My question, I guess to Mr. Brennan and Mr. Kojm, is to whether an on-the-ground FBI agent is more likely to actually get the information needed under the TTIC model or under the NCC model? Which model will actually make it more likely that an on-the-ground FBI agent might actually get the important information?

The third question, I guess to Mr. Pistole, is if you could provide us with the employment diversity of the FBI and if somebody has access to the other agencies I think that would be helpful. I think there were some questions prior to 9/11, and I believe improvements have been made since then so we're better able to do our job.

The other is on the No-Fly List. Exactly what database is being used? When the press reports have T. Kennedy being the name that was on the No-Fly List—and there must have been thousands if not millions of people whose names are inadvertently on the list—how many hijackers would have actually been stopped by our database and what efforts have been made to prevent it from being overly inclusive?

My question to Mr. Pistole on the FISA wiretaps, does—at the request of the Department of Justice, we watered down the requirement that the purpose of the wiretap be foreign intelligence, to a significant purpose is foreign intelligence, which invites the question what was the primary purpose of the wiretap to begin with if it was not—if you're getting a FISA wiretap and it wasn't for foreign intelligence, what was it for?

And once you've gotten the wiretap, then you get the roving wiretap. You can start placing wiretaps and listening to a lot of conversations without a crime ever being alleged. You're listening to a lot of conversations. And that is the information that, without a crime, the wiretaps without a crime ever have been alleged, that information is what's being turned over to the CIA and FBI and everybody else in town. That is our concern, that you're listening

to a lot of stuff and can use it as a pretense—a pretext, excuse me, for the investigation to begin with.

If the primary purpose was a criminal investigation without probable cause, you can conduct the whole investigation as long as somebody in there is an agent of a foreign government, is that right?

Mr. PISTOLE. Well, I think what you touched upon is the fundamental distinction between the criminal wiretap authority under title III, the Omnibus Crime Control Act of 1968, and the FISA authority. And clearly the protection of national security is at least as significant if not more significant than criminal activity.

As far as the event of the 9/11 hijackers, even though there were some minor infractions of law that took place while they were here that had been documented very well by the Commission, it wasn't up until the time that they were actually hijacking the aircraft that there was a clear violation of law. Even the smuggling of the blades onto the planes at that time, as best we can tell, were under the four-inch requirement. So even though they weren't violating a law, we still need the authority to conduct intelligence investigation under the Foreign Intelligence Surveillance Act and the court to ensure that we are preventing future terrorist acts, and I would state that we have never used a Foreign Intelligence Surveillance Act wiretap as a subterfuge or a device.

Mr. SCOTT. What purpose—if it is not the primary purpose of the wiretap, what is the purpose?

Mr. PISTOLE. Is to protect national security from either foreign powers or those who are affiliated with a terrorist organization.

Mr. SCOTT. So if we added that to the PATRIOT Act that wouldn't offend you.

Mr. PISTOLE. Add what, sir?

Mr. SCOTT. Add that the primary purpose has to be foreign intelligence or national security.

Mr. PISTOLE. Well, the PATRIOT Act, the significant purpose, if you want to, obviously, debate the importance of significant or primary, that was done by Congress.

Mr. SCOTT. Actually, Congress increased the standard. Because the Department of Justice asked for "a purpose," which meant any purpose, and the primary purpose could have been something else. My question is, if we limit the use of FISA wiretaps to foreign intelligence and national security as the only purposes you can be getting the wiretap for, would that offend you?

Mr. PISTOLE. That's generally the situation now. If you're thinking of a specific example that I am missing, then I may have a problem with that.

Mr. SCOTT. A specific example you're missing is a pretext for running an investigation without probable cause.

Mr. PISTOLE. Which we don't do. We still need a level of probable cause to——

Mr. SCOTT. So I am hearing that you would not be offended if we restricted the use of FISA to what FISA is supposed to be there for.

Mr. PISTOLE. Absolutely, not because that's what we use it for.

Mr. COBLE. I thank the gentleman.

Folks, I thank not only the panel but I thank those in the audience who have expressed interest by your presence here.

We are in very trying times, folks. I think Mr. Green or Mr. Chabot, one of the two, indicated, quoting from the 9/11 Commission report, that we are safer than we were prior to 9/11, but we are not safe. We are dealing with people who not only are interested—unlike Hitler, not only are interested in conquering the world, they're not adverse to destroying the world. And they'll destroy you and they don't mind destroying themselves. How do you respond to that? That is so fanatical it's beyond my grasp. I'm not smart enough to grab it.

But I appreciate what you all are doing. I think this has been a very productive hearing.

I thank the witnesses for your testimony, and this concludes our oversight hearing on the recommendations of the 9/11 Commission.

The record, by the way, will be open for 1 week. If you have additional information to submit, we will happily receive same.

The Subcommittee stands adjourned.

[Whereupon, at 12:18 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE STEVE CHABOT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO, AND CHAIRMAN, SUBCOMMITTEE ON THE CONSTITUTION

I'd like to first thank Chairman Coble for agreeing to hold this important hearing today. I would also like to thank today's witnesses for appearing before us. Over the last 20 months, the National Commission on Terrorist Attacks Upon the United States—commonly referred to as the 9/11 Commission—has worked tirelessly. Our nation owes a great debt of gratitude for their work, and I am confident that we will benefit from their expertise, as well as from the rest of our panelists, this morning.

As we know far too well, September 11, 2001 changed our world. It changed the way in which we must deal with terrorism and the way in which we, as a country, must protect ourselves.

Since that tragic day, Congress and the Administration have taken steps to help better protect our nation at home and abroad. Through passage of the Patriot Act and the creation of the Department of Homeland Security, we have provided law enforcement with enhanced investigative tools and improved our ability to coordinate activities designed to protect against the future threat of terrorism. Through the heroic actions of the brave men and women serving in our armed forces, we have also pursued the terrorists and those who assist them in places such as Afghanistan and Iraq.

Yet, these actions are not enough to guarantee our nation's security or freedom. This can only be accomplished through continued vigilance and a willingness to challenge conventional wisdom. We must continue to improve our intelligence capabilities, strengthen our defenses, and stay a step ahead of our enemies.

To help accomplish these critical goals, it is imperative that Congress provide a comprehensive and expeditious review of the 9/11 Commissions recommendations—then move forward with initiatives that will further improve our ability to combat terrorism and defend our citizens.

As the Commission notes, we must also be mindful of the protections afforded by our Constitution and our need to guard them as we work to better protect our country. Ignoring important civil liberties will not only erode our freedoms, but will undermine legitimate efforts to increase our security.

I look forward to discussing the Commission's recommendations with our witnesses today and determining what Congress can do to better protect our nation.

Copyright 2004 Associated Press
All Rights Reserved
Associated Press Online

These materials may not be republished without the express written consent of The Associated Press

August 21, 2004 Saturday

SECTION: DOMESTIC NEWS

LENGTH: 563 words

HEADLINE: Terror 'No-Fly' List Tough to Get Off

BYLINE: LOLITA C. BALDOR; Associated Press Writer

DATELINE: WASHINGTON

BODY:
The nation's confusing array of terrorist watch lists - like those that snagged Sen. Edward M. Kennedy and Rep. John Lewis - can be easy to get on, but far more difficult to get off.

It took Kennedy, one of the country's best known senators, three weeks and several calls to federal officials to separate his identity from that of a person with a similar name on the no-fly list. Lesser-known Americans face greater hurdles when their name is flagged by an airline computer.

"This really speaks to just how difficult it can be for ordinary people," said Jay Stanley, spokesman for the American Civil Liberties Union, which has filed two lawsuits on this issue. "The complaints reflected in our litigation are serious."

Kennedy, a Massachusetts Democrat, was stopped at least five times while trying to board US Airways flights because a name similar to his was being used as an alias for someone on the watch list. Though Kennedy has been a vocal critic of the Bush administration, he does not believe politics played a role in his being linked to someone on the Transportation Security Administration's no-fly list, according to his spokesman David Smith.

Homeland Security Department spokesman Brian Roehrkasse also said politics was not involved.

Lewis, a Georgia Democrat, has filed a complaint with the Homeland Security Department. He said he routinely can't get an electronic ticket, must show extra identification and has his luggage combed through by hand. And, he said, one airline representative in Atlanta told him, "Once you're on the list, there's no way to get off it."

TSA and DHS do not disclose the names on the watch lists or any details about the lists. But a government official, speaking on the condition of anonymity, said that a number of watchlists are being consolidated, and it wasn't clear which agency put a name similar to Kennedy's on the list.

The TSA has about a few thousand names on a "no fly" list, which bans people from boarding plans, and another few thousand on a list that identifies people for additional screening, the official said.

The task of clearing up the problems belongs to the agency's ombudsman, Kimberly Walton, and her 26 staff members.

Airline passengers who believe they've been wrongly detained or confused with someone on the watch

lists can call that office at 877-266-2837, or 877-2OMBUDS. They'll receive a form letter requiring additional personal information that must be notarized.

The TSA will check that information with its intelligence office and notify the airline if an individual is not on the watch list.

Last month, the office received 579 inquiries related to the no-fly lists. Of those, 258 forms were sent to callers seeking more information, and so far 135 have responded.

Critics say TSA has created a system that flags too many innocent passengers because of its secrecy in compiling the lists, combined with antiquated software to match names to suspected terrorists. As a result, many people are getting pulled over for secondary security checks and don't know why.

Mark Rotenberg, executive director of the Electronic Privacy Information Center, said about 100,000 people are on watch lists. Using the ombudsman to get off the list "is a flawed process," he said.

"This is a whole TSA activity that requires congressional scrutiny and a real overhaul," said Rotenberg.

LOAD-DATE: August 22, 2004

Document 1 of 2 next

About LexisNexis™ | Terms and Conditions | Privacy Policy | Support Identifier
Copyright © 2004 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

Copyright 2004 The Houston Chronicle Publishing Company
The Houston Chronicle

August 22, 2004, Sunday 4 STAR EDITION

SECTION: A; Pg. 1

LENGTH: 1692 words

HEADLINE: Science seen as slipping in U.S. ;
Visa hurdles are turning away foreign talent, experts argue

SOURCE: Staff

BYLINE: ERIC BERGER

BODY:
Hidden amid the hoopla of finding planets orbiting other stars, decoding the human genome and discovering miracle materials with nanotechnology, there's a seemingly improbable but perhaps even more important story - U.S. science may be in decline.

After 50 years of supremacy, both scientifically and economically, America now faces formidable challenges from foreign governments that have recognized scientific research and new technology as the fuels of a powerful economy.

"The Chinese government has a slogan, 'Develop science to save the country,' " said Paul Chu, a physics professor at the University of Houston who also is president of Hong Kong University of Science & Technology. "For a long time they have talked about it. Now they are serious."

According to the National Science Foundation and other organizations that track science indicators, the United States' share of worldwide scientific and engineering research publications, Nobel Prize awards, and some types of patents is falling.

A recent trend in the number of foreign students applying to U.S. schools is even more troubling, scientists say.

As American students have become less interested in science and engineering, top U.S. graduate schools have turned increasingly toward Europe and Asia for the best young scientists to fill laboratories. Yet now, with post-Sept. 11 visa rules tightening American borders, fewer foreign students are willing to endure the hassle of getting into the country.

"Essentially, the United States is pushing the best students from China and other countries away," Chu said.

The new restrictions also hassle students who are already here, like Lijun Zhu, a physics graduate student at Rice University since 1998 who returned two years ago to China to get married. The honeymoon became a nightmare when he and his new wife were stranded for more than two months, awaiting visa renewals.

"I was afraid of going outside my home for even a moment and missing the call from the consulate," Zhu recalled.

Losing future students like Zhu would cost more than just prestige in ivory towers. It could very well mean losing the nation's technological leadership, with implications for the nation's job market and

security, to say nothing of culture.

Decline called 'ridiculous'

Although President Bush's science adviser, John Marburger, dismisses as "ridiculous" the notion that America could lose its scientific prestige, scientists and policy-makers lay the blame in several areas: the drying well of foreign students, limited stem cell research and less federal funding for basic science research.

Since the visa restrictions were tightened in 2002, foreign-student applications to U.S. universities have fallen from 400,000 a year to 325,000, a 19 percent drop. Graduate school applications nationally are down even further, by up to 40 percent, said Jordan Konisky, vice provost for research and graduate studies at Rice University.

The problem, he said, is that when additional screening requirements were added, extra staffing in U.S. consulates to handle the workload was not.

And the atmosphere in these foreign offices, simmering with tension from terrorism's threat, breeds caution.

"No bureaucrat wants to make a mistake and approve a visa for someone that comes to this country and causes a problem," Konisky said. "So they tend to be very conservative about this, and that's good. But I think they're being overly conservative."

Graduate science programs at Rice and elsewhere are heavily dependent on foreign students.

Nearly half of engineering graduate students are foreign, as are more than one-third of all natural sciences graduate students.

These students invigorate research, professors say. They publish papers, bring new ideas and play a major role in patent applications.

Afraid to leave the U.S.

In 2003, the Rice graduate physics program admitted 16 foreign students. Two were delayed more than six months, and three were permanently blocked from entering the United States. Southern Methodist University has a smaller program, and in 2002, the two foreign students who were accepted didn't get visas. School officials briefly considered ending the program, but enough students gained visas in 2003 and this fall to keep it open, said Fredrick Olness, the SMU physics department chairman.

Yet even if students make it into the United States, their visa troubles, as evidenced by the plight of Zhu, aren't over.

Scientific conferences are held worldwide, and many students with families or looming deadlines at school opt not to travel for fear that they won't be able to come back. Likewise, meeting planners say the number of foreign scientists attending conferences in the United States has dropped because they don't want to bother with obtaining a temporary visa.

Then there are the physicists who want to work at some of the world's best particle accelerators, which are in Switzerland and Germany.

"All of the foreign faculty we have are afraid to leave the country because of visa problems," Olness said. "If this keeps up, the United States is going to take a hit on its stature in the worldwide physics community."

Seizing the opportunity

Marburger, himself a physicist, said changes to streamline visa problems, including adding staff in U.S. consular offices abroad, should be announced soon.

"This has very high visibility in Washington, all the way up to the president," Marburger said.

The winner, for now at least, is clear - scientific enterprise everywhere else.

At Hong Kong University, applications from Chinese students have more than doubled in the past three years. Chu says his faculty is thrilled.

Chu said Great Britain and Australia have seized the opportunity and opened recruiting offices in China. The European Union, too, has set a goal of having the most competitive and knowledge-based economy in the world by 2010.

What concerns U.S. scientists is that a decades-long brain drain into America may be coming to an end.

America began attracting scientists in the 1930s when the shadow of Hitler's political and religious persecution fell over Europe. Hordes of leading scientists such as Albert Einstein and Enrico Fermi, whose work with nuclear chain reactions led to the atomic bomb, immigrated to the United States.

Focus on science funding

After the war, the United States began spending billions of dollars on basic and defense-related research. Other great foreign scientists followed, drawn to new facilities and money. Their work laid the foundation for the technology bonanza of the 1990s, when one-third of Silicon Valley start-up companies were begun by foreigners.

Attracting top graduate students from other countries, then, is the first step toward continuing the trend.

"The United States used to welcome foreign scientists," said Zhu's adviser at Rice, physics professor Qimiao Si. "Nearly a century ago, the center of gravity shifted to the United States. We don't want that to happen in a reverse direction."

There are other policy areas that U.S. scientists say harm their ability to compete. Scientists say the Bush administration's policy to limit the use of embryonic stem cells will blunt advances made in biomedical research. "The stem cell decision has certainly put us behind at the front end of the curve," said Neal Lane, Clinton's science adviser. "It's a huge barrier."

The president's decision also led some U.S. researchers to seek private funds for their work. But this, said Sen. Kay Bailey Hutchison, usually a stalwart ally of Bush, is no solution to the issue.

"It's the federal research that is the big opportunity," the Texas senator said. "That's where the big dollars are. And to have these avenues to federal resources closed is going to hurt us in the long run."

Another problem, said Albert Teich, director of science and policy programs at the American Association for the Advancement of Science, is an increasing focus in the federal budget on applied military and homeland security research. Excluding a modest increase for biomedical research, nondefense research and development in the proposed 2005 federal budget would decline 2.1 percent, according to the association.

Marburger said federal science spending is still far greater than in any other country. The United States,

he said, spends 1 1/2 times more on research and development than all of the European Union countries combined.

Teich agreed, but only to a point.

"It is probably wrong to say U.S. science is currently in decline," he said. "But it is certainly in danger of declining. We're perched on the edge."

Another troubling trend

A fundamental problem, scientists and policy-makers say, is the lack of interest in science from American children.

Between 1994 and 2001, the number of U.S. students enrolling in science and engineering graduate programs fell 10 percent. Foreign enrollment jumped by 31 percent to make up for the shortfall.

National reports on this trend have offered suggestions to address the problem, such as giving money to community colleges to assist high-ability students in transferring to four-year science and engineering programs.

"Unfortunately, there's no silver bullet," said President Clinton's science adviser, Neal Lane.

Although there are some encouraging trends - the number of U.S. Hispanics enrolling in science graduate programs between 1994 and 2001 increased by more than one-third - the number of U.S. minorities in science graduate programs remains well below their representation in the total population.

. . .

A CRISIS IN SCIENCE?

Some statistics suggest U.S. science may be in decline.

U.S. productivity in publishing science and engineering research has been flat for more than a decade:

250

United States

200

Western Europe

100

China, South Korea, Singapore, Taiwan

50

Japan

. . .

As other nations publish more, the U.S. worldwide share decreases:

40%

. . .

U.S. science has increased its reliance on foreign students:

1983

Makeup of 346,952 science and engineering graduate students in U.S.

. . .

2001

Makeup of 429,492 students

GRAPHIC: Photo: 1. VISA HASSLES: Lijun Zhu, a physics graduate student at Rice University, went back to his homeland of China two years ago to get married. He and his wife then spent two months waiting for their visas to be renewed; Graph: 2. A CRISIS IN SCIENCE? (P. 21, TEXT); 1. E. JOSEPH DEERING: CHRONICLE, 2. ROBERT DIBRELL : CHRONICLE, Sources: Institute for Scientific Information, Science Citation Index and Social Sciences Citation Index; CHI Research, Inc.; and National Science Foundation, Division of Science Resources Statistics

LOAD-DATE: August 22, 2004

Document 1 of 1

About LexisNexis™ | Terms and Conditions | Privacy Policy | Support Identifier
Copyright © 2004 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

SHEILA JACKSON LEE
[illegible]

COMMITTEES
SELECT COMMITTEE ON
HOMELAND SECURITY
[illegible]
[illegible]
[illegible]

JUDICIARY
[illegible]
[illegible]
FOREIGN AFFAIRS
[illegible]
SCIENCE
[illegible]
[illegible]
DEMOCRATIC CAUCUS POLICY AND
STEERING COMMITTEE
[illegible]
CONGRESSIONAL BLACK CAUCUS

Congress of the United States
House of Representatives
Washington, DC 20515

[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

STATEMENT

BY

CONGRESSWOMAN SHEILA JACKSON LEE
HOUSE JUDICIARY SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
OVERSIGHT HEARING ON THE RECOMMENDATIONS OF THE 9/11 COMMISSION REPORT

AUGUST 23, 2004
10:00 A.M., 2141 RHOB

Chairman Coble and Ranking Member Scott, today's hearing is very necessary to the business of keeping this nation safe, and I appreciate the effort you have taken to hold it. It also appears incumbent upon other committees and subcommittees

whose jurisdiction deals with the recommendations found in the Report. The Subcommittee on Immigration and Claims, in which I serve as the Ranking Member, should hold a hearing to analyze the recommendations that deal specifically with border *issues*. I also thank the panelists for their testimony and participation on this very important matter. Our nation's safety cannot afford delay in the analysis and implementation of the recommendations made by the 9/11 Commission.

The National Commission on Terrorist Attacks upon the United States, known as "the 9/11 Commission," released its final report on July 22, 2004. The report provides an account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks, and it makes recommendations designed to guard against future attacks.

The Commission's report also cites to various immigration-related "missed opportunities" whereby intelligence and law enforcement could have hampered the 9/11 hijackers' ability to enter or remain in the United States. Some of the hijackers presented fraudulent passports; some of them made detectable false statements on visa applications; some made false statements to border officials to gain entry into the United States; and some violated immigration laws while in the United States by overstaying their visas.

According to the Commission, border security was not considered to be a national security matter prior to 9/11, so neither the State Department's consular officers nor the Immigration and Naturalization Service's inspectors or agents

were considered to be "full partners" in national counterterrorism efforts.

It is apparent to me that prior to 9/11, we were focusing on the wrong enemy, illegal immigrants, mostly from Mexico, who posed no threat to our national security. Immigration does not equate to terrorism. Nevertheless, our border control efforts on the ground still are overwhelmingly skewed towards keeping out illegal immigrants seeking work in the United States. We must focus our national security efforts on keeping out terrorists.

The Commission recommends a biometric entry-exit screening system that would apply to everyone crossing our borders. The Commission finds that Americans should not be exempt from carrying biometric passports or otherwise enabling their identities to be securely verified when they enter the United

States; nor should Canadians or Mexicans. I have some concerns about whether these measures would have a negative impact on travel and commerce. I agree fully, however, with the related recommendation that a system should be established to identify and expedite the admission of known travelers. This would permit inspectors to focus on those who pose greater risks. The daily commuter should not be subject to the same security measures as first-time travelers.

I agree with the Commission that we must know who is coming into the country. We also must be able to monitor and respond to entrances between our ports of entry, working with Canada and Mexico as much as possible. This is an awesome challenge for a nation that has 7,000 miles of land borders and 95,000 miles of shoreline.

A sledge hammer approach to border security could adversely effect our economy. Visiting international tourists and business entrepreneurs are a valuable component of our nation's economy. Last year, more than 41 million international visitors generated $88 billion in expenditures and accounted for more than one million jobs nationwide.

According to the Commission, new insights into terrorist travel have not been integrated yet into the front lines of border security, such as by training Homeland Security officers at airports and overseas consulates, and providing them with access to terrorist information databases. The Commission also found a lack of coordination and information-sharing among the U.S. intelligence community. The U.S. intelligence structure currently is not organized in a manner to allow for a unity of effort across the government.

The Commission recommends developing a National Counter terrorism Center (NCTC) that would direct and facilitate joint intelligence operations. The Commission believes that the NCTC should not be a policy-making body. The Commission wants NCTC operations and planning to follow the policy direction of the President and the National Security Council. The Commission wants a new National Intelligence Director to take on parts of the CIA Director's responsibilities and oversee national intelligence centers and agencies that contribute to the national intelligence program. I agree. I would make this a cabinet level position.

Early this month, I visited New York's financial district and the New York Stock Exchange (NYSE) today to assess the measures taken as a result of the recent "spot-elevation" in terror

threat level that has occurred in New York, New Jersey, and in Washington, D.C. During the visit, she reviewed the NYPD's anti-terrorism presence and procedures taken for the perimeter of the Exchange building, received a briefing on security at the NYSE and in New York's financial district by its Security Division, and toured the NYSE trading floor.

On pages 395-6 of the report, the Commission recommends that homeland security financial assistance should "**supplement state and local resources based on the risks or vulnerabilities that merit additional support.**" In addition, it suggests "that the allocation of funds should be based on an assessment of threats and vulnerabilities. That assessment should consider such factors as population, population density, vulnerability, and the presence of critical infrastructure within each state. In addition, the federal government should require each state

receiving federal emergency preparedness funds to provide an analysis based on the same criteria to justify the distribution of funds in that state."

Local areas that experience an increase in terror threat level should not be forced to spend valuable time recovering from the costs of the elevation when they should be actually *preparing* for a potential attack.

I am pleased to say, nevertheless, that the report stresses the need for protecting civil liberties while simultaneously enhancing our national security, and recommends that guidelines be established for gathering and sharing information in the new security systems which integrate safeguards for privacy and other essential liberties. The report recognizes that in protecting

our homeland, Americans should be mindful of threats to vital personal and civil liberties.

August 26, 2004

The Honorable Howard Coble
Chairman
Subcommittee on Crime, Terrorism and Homeland Security
House Judiciary Committee
207 Cannon House Office Building
Washington, DC 20515

The Honorable Bobby Scott
Ranking Member
Subcommittee on Crime, Terrorism and Homeland Security
House Judiciary Committee
207 Cannon House Office Building
Washington, DC 20515

Chairman Coble, Ranking Member Scott and Members of the Subcommittee:

At the oversight hearing on the recommendations of the 9/11 Commission held on August 23, 2004, there was some discussion of the commission's proposal to federalize state-issued driver's licenses. This proposal is similar to an initiative by the American Association of Motor Vehicle Administrators and is a back door approach to a National ID.

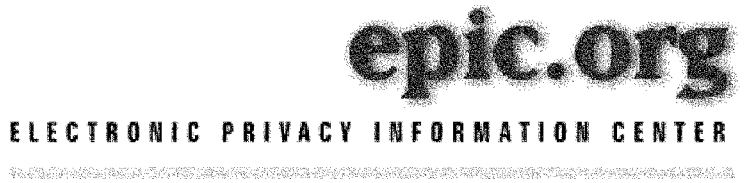
Enclosed is a report by the Electronic Privacy Information Center showing how such proposals would threaten privacy. Please enter this letter and the attached report into the record of the referenced subcommittee hearing.

Thank you for your kind and prompt attention to this request.

Sincerely,

Gregory T. Nojeim
Associate Director and Chief Legislative Counsel

cc: members of the Subcommittee



WATCHING THE WATCHERS – Policy Report #1 (February 2002)

"YOUR PAPERS, PLEASE: FROM THE STATE DRIVERS LICENSE TO A NATIONAL IDENTIFICATION SYSTEM"

An Assessment of the Proposal of the American Association of Motor Vehicle Administrators (AAMVA) to Transform the State Drivers License into a De Facto National ID Card

SUMMARY

The American Association of Motor Vehicle Administrators (AAMVA) Special Task Force on Identification Security has issued recommendations that would turn the state driver license into a de facto national ID card. The proposed scheme, analyzed in detail below, seeks federal legislation to require all states and other jurisdictions to conform to uniform standards for driver license eligibility, proof of identity, license content and document security. It would facilitate greater information sharing between jurisdictions and with state and federal agencies. It seeks to reduce fraud by encoding unique biometric identifiers on licenses and strictly enforcing prohibitions on credential fraud. But the biometric identifier would also enable new systems of identification in the private sector, and will contribute to greater profiling and surveillance of American citizens.

EPIC supports efforts to detect and prevent fraud occurring by means of the state driver's license. New technologies can reduce the risk of counterfeiting and fraud. It is also appropriate for the state Departments of Motor Vehicles (DMVs) to implement improved document security measures to prevent forgery. However, EPIC opposes AAMVA's move to standardize driver's licenses, to collect more and more invasive personal information, and to expand the information sharing capacities of DMVs.

This proposal has all the elements, risks and dangers of a national identification card system. The only distinctions between the AAMVA proposal and other National ID proposals rejected in the past are that (a) the card will not be issued by the federal government but by state motor vehicle agencies under mandatory federal regulations, and (b) the driver's license and DMV issued identity cards, held by 228 million individuals, are not (yet) mandatory. These distinctions are illusory rather than substantive, do not diminish the harm to individuals' privacy, and should not dissuade public opposition to the scheme.

The AAMVA proposal will have far-reaching and profound impacts on individual privacy. It significantly transforms the legitimate purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. It does not accomplish its stated aims of increased safety and security, but merely shifts the potential for fraud and identity theft to a higher plane, where the intrinsic privacy invasion is greater, and the means of remedying inevitable flaws in the system is more complex and difficult.

⇒ ***There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.***

AAMVA and its industry advisors[1] have not given adequate consideration to either the details of their proposed system or its consequences. They have failed to define the scope of proper access to and use of personal information, failed to consider mechanisms to prevent internal breaches or misuse by third parties, and failed to provide a means to correct abuses when they inevitably occur.

There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.

EPIC favors legislative proposals that would reduce the risks of counterfeiting and tampering, that would enable greater accuracy and reliability, and that would give individual license holders greater control over the subsequent use of their personal information. EPIC opposes provisions that would facilitate linkage of personal data among federal and state agencies, that would expand profiling of licensed drivers, and that would turn the state drivers license into an open-ended system of identification that could be routinely requested for purposes unrelated to the administration of motor vehicles and the safety of public roads.

Background of Driver's License Privacy

For more than a decade, state legislatures, the Congress, and even federal courts have worked to safeguard the privacy of driver record information. Aware that the widespread availability of the personal information obtained by state agencies for the purpose of licensing drivers has contributed to identity theft, financial loss, and even death, efforts to limit the use of driver's record information has been a high priority in the United States beginning with passage of the Drivers Privacy Protection Act of 1994, which limited the ability of state DMVs to circulate information obtained from individuals who applied for drivers licenses. The law, which was challenged by several states on federalism grounds, was upheld by the United States Supreme Court in one of the few recent opinions where the Court has held that the federal government has the authority to regulate state practices.[2]

Other steps taken to limit or reduce the risks of disclosure of personal information include efforts to allow non-commercial drivers to designate an identification number other than the Social Security Number. This change came about in part because of the awareness that the

[1] See http://www.aamva.org/links/mnu_lnkAssociate Members.asp for a list of AAMVA Associate Members & Industry Advisory Board Members and http://www.aamva.org/drivers/drvIDSecurityDocume nts.asp for a list of identification technology companies submitting reports to AAMVA's Special Task Force on Identification Security.

[2] *Condon v. Reno*, 528 U.S. 141 (2000) http://supct.law.cornell.edu/supct/html/98-1464.ZO.html. See also EPIC's Amicus Brief at http://www.epic.org/privacy/drivers/epic_dppa_brief.pdf

use of a single identifier, such as the SSN, was contributing to identity theft and white-collar crime.

States have also passed laws restricting the circumstances when a person can be required to provide a drivers license. And a federal appeals court ruled recently that it is unconstitutional for police to arrest someone for failure to provide identity documents.[3]

All of these developments in the United States over the past decade indicate widespread efforts at all levels of government to protect privacy and to reduce the risk that could result from the use of the state drivers license as a de facto national identifier.

Analysis of AAMVA recommendations[4]

Set out below is an assessment of the eight principles contained in the initial AAMVA report. The first three principles put forward by AAMVA are:

AAMVA(1) Improve and standardize initial driver's license and ID card processes
AAMVA(2) Standardize the definition of residency in all states and provinces
AAMVA(3) Establish uniform procedures for serving non-citizens

AAMVA seeks to "improve and standardize initial driver's license and ID card processes." This would include standardizing the definition of residency and imposing uniform procedures for non-citizens[5]. Such a proposal raises serious questions about the appropriate scope of state DMV authority and infringes on a state's right to develop systems and processes to serve the particular needs of its citizens.

AAMVA states its aim to "develop/capture citizenship/residence on document and/or database" within the next year.[6] It is not clear what role establishing citizenship and uniform residency status plays in the core function of a driver's license: ensuring that there are trained, safe drivers on the roads. In fact, the proposed requirements would undermine the public safety rationale of a driver's license by discouraging undocumented aliens from getting licenses, leading to more uninsured and untrained drivers on the roads and contributing to the national road toll of 40,000 deaths per year.[7] Different states have formulated specific responses to this issue based on their individual circumstances, and there is no overriding federal need to establish uniform procedures.

> ⇒ ***Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.***

Establishing citizenship and residency status shifts the role of the state DMVs from licensing drivers to verifying the identity of all Americans. AAMVA relies on faulty reasoning to make its argument: driver's licenses are used as identity cards for purposes unrelated to the operation of a motor vehicle, such purposes

[3] *Carey v. Nevada Gaming Control Board*, No. 00-16649 (9th Cir. 2002) http://caselaw.lp.findlaw.com/data2/circs/9th/0016649p.pdf

[4] AAMVA Press Release, January 14 2002 [http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp].

[5] Other consequences of standardization are discussed below in the context of AAMVA's proposal for a "uniform" national driver's license.

[6] AAMVA Special Task Force on Identification Security Report to the AAMVA Board at 4 [Hereinafter "AAMVA Task Force Report"].

[7] The National Institute of Health reports 41,717 traffic fatalities in 1999. [http://www.niaaa.nih.gov/databases/crash01.txt].

include verifying employment status, opening bank accounts, and renting apartments. Since there are people who mistakenly rely on a driver's license to prove lawful status, and there are those who might seek to exploit this weakness, the appropriate solution is to change the driver license into a document that does, in fact, verify lawful presence. This is a dramatic and unwarranted expansion of function for a state *motor vehicle* department. Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification in cases where there is a genuine need to establish identity. Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.

> ⇒ ***Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification.***

AAMVA(4) Implement processes to produce a uniform, secure, and interoperable driver's license/ID card to uniquely identify an individual.

Strategy 4 is the core of AAMVA's driver license reform proposal, and contains several distinct elements that are yet to be adequately explored, developed, or discussed with the public. This strategy incorporates the following distinct ideas: uniformity (of both issuing standards and documents); security (of the identity of the applicant, and of the integrity of the document itself); interoperability (requiring uniformity, and mandating data sharing between states and with other parties); and a unique identifier.

Uniformity

AAMVA proposes that the issuing processes and requirements, as well as the information collected and maintained by the DMV, should be uniform across all states.

Uniformity of Issuing Standards

The AAMVA proposal relies upon the imposition of a national uniform standard for driver's license issuing processes.[8] AAMVA is also lobbying for Congress to delegate "the criteria and implementation of the uniform standard" to AAMVA itself.[9]

However, AAMVA have not demonstrated that uniformity is necessary to address any specified problem with the current system. They claim that "Unscrupulous individuals shop for the easiest and fastest way to get a license. They find the loopholes and they put you and me at risk."[10] There has been no substantiation from AAMVA of their claim that such "weak" licensing requirements have allowed dangerous individuals to obtain licenses, and no analysis of any security threat posed.

> ⇒ ***As yet, none of the parties involved in the proposal have announced what the new uniform processes should be.***

Further, if such a problem does exist, it can be addressed equally effectively, and without the disadvantages of a national ID system, by strengthening the issuance standards in those

[8] AAMVA Task Force Report at 2, Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

[9] Statement of Senator Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

[10] Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

states that are the "weakest links" in the system. In fact, in recent months several states have changed their application procedures to address perceived loopholes[11]. The proposal does not even demonstrate the advantages of a national uniform system over a national minimum standard, or of state-specific actions to close existing loopholes. Thus it is not narrowly tailored to the perceived problem and infringes on individual privacy for no justifiable ends.

As yet, none of the parties involved in the proposal have announced what the new uniform processes should be. It is therefore impossible to evaluate whether uniform standards would be effective in meeting perceived problems in the system, to what extent privacy interests would be compromised, and whether the proposal appropriately balances the interests of identification security and privacy.

AAMVA is not the appropriate body to be determining the balance between identification and privacy. AAMVA is a trade association that "represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws."[12] with a large industry advisory board including insurance, identification technology and information management companies.[13] The determination of uniform national standards and procedures is not appropriate for a bureaucracy with no direct accountability to the public, and a vested interest in the proposed system.[14] These decisions properly belongs to the state legislatures and the Congress, after a period of public debate and consultation.

Uniformity of License Documents

Just as there is no proven need for uniform application procedures and standards, there is no demonstrated need for uniformity of state driver's licenses. There are already mutual recognition programs and database pointer systems in place to address the needs AAMVA has identified. The primary reason for uniformity would be to enable information sharing with both government and private sector organizations as discussed below. In this context, uniformity intrinsically facilitates tracking, monitoring, profiling and other privacy invasive practices.

AAMVA's 90-day action plan includes efforts to "encourage voluntary short-term use of AAMVA standards in all jurisdictions," and "work with Congress to introduce DRIVerS legislation,"[15] before introducing model legislation in each AAMVA jurisdiction within one year.[16]

The adoption of the AAMVA standard by states would allow the use of driver's licenses as an identification and information gathering mechanism not only for government, law enforcement and security purposes, but also in the private sector. Products are already available that scan the AAMVA-compatible magnetic strip on a driver's license, and download 16 data fields captured on the license.[17] The information can then be compiled

[11] For example, Virginia no longer allows online renewal of driver's licenses, and has changed the identification documents required for a driver's license or identification card application: http://www.dmv.state.va.us/webdoc/citizen/drivers/applying.asp.

[12] AAMVA website http://www.aamva.org/about/

[13] AAMVA website http://www.aamva.org/links/mnu_lnkAssociateMembers.asp.

[14] AAMVAnet currently administers, and charges DMVs for access to driver and vehicle databases, and online verification networks: http://www.aamva.org/products/mnu_proAAMVANetApp.asp.

[15] AAMVA Task Force Report at 5.

[16] Id. at 3.

[17] The fields include: Last Name, First Name, Middle Name, Address1, Address2, City, State, Zip Code, Birthday, Drivers License Number, Drivers License

with data entered by the company, including a date/time stamp to track the individual's presence and information on their purchases. It may also be retained by the company, producing a database of detailed customer information that could not economically be compiled in the absence of such technology. These products are being marketed to companies that routinely check driver's licenses as identification or proof of age, including auto dealerships, clubs, bars, restaurants, and convenience stores. They are also suggested for use by health clubs and personal trainers "for use as a billing aid" and in the general retail market "to expedite adding customers to your monthly mailer."[18] AAMVA has also publicly stated that it seeks to share its model with retailers, car rental companies, insurers and banks.[19]

Security

AAMVA presents driver's license security as a single problem, but it can be distinguished into two different issues - document security and identification. EPIC supports the use of creative technology to improve document security if it is aimed at making it more difficult to counterfeit driver's licenses.[20] There is no demonstrated need, however, to establish uniform document security features across the 50 states. Each state DMV is capable of determining the needs of its customers and can incorporate features best situated to them.

Identity security concerns stem from the "one-driver, one-license, one-record" concept touted by AAMVA. In the AAMVA Special Task Force on Identification Security Report to the AAMVA Board, any pretense of a system concerned primarily with drivers is eliminated: the revised motto is "one card, one person, one record."[21] There are two main problems with such a concept. First, serving as the nation's main identity authenticators will distract a state DMV from its core function of licensing competent drivers and registering safe vehicles. Second, attempting and claiming to establish proof-positive identity is a very complex and error-prone task that creates more problems that it might solve.

Increasing reliance on the driver's license as an internal passport dramatically raises the incentives to forge or steal such credentials. If DMVs limited the use of the document for driver's licensing purposes the fraud incentives would drop significantly, particularly if the cost of fraud were raised by better document security features and stringent enforcement of identity theft laws.

> ⇒ ***As the importance of the card increases, the incentives to create fraudulent documents will also rise.***

Expiration Date, Sex, Height, Weight, Hair Color, Eye Color. See http://www.intellicheck.com/What_is_IDCheck.htm for the Intelli-Check IDCheck system, which operates not only on mag stripe cards but also 1D and 2D barcodes, and allows downloads for permanent archiving of customer identification and transaction information. See also http://www.dgahouston.com/dlsplit1.htm for product information on DLSPLIT "software to separate, format and display driver's license data," available online for US$169.60, including mag stripe reader.

[18] http://www.dgahouston.com/dlsplit1.htm for examples of "DLSPLIT Uses"

[19] "Task G: Promote the use of the Uniform Identification Practices model program developed by this Working Group to various potential customers, such as: all AAMVA jurisdictions; insurance companies, banks; travel industry; car rental agencies; retailers; others." AAMVA Uniform Identification Practices Working Group available at http://www.aamva.org/drivers/drvDL&CuniformIdentificationWG.asp

[20] Examples of such physical security features can be found listed in Appendix H of AAMVA's DL/ID Standard. Available at http://www.aamva.org/documents/stdAAMVADLIDStandrd0006630.pdf

[21] AAMVA Task Force Report at10.

DMVs must necessarily continue to rely on "breeder" documents such as birth certificates and Social Security card to establish identity. These documents are easily forged or obtained and are the main sources of identity fraud. There are currently 14,000 different versions of birth certificates in circulation.[22] A major source of fraudulent drivers licenses is DMV employees.[23] As the importance of the card increases, the incentives to create fraudulent documents will also rise. Moreover, the technology to uniquely identify individuals is untested for a large population, and previous applications of similar technology reveal significant technical error rates.[24] The enrollment process -- how we move from our current system to a unique identifier system -- will also present a number of difficult problems, including an anticipated rise in identity theft by criminals seeking to take advantage of the new procedures to establish "hardened" identities. The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

Interoperability

For licenses to be "interoperable," they must be (a) in a compatible format across the nation, and (b) supported by a network allowing different parties to access the information linked to the individual license holder.

If AAMVA succeeded in making driver's licenses uniform across the nation (as discussed above), it would automatically satisfy the first criteria of interoperability: because there would be no relevant differences between licenses from Connecticut and Colorado, they would be interoperable.

> ⇒ ***The combination of cost, technical obstacles, and American constitutional values argue against a national identification system in the United States.***

To achieve functional interoperability, AAMVA plans to link information systems. This would enable a DMV or other authorized person to obtain the same information about a license holder regardless where the license was issued. It would also enable other entities, including government agencies and the private sector to access the information on the card. Both means of information sharing would compromise the privacy of driver's license holders.

Information sharing between states

There is already information sharing between states with regard to problem drivers in the Problem Driver Pointer System (POPS) and Commercial Drivers License System (CDLIS). There has been no demonstrated need to expand interstate information sharing beyond the existing capacity, which addresses the problems articulated thus far by AAMVA such as multiple licenses and avoidance of penalties. To the extent that AAMVA claims that PDPS does not capture problem drivers adequately, then that system should be improved, rather than creating a new system covering all drivers, including those with unblemished records.

[22] Birth Certificate Fraud (OEI-07-99-00570;9/00), September 2000, Office of Inspector General, Department of Health and Human Services, http://oig.hhs.gov/oei/reports/a492.pdf

[23] 127 California DMV employees were disciplined over the past 5 years for facilitating ID fraud. "Legislators Order DMV Audit", *Orange County Register*, February 27, 2001

[24] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (revision 2), San Jose State University, December, 1997 http://www.engr.sjsu.edu/biometrics/publications_fhwa.html

AAMVA's proposal for information sharing between states includes a complete feasibility study for photo exchange and specifications within 90 days.[25] But apparently regardless of the outcome of the study, AAMVA also plans to "obtain commitments for photo exchange as feasible" within the year, and begin to "implement standard image exchange" in 2003.[26]

AAMVA has set no limits on future information sharing between DMV administrators in different jurisdictions. It includes as stated goals to "coordinate effort to verify out-of-jurisdiction licenses electronically" and "continue efforts in North America *and internationally* regarding driver license/ID standards" (emphasis added).[27]

Information sharing with other entities

AAMVA has announced that it would like to link the state DMV databases with, and provide mutual access rights to, various government agencies, including SSA, INS, FBI, and some commercial organizations.

AAMVA wants its members in state DMV offices to have access to the records held by SSA, INS and Vital Statistics to assist in verifying the identity of license applicants.[28] Despite the history of abuse of personal information by DMV employees, and the privacy harm in releasing other government-held information for the unrelated purpose of driver's license ID verification, AAMVA has proposed no new safeguards to protect individuals' privacy under this practice. The AAMVA proposal to allow DMV employees to access information in state and federal agencies may require amendments to current law that protects the privacy of these records.

AAMVA has not specified the agencies that will be provided with access to driver's license information, or provided any suggested regulations to guard against a future expansion of its availability.

There is a long history of opposition by the DMVs themselves to increased information sharing, and an expansion of their information gathering function. One example of AAMVA's proposed information sharing schemes is to "improve social security number on-line verification" within one year. A similar proposal was widely rejected in 1998 under the NHTSA's Notice of Proposed Rulemaking Docket No. NHTSA-98-3945, pursuant to the (now repealed) §656(b) of the Immigration Reform Act of 1996. In a letter dated July 31 1998, opposing the NHTSA proposal, Betty Serian, Deputy Secretary of the Pennsylvania Department of Transportation, later Chair of the AAMVA Task Force on Identification Security, highlighted many of the concerns of states.[29]

Ms. Serian wrote that "the proposed requirement that states must, in all cases, verify social security numbers exceeds the statutory authority of the law" by "usurp[ing] each state's discretionary authority . . . creating a national driver's license." States require flexibility to determine what identification documents they find acceptable, based on their particular local or historical factors. Ms. Serian argued, "states

[25] AAMVA Task Force Report at 5.
[26] Id. at 3 and 5.
[27] Id. at 5.
[28] "AAMVA supports and encourages the access by its members (government entities) to other databases, such as SSA, INS and Vital Statistics to confirm identify, residency, citizenship and address verification" AAMVA Task Force Report at 8. They also plan to "improve jurisdiction access to SSA, INS and others" within a year (p. 5), "implement on-line address verification" after one year (p. 4), "continue to improve verification with the INS" within the year (p. 4)

[29] Letter on file with EPIC and available at http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html.

must have the flexibility to provide for exceptions without draconian federal intervention."

Ms. Serian also cautioned of the administrative burden of the proposal, estimating that "the social security check will not match the SSA's records in approximately 20% of the cases because of the use of nicknames . . . unmarried names, data entry errors, etc. on the social security record." The SSA provides only a "Not Valid" message when the name and number do not match, forcing DMV administrators to interact with customers repeatedly. Additionally, the burden required to change data formats to achieve uniformity would be untenable. Ms. Serian stated that adding a full middle name to driver license records "would require 28 data entry clerks four years to complete the conversion" just for Pennsylvania's records. Ms. Serian concluded that the requirements were "very costly, ineffective, and customer hostile, once again adopting a theoretical approach while ignoring basic service needs of law abiding customers... Government at the state level . . . would be harmed." The additional burden in the AAMVA proposal of extra fields, including complex encoded biometric data, and altered formats to accommodate information sharing would constitute an unjustified and extravagant burden on state DMVs.

Existing Legislative Limitations on Information Sharing

Existing legislation limits the ability of DMVs and other agencies to share information. AAMVA's proposal would require substantial amendment to these laws, removing significant privacy protections that have been in place for many years.

The **Driver's Privacy Protection Act** presently contains no provisions governing the use of biometric identifiers. Before a system such as that proposed by AAMVA could come into effect, an amendment would be required incorporating biometric identifiers into the definition of "personal information" in 18 USC 2725(3),[30] and providing greater protection for the privacy of such information.

Biometric identifiers should also be incorporated in the definition of "highly restricted personal information," as defined in section 2725(4). This category currently includes "an individual's photograph or image, social security number, medical or disability information."

The prohibition on the use and disclosure of personal information in section 2721 is subject to many exceptions. The initial portion of sub-section 2721(b) requires that personal information (including highly restricted personal information) shall be disclosed in connection with the administration of a wide variety of motor vehicle related laws,[31] including

[30] 18 USC 2725(3) currently provides that "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and the driver's status.

[31] 18 USC §2721(b): "Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 USC 1231 et seq.), the Clean Air Act (42 USC 7401 et seq.), and chapters 301, 305, and 321-331 of title 49 [49 USC §§30101 et seq., 30501 et seq., 32101-33101 et seq."

environmental standards and investigation by motor vehicle manufacturers.

The prohibition on information sharing is also subject to the "permissible uses" listed in sub-section 2721(b). The permissible uses of highly restricted personal information are a subcategory of these uses, and comprise:

> (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
>
> (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
>
> (6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
>
> (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49 [49 USCS §§ 31301 et seq.].

Highly restricted personal information may be disclosed to any party for any with the express consent of the person to whom the information applies.[32]

There are several currently permitted uses of highly restricted personal information which would constitute further privacy violations if a biometric identifier was included on the driver's license and in the information collected by the DMVs.

The required disclosure of biometric identifiers in connection with motor vehicle laws under sub-section 2721(b) allows access to personal information by a wide variety of organizations for many purposes, where there is no demonstrated need to use such information.

The exceptions under sub-section 2721(b)(1) for sharing information with other government agencies could allow AAMVA to go even further. The provision is not limited to the SSA, INS, FBI or other agencies concerned with national security, but extends to any function of any government agency, including State and local governments and those acting on their behalf. DMV administrators thus already have the authority to share information (including biometric identifiers), and thus make provision of a driver's license a prerequisite of any interaction with government agencies.

The sensitivity of biometric information, and its use by motor vehicle administrators, was not considered by Congress at the time the Driver's Privacy Protection Act was passed in 1994.[33] The Act would require substantial amendment to take account of changes in technology, and to protect the privacy interests of driver's license holders.

[32] 18 USC §2721(a)(2).
[33] See also the discussion of biometric unique identifiers below.

There is as yet no proposal for auditing requests for access made to the DMV, or any avenue for appeal or review of decisions to grant disclosure based on the factors in the DPPA. AAMVA's proposal should include a provision requiring all DMVs to keep a record of all disclosures of personal information, and make those requests accessible to the individual to whom the information pertains.[34] If the Canadian members of AAMVA decide to join the scheme, amendments would likely be required to Canadian Provincial privacy laws, which are generally more stringent than either state or federal regulation in the United States.

Technological feasibility of information sharing

Creating a national database on 228 million Americans creates myriad problems[35]. Such a database would probably use a pointer or index system to link distinct state databases -- this is precisely how most large databases are constructed. The key issue is determining the data elements that would be used to create the index. AAMVA is lobbying for the use of the Social Security number along with name and date of birth to link the records. This is in spite of the fact that §656(b) of the Immigration Reform Act of 1996, which would have mandated the display of SSNs on state driver's license, was repealed because it would have facilitated precisely the sort of information sharing AAMVA is currently contemplating.[36]

Aside from the important policy arguments against creating such a database, these databases are notoriously mistake-prone, difficult to secure, open to abuse, and expensive to compile and operate. Reconciling different databases such as those of the Social Security Administration is expected to generate 20% error rates.[37] Linking with INS and FBI databases will likely present similar issues.

> ⇒ ***The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database.***

Actually connecting the different databases is also a significant problem -- the FBI and INS have been trying to link their databases for over a decade. Moreover, large databases do not present any solution to the problem of bad data: once in a database of any sort, data -- errors and all -- tend to be authoritative, pervasive and persistent. A U.S. PIRG study found 30% of credit reports contain serious errors and 70% contain some errors.[38] The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database. Instead of solving public safety problems, the government will create a bureaucratic headache that will take resources away from performing the functions that specific agencies are meant to

[34] Such a requirement exists in many state jurisdictions, often with an exception that the request information need not be provided where it relates to an ongoing criminal investigation of the person to whom the information pertains and the release would prejudice the investigation.

[35] AAMVA states that 228 million US and Canadian citizens have either a driver's license or a DMV issued identity card, representing 75 percent of the total population: AAMVA Task Force Report at 8.

[36] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001,, section 3.4.4 p. 41

[37] See Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA, July 31, 1998 http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html. See also the problems faced in California last year when the DMV began to verify social security numbers. "Glitch in DMV crackdown leaves some drivers unable to renew licenses", San Jose Mercury News, June 23, 2001

[38] Available at http://www.pirg.org/reports/consumer/mistakes/

carry out. State DMVs already operate with over-stretched resources and there is no reason why they ought to take on the burden of administering a national database.

Unique Identifier

> ⇒ ***The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy.***

AAMVA has not determined the mechanism will be used to uniquely identify individual license holders, although it has acknowledged that it contemplates the use of biometric technology. [To uniquely identify an individual, an identifier must be verifiable against the person's actual identity, that is, their permanent physical characteristics. Any alphanumeric identifier can only be verified by the possession of corresponding documents; a biometric can be used to verify the information held by the agency or on a card by reference to the actual physical characteristic it refers to. Thus it appears that AAMVA intends to implement some kind of biometric identifier.]

The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy. Whereas a license number or a PIN number can be randomly assigned, and is not in itself personally identifiable information, a biometric is inextricably linked to the particular individual it codes for. A recent opinion of the Eastern District of Pennsylvania noted that analysis of fingerprints may yield other personal information, such as the individual's environmental conditions, disease history and genetics.[39]

Notwithstanding the close link between biometrics and identity, biometrics are not fraud-proof. For example, licenses may currently be fraudulently obtained with mismatched details, such as the name, address, SSN and date of birth of one person and the photograph of another person who holds the card and may impersonate the named person. The photograph is a biometric, although not usually a digitized biometric such as AAMVA proposes, and it can be falsified. Other biometrics, such as fingerprints and retinal scans, may thus also be fraudulently placed on licenses. Their inclusion would make it extremely difficult for victims of identity theft to prove their identity, once a biometric other than theirs is associated with their driver's license.

> ⇒ ***Biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers.***

To remedy the fact that biometric identifiers can be compromised in much the same way as the Social Security number or a photograph. AAMVA is contemplating the inclusion of multiple biometric identifiers on the license. Of course, this proposal does not make the license fraud-proof, nor change the nature of biometrics. Instead it compromises privacy and further hampers victims of identity theft with no commensurate security benefits.

Finally, biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers. Even fingerprinting, a common technique used in law enforcement, has not been subjected to such large-scale use and there are important limitations emerging about the

[39] *USA v Llera Plaza et al*, Nos. CR 98-362-10 to 98-362-12, at 2 (E.D.P.A. filed Jan. 7, 2002) [http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM].

reliance on the technique.[40] Automated fingerprint examination is not foolproof -- a 3% error rate (a conservative guess assuming the technology and databases are used following precise directions) will mean that over 6 million Americans might be incorrectly identified in the database.[41]

For these reasons, EPIC opposes the inclusion of biometric identifiers on driver's licenses and identification cards.

AAMVA(5) Establish methods for the prevention and detection of fraud and for auditing of the driver's license/ID processes.

AAMVA(6) Ensure greater enforcement priority and enhanced penalties for credential fraud.

EPIC supports internal reform at the DMVs to remedy their record of fraud and abuse of personal information. The Driver's Privacy Protection Act provides that violations of its provisions may be addressed by individual criminal fines, per diem penalties against the DMV, and civil actions resulting in actual damages of not less than $2,500, punitive damages and costs.[42]

AAMVA have not demonstrated a need for additional laws or penalties regarding driver license fraud and unauthorized use of data. The existing laws provide strict penalties and prohibitions but AAMVA's member jurisdictions have failed to implement successful investigation and enforcement strategies. In a previous effort to combat terrorism through reducing ID fraud, the specially formulated Federal Advisory Committee on False Identification rejected the idea of a unique identifier and instead recommended better enforcement and higher penalties. These recommendations were codified in 18 USC §1028. The Internet False Identification Prevention Act of 2000 amended §1028 to address changes in technology. That Act also established a multi-agency Coordinating Committee on False Identification, which is due to report on the efficacy of current ID fraud laws in March 2002 and again in March 2003.

AAMVA(7) Seek U.S. federal and other national requirements for legislation, rule making and funding in support of AAMVA's identification and security strategies.

AAMVA proposes to "seek mandatory US federal and Canadian legislation to impose and fund national and uniform driver license/ID standards."[43] AAMVA states that such legislation would be required before any significant progress is made on its strategy. While legislative support is needed for certain key elements in the strategy, state DMVs can still move ahead on other parts without Congressional mandate. For instance, AAMVA is encouraging the voluntary use of its DL/ID standard, which facilitates information sharing among the states, enforcement authorities, and private industry.[44] AAMVA is also encouraging states to adopt uniform citizenship and residency standards as well as Social Security number verification. The problem for AAMVA is that as long as all states are not on board, the system continues to be limited. Its proposed national strategy is a way of compelling states to adopt uniform standards.

---

[40] Pankanti et al., *On the Individuality of Fingerprints* (Michigan State University 2001) http://biometrics.cse.msu.edu/cvpr230.pdf.

[41] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (San Jose State University December, 1997).

[42] 18 USC sects. 2721, 2723(a), 2723(b).

[43] AAMVA Task Force Report at 6.

[44] See http://www.intellicheck.com/Jurisdictions.htm for the states that have machine-readable licenses.

AAMVA must also make transparent the detailed financial structure of its program. It has asked the federal government for $100 million, however, a report from last July to Congress in which AAMVA was a co-author stated that $24 to S35 million would be required to implement an Integrated Driver License Identification System (IDLIS), with an annual operating cost of $17-S21 million.[45] The report notes that there are "substantial costs involved in developing and converting to a system encompassing all drivers" but that "once such a system would be operational, states could recover costs of operating by assessing driver license fees and related fees."[46]

AAMVA(8) Establish public and stakeholder awareness and support

It is clear that such a wide-ranging proposal requires public debate and thorough scrutiny. AAMVA's legislative schedule, as currently formulated, does not accommodate the time that would be needed for Americans to examine the appropriateness of introducing a national ID system through the state DMVs. Moreover, the technical and procedural consequences if such a scheme is implemented have not been adequately explored. At the very least, there must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.

⇒ ***There must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.***

UNEXPECTED RESULTS

AAMVA states that it expects it national ID strategy to result in a safer America through:

a) increased security,
b) increased highway safety,
c) reduced fraud and system abuse,
d) increased efficiency and effectiveness,
e) uniformity of processes and practices.

AAMVA's scheme in fact diverts resources away from current priorities and fails to resolve any of the perceived problems. Each of its expected results is briefly refuted below:

⇒ ***A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact be terrorists -- to avoid heightened security measures.***

Increased Security

An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain -- by legal and illegal means -- the documents needed to obtain a government ID, such as birth certificates and social security numbers. A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact pose security threats -- to avoid heightened security measures.

A national ID program should be evaluated in the same way we might evaluate other security countermeasures. First, what problem are IDs

[45] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001, Section 3.6 at 43

[46] Id. at 3

trying to solve? Second, how can an ID system fail to achieve its goals in practice? Third, given the failures and the loopholes in the system, how well do IDs solve the security problem? Fourth, what are the costs associated with IDs? And finally, given the effectiveness and costs, are IDs worth it?

Increased Highway Safety
Information on problem drivers is already shared between states under the Problem Driver Pointer System, administered by AAMVA. Any deficiencies in this system can be remedied by amending its scope and operation: a new system for law-abiding motorists is unnecessary. Establishing uniform residency and citizenship standards and cross-checking applications with criminal records would discourage many people from getting licenses and therefore increase the number of untrained and unlicensed drivers on the roads.

> ⇒ ***Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy.***

Reduced Fraud & System Abuse / Increased Efficiency & Effectiveness
If the driver license acquires more importance in society as a "gateway" or internal passport document, the incentives for fraud will greatly increase. The unprecedented infrastructure required for creating a national ID scheme would make it difficult to differentiate abuses from technical errors and glitches. Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy. The error rates alone will reduce system-wide efficiency and make the process of obtaining a driver's license a nightmare. There is no precedent for such a large database being effectively compiled and securely managed. If prior experience is any guide, the technological, privacy and security problems will be formidable.

Uniformity in Processes & Practices
There is no reason to impose uniform processes and practices, and override each state's right to develop its own practices. It will take significant resources to ensure that processes and practices are truly uniform across the country. California, for instance has been collecting fingerprints for over 20 years but most of the 60 million prints in its database are useless because of poor operating practices in collecting the data.[47] Such errors will only be magnified in a national program. Finally, AAMVA does not demonstrate how "uniformity in process and practices" is either necessary or effective in creating a "safer America."

> ⇒ ***There are several less expensive, less invasive and better-crafted alternatives***

Alternatives

There are several less expensive, less invasive and better-crafted alternatives which would not lead to the creation of a national ID card yet would address AAMVA's perceived problems of poor document security. For instance, AAMVA might develop training programs to improve the ability of DMV staff to detect fraudulent documents. Technology can be used creatively to enhance document security using features such as holograms and ultra fine lines. AAMVA can also help develop model audit and verification systems that states can choose to implement if they feel their procedures are inadequate.

[47] "Failure to finger fraud: DMV's thumbprint database is insufficient -- and costly to fix." Orange County Register, December 31, 2000

Recommendations

AAMVA's proposal to implement a national ID scheme through the driver's license system is a backward step for individual privacy with no substantial countervailing safety or security benefits. At present, the case against adoption of a national ID card in the United States is compelling.

- Efforts to detect and prevent fraud occurring within DMVs, or with the assistance of DMVs and their employees, should be pursued.

- Improved document security measures to prevent counterfeiting and tampering are overdue and should be pursued, but measures that enable profiling and tracking of licensed drivers in the United States raise far-reaching policy concerns.

- AAMVA's move to standardize driver's licenses nationally, to collect more and more invasive personal information, and to expand the information sharing capacity of DMVs raises substantial privacy concerns that have not been adequately addressed

- AAMVA's proposal has all the elements and problems of a National ID Card. Although the card would not be mandated by federal law or issued by a federal agency, in many respects it reaches further than a simple ID card and might be better understood as the creation of a National Identification System. AAMVA recognizes this, citing as a "major implication" of their proposal that "the continued evolution and improvements of the driver license/ID card precludes the need for a new, separate national identification card."[48]

- AAMVA's proposal significantly changes the purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. In diluting this central function, the AAMVA proposal may reduce public safety.

- The increasing reliance on a single centralized form of identification makes ID theft simpler, and more difficult for victims to remedy.

- AAMVA must define the scope of proper access to and use of personal information, consider mechanisms to prevent internal breaches or misuse by third parties, and provide a means to correct abuses when they inevitably occur, before its proposal can be thoroughly analyzed.

- There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system. This proposal is moving too quickly, with too little consideration of the long-term impact on privacy and the risk of new forms of identity theft and fraud.

CONCLUSION

The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

REFERENCES

AAMVA website: http://www.aamva.org

AAMVA Driver's License / Identification Card Standard
http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp (summary)

[48] AAMVA Task Force Report at10.

http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf (full report)

AAMVA Executive Committee Resolution establishing the Special Task Force on Identification Security
http://www.aamva.org/Documents/hmExecResolution.pdf

AAMVA Special Task Force on Identification Security information
http://www.aamva.org/drivers/drvIDSecurityindex.asp

AAMVA Special Task Force on Identification Security Report to the AAMVA Board, Executive Summary
http://www.aamva.org/drivers/drvIDSecurityExecutiveSummary.asp. (Full report on file with EPIC).

Commercial Applications of AAMVA Standard Driver's Licenses:
http://www.dgahouston.com/dlsplit1.htm
http://www.intellicheck.com/

Driver's Privacy Protection Act 18 USC §2721 et seq.

Statement of Senator Richard Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA dated July 31 1998
http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html

USA v Llera Plaza et al, Nos. CR 98-362-10 to 98-362-12 (E.D.P.A. filed Jan. 7, 2002) (motion to preclude the US from introducing latent fingerprint identification evidence)
http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM

Condon v. Reno, 528 U.S. 141 (2000).
http://supct.law.cornell.edu/supct/html/98-1464.ZO.html

Carey v. Nevada Gaming Control Board, No. 00-16649 (9th Cir. 2002)
http://caselaw.lp.findlaw.com/data2/circs/9th/0016649p.pdf.

Reports

James L. Wayman, *Biometric Identification Standards Research. Final Report Volume* I, San Jose State University December, 1997
http://www.engr.sjsu.edu/biometrics/publications_fhwa.html

Office of Inspector General, Department of Health and Human Services. *Birth Certificate Fraud.* September 2000
http://oig.hhs.gov/oei/reports/a492.pdf

John J. Miller and Stephen Moore, *A National Id System: Big Brother's Solution to Illegal Immigration*, September 7, 1995
http://www.cato.org/pubs/pas/pa237es.html

Sharath Pankanti, Salil Prabhakar & Anil K. Jain, *On the Individuality of Fingerprints.* Michigan State University, 2001
http://biometrics.cse.msu.edu/cvpr230.pdf

Public Interest Research Group (PIRG), *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose.* March 1998
http://www.pirg.org/reports/consumer/mistakes/

National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, *Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies,* July 2001

http://www.aamva.org/Documents/Library/libNHTSAReportToCongress.pdf

Robert Ellis Smith, *A National ID Card: A License to Live, Privacy Journal,* December 2000.

Shane Ham and Robert D. Atkinson, *Modernizing the State Identification System: An Action Agenda*, February 2, 2002 http://www.ppionline.org/documents/Smart_Ids_Feb_02.pdf

Charlotte Twight, *Why Not Implant a Microchip?*, February 7, 2002 http://www.cato.org/dailys/02-07-02.html

Adam Thierer, *National ID Cards: New Technologies, Same Bad Idea*, TechKnowledge No. 21, September 28, 2001 http://www.cato.org/tech/tk/010928-tk.html

Lucas Mast, *Biometrics: Hold On, Chicken Little*, TechKnowledge No. 31, January 18, 2002 http://www.cato.org/tech/tk/020118-tk.html

Simon G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine," *Information Technology & People,* Vol 7, No. 4 1994. http://www.privacy.org/pi/reports/biometric.htl

EPIC ID Card Resource Page http://www.epic.org/privacy/id_cards/

ABOUT EPIC

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, freedom of expression and constitutional values in the information age. EPIC pursues a wide range of activities, including policy research, public education, conferences, litigation, publications, and advocacy. The Watching the Watchers Project was undertaken by EPIC in 2001 to assess the impact of proposals for public surveillance put forward after September 11.

Question for the Record
Response to the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives

Q. Is the FBI agent on the ground more likely to have actionable intelligence information under the current TTIC arrangement or the proposed NCTC structure?

A. It is our strong belief that the FBI is more likely to have actionable intelligence under the proposed National Counterterrorism Center (NCTC) structure than through the current Terrorist Threat Integration Center.

First, there will be greater fusion of domestic and foreign intelligence across the entire intelligence community in the National Counterterrorism Center that far exceeds the current or planned capabilities of the Terrorist Threat Integration Center. The specific purpose of the NCTC is to overcome the foreign domestic-divide and to enable joint operations planning across the foreign-domestic divide, using actionable intelligence.

Second, FBI agents will be able to submit intelligence requirements through the NCTC, and the Director of the NCTC will have tasking authority across the intelligence community. In short, it is far more likely under the NCTC structure that FBI agents will have their requirements for intelligence met, including actionable intelligence.

Third, intelligence produced by the FBI is far more likely to be disseminated and utilized effectively through a unified NCTC, which will be able to share terrorism intelligence widely and quickly to all USG agencies requiring such intelligence. The current TTIC provides a fused all-source analytic product to senior policymakers, but does not share its all-source analysis – including actionable intelligence – widely. The cop on the beat and the FBI agent on the street will be able to feed their information more quickly to intelligence community analysts, and in turn they will benefit directly and quickly from the actionable intelligence produced by the NCTC.

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 1, 2004

The Honorable Howard Coble
Chairman
Subcommittee on Crime, Terrorism
and Homeland Security
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Enclosed please find responses to questions posed to Mr. John Pistole of the Federal Bureau of Investigation following Mr. Pistole's appearance before the Subcommittee on August 23, 2004. The subject of the Subcommittee's hearing was the recommendations of the 9/11 Commission.

We hope that this information is helpful to you. If we may be of additional assistance, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosures

Responses of the Federal Bureau of Investigation
Based Upon the August 23, 2004 Hearing Before the
House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Regarding the Recommendations of the 9/11 Commission

Questions Posed by the Honorable Bobby Scott

1. How is the FBI doing on diversifying its workforce?

Response:

In Fiscal Year (FY) 2004, the FBI's efforts to recruit a diverse Special Agent (SA) workforce were very successful; the FBI hired 1,203 SAs, of which 19% were minorities and 22% were women. These diversity accomplishments were a direct result of aggressive recruiting and efficient applicant processing. The FBI was also very successful in its recruitment of support employees, hiring approximately 30% minorities and 42% women in FY 2004.

The FBI uses numerous recruitment mechanisms to ensure that FBI employment opportunities are widely known. Among these, which include participation in numerous university programs, job fairs, and community awareness programs, the FBI has developed several initiatives to ensure that minorities are included in these programs. A few examples of these initiatives follow.

- The FBI's Honors Internship Program (HIP) continues to be a successful means of providing exceptional undergraduate and graduate students an insider's view of FBI operations and an opportunity to explore the many career opportunities within the Bureau. The program runs from June to August and is available to full-time undergraduate students between their junior and senior years and to full-time graduate students. Students must have a cumulative grade point average (GPA) of 3.0 or above on a 4.0 scale. In FY 2004, 58 students were selected to participate in the HIP, 43% of whom were minorities and 36% of whom were Caucasian women.

- A contractor, EdVenture Partners, was tasked with developing partnerships and recruitment initiatives with Middle Eastern and African American communities to assist us in identifying qualified applicants on a national level. These partnerships will also improve the FBI's relationships with these communities, which will enhance the FBI's ability to conduct successful investigations.

- In FY 2003, the FBI initiated the FBI/National Association for Equal Opportunity (NAFEO) Critical Skills HIP (NAFEO serves as an umbrella association for 118 historically and predominantly Black colleges and universities (HBCUs)). The FBI/NAFEO Critical Skills HIP fosters a relationship between the FBI and HBCUs, many of which offer particularly high quality educations in engineering, computer science, information technology, physical sciences, and foreign languages. The second class of FBI/NAFEO interns was employed in the summer of 2004 and was comprised of 32 students, including 88% African Americans, 3% Hispanic Americans, and 9% Caucasians. These students were highly skilled, dedicated, and knowledgeable in their areas of concentration.

- To ensure that Native American candidates are aware of FBI employment opportunities, the FBI has partnered with American University's Washington Internships for Native Students (WINS) Program. The WINS program offers American Indian and Alaskan Native students the opportunity to gain quality work experience, to learn firsthand the inner workings of government agencies, and to meet other native students from across the country. Pursuant to this program, American Indian and Alaskan Native students who are enrolled full time in colleges or universities as juniors or seniors and who possess GPAs of at least of 3.0 are eligible to apply for employment as FBI summer interns. While working full time for the FBI in an academically supervised and supported internship, students earn 6 credits for the 10-week summer term. American University provides full academic support for the internship, including additional course work during evenings so students can continue to make academic progress. The WINS program will include colleges and universities on or near Indian Reservations with international studies and language departments this year.

- The FBI formed the Faith-Based Intelligence Community Council as a pilot program in February 2004 in Baltimore, Maryland. This program has provided the FBI with a means of networking and partnering with community leaders such as pastors, the President of the Baltimore Chapter of the National Association for the Advancement of Colored People, and other representatives from Baltimore City and County. This group will enable the FBI to reach qualified candidates in the Baltimore community who would otherwise be inaccessible to us. In addition, the FBI will expand the Faith-Based program to the Washington metropolitan area by partnering with Seacole Diversity Solutions, LLC. This firm will assist the FBI in accomplishing its goal of identifying qualified African American candidates who possess the technical qualifications and skill sets critical to

success as FBI Special Agents.

2. How is the database for "no fly" made up and how over-inclusive is it? What is the procedure for getting off the "no fly" and other watchlists? What is the function of the Ombudsman regarding watchlists, and how well is it working?

Response:

The "no fly" list is a watchlist maintained by the Transportation Security Administration (TSA), Department of Homeland Security. The FBI defers to TSA for this response.

Central Intelligence Agency

Washington, D.C. 20505

26 October 2004

The Honorable Howard Coble
Chairman
Subcommittee on Crime, Terrorism,
and Homeland Security
Committee on the Judiciary
House of Representatives
Washington, DC 20515

Attention: Ms. Emily Newton

Dear Mr. Chairman:

As requested, enclosed is the 23 August 2004 House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security hearing transcript with reviewed comments inserted by the Terrorist Threat Integration Center (TTIC).

Additionally, TTIC's reply to the two provided Questions For the Record are also enclosed.

Should you have any questions, please do not hesitate to call me or have a member of your staff call Gary Dionne of my staff at (703) 482-8794.

Sincerely,

Stanley M. Moskowitz
Director of Congressional Affairs

Enclosures

Questions for Mr. Brennan from The Honorable Bobby Scott

QUESTION 1. Is the FBI agent on the ground more likely to have actionable intelligence information under the current TTIC arrangement or the proposed NCTC structure?

Response: This question is best deferred to the Executive Assistant Director, Office of Intelligence, Federal Bureau of Investigation (FBI). The mission of the FBI's Intelligence Program is to optimally position the FBI to meet current and emerging national security and criminal threats by (1) aiming core investigative work proactively against threats to US interests; (2) building and sustaining enterprise-wide intelligence policies and human and technical capabilities; and (3) providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities.

QUESTION 2. How is the database for "no fly" made up and how over-inclusive is it? What is the procedure for getting off the "no fly" and other watchlists? What is the function of the Ombudsman regarding watchlists, and how well is it working?

Response: Since this question does not deal with TTIC, we defer to the Department of Homeland Security (DHS) for a response. DHS has the statutory responsibility for the operations of the Transportation Administration and its "no fly" program.

○