AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PRIVACY IN THE HANDS OF GOVERNMENT: THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE PRIVACY OFFICER FOR THE U.S. DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 24, 2007

Serial No. 110–142

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

37–007 PDF WASHINGTON : 2008

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

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

LINDA T. SÁNCHEZ, California, *Chairwoman*

JOHN CONYERS, JR., Michigan
HANK JOHNSON, Georgia
ZOE LOFGREN, California
WILLIAM D. DELAHUNT, Massachusetts
MELVIN L. WATT, North Carolina
STEVE COHEN, Tennessee

CHRIS CANNON, Utah
JIM JORDAN, Ohio
RIC KELLER, Florida
TOM FEENEY, Florida
TRENT FRANKS, Arizona

MICHONE JOHNSON, *Chief Counsel*
DANIEL FLORES, *Minority Counsel*

CONTENTS

JULY 24, 2007

OPENING STATEMENT

Page

The Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law 1

The Honorable Chris Cannon, a Representative in Congress from the State of Utah, and Ranking Member, Subcommittee on Commercial and Administrative Law 2

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Member, Subcommittee on Commercial and Administrative Law, and Chairman, Committee on the Judiciary 4

WITNESSES

The Honorable Alan Charles Raul, Esq., Privacy and Civil Liberties Oversight Board, The White House, Washington, DC

Oral Testimony 16

Prepared Statement 18

Lanny J. Davis, Esq., Orrick, Herrington & Sutcliffe, LLP, Washington, DC

Oral Testimony 33

Hugo Teufel III, Esq., U.S. Department of Homeland Security, Washington, DC

Oral Testimony 34

Prepared Statement 36

Ms. Linda Koontz, U.S. Government Accountability Office, Washington, DC

Oral Testimony 54

Prepared Statement 56

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on Commercial and Administrative Law 6

Article from *The Washington Post*, dated November 28, 2006, "Justice Dept. to Examine Its Use of NSA Wiretaps; Review Won't Address Program's Legality," submitted by the Honorable Christopher B. Cannon, a Representative in Congress from the State of Utah, and Ranking Member, Subcommittee on Commercial and Administrative Law 13

Article from Salon.com, dated July 23, 2007, "Bush's torture ban is full of loopholes," submitted by the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Chairman, Committee on the Judiciary, and Member, Subcommittee on Commercial and Administrative Law 94

Page

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Redline version of the Privacy and Civil Liberties Oversight Board, 2007 Report to Congress with edits by The White House, submitted by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law 101
Answers to Post-Hearing Questions posed by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law to the Honorable Alan Charles Raul, Esq., Privacy and Civil Liberties Oversight Board, The White House, Washington, DC 145
Answers to Post-Hearing Questions posed by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law to the Honorable Hugo Teufel III, Esq., U.S. Department of Homeland Security 153
Answers to Post-Hearing Questions posed by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law to Ms. Linda Koontz, U.S. Government Accountability Office 184
Privacy and Civil Liberties Oversight Board, 2007 Report to Congress, submitted by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law 190

PRIVACY IN THE HANDS OF GOVERNMENT: THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE PRIVACY OFFICER FOR THE U.S. DEPARTMENT OF HOMELAND SECURITY

TUESDAY, JULY 24, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCIAL
AND ADMINISTRATIVE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 1:50 p.m., in Room 2237, Rayburn House Office Building, the Honorable Linda Sánchez (Chairwoman of the Subcommittee) presiding.

Present: Representatives Sánchez, Conyers, Watt, Cannon, Feeney, and Franks.

Staff present: Susan Jensen-Lachmann, Majority Counsel; Stewart Jeffries, Minority Counsel; and Adam Russell, Majority Professional Staff Member.

Ms. SÁNCHEZ. This hearing of the Committee on the Judiciary, Subcommittee on Commercial and Administrative Law will now come to order.

And I will now recognize myself for a short opening statement.

Since the September 11 terrorist attacks, Congress has been challenged with protecting individual liberties while working to keep our Nation secure. Unfortunately, and all too often, security and liberty have been seen as competing interests, and in this competition, the right to privacy has tended to be the first victim.

I do not believe that the two are necessarily in conflict. With hard work, we can achieve both goals. In fact, it is imperative to our way of life that we do so.

The Subcommittee on Commercial and Administrative Law has played a major role with respect to protecting personal privacy and civil liberties in this era of heightened government authority over the years. It is with that in mind that the Subcommittee is holding a hearing to review the work and performance of the Privacy and Civil Liberties Oversight Board and the Department of Homeland Security's privacy officer.

As part of our ongoing interest in privacy issues, the Subcommittee has participated in the effort to create the Privacy and Civil Liberties Oversight Board. As we all know, the board was established in 2004 in direct response to the 9/11 Commission's rec-

ommendation that there be an entity within the executive branch to oversee the government's commitment to protecting our privacy and defending our civil liberties.

Recently, there has been increased criticism that the final formulation of the board fell far short of expectations. We hope those issues will be addressed during today's hearing.

The Subcommittee was also instrumental in establishing the first statutorily created privacy office in a Federal agency, namely the Department of Homeland Security, and spearheaded the creation of a privacy office in the Justice Department with similar responsibility.

At this very moment, a Conference Committee tapped with resolving the differences between House and Senate legislation that would substantially increase the powers and responsibilities of both the DHS privacy office and the board has nearly completed its work.

Further, in keeping with our oversight duties, we have conducted several hearings in the past two Congresses as well as requested a GAO study of the DHS privacy office which will be the subject of at least part of today's hearing. Accordingly, the testimony of all of our witnesses is particularly timely.

We are very pleased to have Hugo Teufel, the Department of Homeland Security's current chief privacy officer, with us today, as well as Linda Koontz, director of information management issues on behalf of the GAO, which has recently issued a report on Mr. Teufel's office.

We expect our witnesses, Lanny Davis, a former member of the Privacy and Civil Liberties Oversight Board, and Alan Charles Raul, vice chair of the board, to help enlighten us about the board and how we can improve it.

I want to thank all of the witnesses for coming today and for your patience in terms of the votes that we just had to complete, and I look forward to hearing your testimony.

At this time, I would like to recognize my colleague, Mr. Cannon, the distinguished Ranking Member of the Subcommittee, for his opening remarks.

Mr. CANNON. Thank you, Madam Chair.

Let me begin this hearing, as I have in the past, with an observation written 220 years ago by Alexander Hamilton, one of our founding fathers. In "Federalist No. 8," he wrote, "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates.

"The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger will compel nations most attached to liberty to resort for repose and security to institutions which have a tendency to destroy the civil and political rights. To be more safe, they at length become willing to run the risk of being less free."

Mr. Davis and I were just talking in advance of this hearing about the fact that this is one of those areas where the left and right sort of meet, and we do so because of that principle enunciated by Mr. Hamilton. In this post-9/11 world, it is not an easy task to balance the competing goals of keeping our Nation secure

while at the same time protecting the privacy rights of our Nation's citizens.

When I was Chair of the Subcommittee, the protection of personal information in the hands of the Federal Government was a top priority, and I am proud of our role in protecting personal privacy and civil liberties.

These accomplishments included the establishment of the first statutorily created privacy office in a Federal agency at the Department of Homeland Security and the mandate that the Department of Justice designate a senior official with primary responsibility for privacy policy included in the Department of Justice Reauthorization Act of 2005.

We also held a hearing on the 9/11 Commission's privacy-related recommendations and a hearing on the respective roles that the Federal Government and information resellers have with respect to personal information collected in commercial databases. In the past, the GAO has found that the Federal agencies' compliance with the Privacy Act and other requirements is "uneven."

Today's hearing provides us an opportunity to revisit some of these issues. We will hear from the GAO which has completed a study of the DHS privacy office at my request along with that of former Ranking Member Watt, current Subcommittee Chairman Nadler, and former Constitution Subcommittee Chairman Chabot.

I am pleased that the GAO found that the privacy office has made significant progress in carrying out its statutory responsibilities. Of course, as with any agency, there is always room for improvement. In this case, GAO found that the privacy office could provide its reports in a more timely manner.

I am pleased, however, to see the privacy office has accepted a number of GAO's recommendations, and I look forward to hearing about how they can continue to improve their performance.

Secondly, we will hear from our current and former members of the Privacy and Civil Liberties Board, which was created in response to the 9/11 Commission's report. Recently, the board came out with its first annual report detailing its governmentwide efforts to advise and provide oversight with respect to privacy issues. Unfortunately, this is likely to be the last of such reports.

Currently, the House and Senate are in conference negotiations over a bill that would take the Privacy and Civil Liberties Board out of its current home in the White House and set it up as an independent body in the executive branch with subpoena power.

While an independent board might have its merits, so too does a board that is located in the White House. As it is currently constructed, the board has direct access to high-ranking White House officials as well as the attorney general, the secretary of homeland security and the director of national intelligence. Whether they will continue to have access if they are moved out of the White House is another matter.

Had the majority waited to conduct oversight before legislating this area, the results of that legislation might have been different. As it stands, we are having our first oversight on the board 6 months after the House voted to dismantle it. That strikes me as odd.

I am also pleased that we have a former board member here, Mr. Lanny Davis. As I understand it, Mr. Davis resigned from the board because of what he viewed as an overintrusive White House review process of the board's report. However, I have a copy of the redlined report from *The Washington Post*, and the vast majority of the changes are typographical or stylistic in nature.

In addition, I would note that Mr. Davis signed on the final version of the report, so I look forward to finding out what he thought was so objectionable about it. And knowing Mr. Davis, I am sure it will come to us in the most articulate manner possible.

With that said, I appreciate the Chair's interest in this matter, and I am glad that we will continue to conduct vigorous oversight of privacy in the hands of government.

I thank you, Madam Chair. I yield back.

Ms. SÁNCHEZ. I thank the gentleman.

And I would like to at this time recognize Mr. Conyers, a distinguished Member of the Subcommittee and the Chairman of the Committee on the Judiciary.

Mr. Conyers?

Mr. CONYERS. Thank you, Chairwoman Sánchez.

I am happy to be with you again today, because this Committee, which was Subcommittee number five, turns out to be the most active in the 110th Congress.

I am also glad that Chris Cannon is still on the Committee and is following these issues as carefully as he always has, and, of course, Tom Feeney has become a very active Member of the Committee.

Actually, I had a quotation that started off: More than 200 years ago, Alexander Hamilton warned——

Mr. CANNON. If the gentleman would yield, great minds are on the same track. I hope that ours are on the track that Alexander Hamilton's was on. That would be good.

Mr. CONYERS. Yes. Well, if you include all three great minds, this is a wonderful way to start our hearing.

But it grabbed me the same way you felt compelled to recite it here, Chris Cannon, because this could have been written in the 21st century without changing anything. "To be more safe, they at length become willing to run the risk of being less free."

And that is the balance we find ourselves caught in in this post-9/11 circumstance. But in this environment, I am worried that our liberties have come under attack by our own government, much like Alexander Hamilton feared.

It seems as if each day we learn of a new law enforcement initiative or antiterrorism program challenging our private rights and civil liberties, and it gives this Subcommittee an awesome responsibility in terms of what our jurisdiction is, and I am so pleased that the Chairperson thought that we should do oversight at this point in time.

Much of our victory against those who oppose us will come when we advance the American values on which our Nation was founded. We must serve as a leader in promoting freedom, liberty and democracy. In the eyes of many in the world, this is no longer the case, and so I come here with a concern about warrantless wiretaps and illegal surveillance, and we haven't been able even to find out

the legal rationale, much less brief the Members of this Subcommittee on what we were doing.

The denial of habeus corpus rights to individuals deemed to be enemy combatants: This Subcommittee recently held hearings—no, it was the Constitution Subcommittee—to examine the detention policy of our government, and the findings were troubling.

It is clear that many of the people whom we were told were the worst of the worst have never been evaluated or charged. Individuals who our own government acknowledges are not "terrorists" and are not a threat are nonetheless still held in custody.

The rampant use of profiling, be it ethnic or racial or religious: Passengers have been denied the right to fly on aircraft. Religious institutions have been subjected to FBI surveillance. Justice Department statistics show that routine automobile traffic stops and their outcomes are frequently connected to the race of the driver.

The Guantanamo tragedy: These include the use of what has been euphemistically referred to as harsh interrogation techniques against prisoners detained by the Defense Department, the imprisonment of hundreds of individuals for years at Guantanamo without meaningful due process as to the reasons or the basis for their captivity, restricting these detainees from having meaningful access to counsel.

And these abuses have been mitigated, except that Friday the President of the United States issued an executive order qualifying what our agreement in terms of lightening up on some of these very obvious techniques that violate our treaty obligations and our sense of decency.

We have other issues that we need to talk about. I will leave them to be included in my statement in the record, and I notice the presence of Mr. Lanny Davis, and I think it is very important that he be here for this hearing, and I welcome the other witnesses as well.

And I thank the gentlelady for her indulgence.

[The prepared statement of Mr. Conyers follows:]

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, CHAIRMAN, COMMITTEE ON THE JUDICIARY, AND MEMBER, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

Statement by the Honorable John Conyers, Jr.
for the Hearing on Privacy in the Hands of the Government:
The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security Before the Subcommittee on Commercial and Administrative Law
July 24, 2007

More than 200 years ago, Alexander Hamilton warned:

> "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free."

Unfortunately, in this post-9/11 environment, I fear at times that our liberties have come under attack by our own Government, much like Mr. Hamilton predicted. It seems as if each day we learn of a new law enforcement initiative or anti-terrorism program challenging our privacy rights and civil liberties.

This situation is further complicated by the fact that technological advances – while greatly facilitating the collection and dissemination of personally identifiable information about our citizens – can more readily be accessed by identity thieves.

A real victory in the War on Terror will come only when we advance the American values on which our Nation was founded. The United States must serve as a leader when it comes to promoting freedom, liberty and democracy. Unfortunately, we have fallen short on these fronts.

We are particularly concerned that –

- *Warrant requirements for certain national security wiretaps have been ignored.* We don't know the extent of this illegal surveillance, because this Administration refuses even to share their legal rationale, much less brief the members of this Committee on what they are doing.

- *The denial of habeas corpus rights to individuals deemed to be "enemy combatants."* The Subcommittee on the Constitution, Civil Rights, and Civil Liberties recently held a hearing to examine the Administration's detention policy. The findings were troubling. It is clear that many people, who we were

told were the "worst of the worst," have never been charged, much less evaluated. Individuals who our own government acknowledges are not terrorists and not a threat are nonetheless still being held in custody.

- *The reauthorization of the USA PATRIOT Act in 2006 includes more than 30 new civil liberties protections.* Are these protections being properly implemented by the Justice Department?

- *Federal law enforcement agencies may be using data mining for inappropriate purposes.* The Technology and Privacy Advisory Committee in its 2004 report to the Secretary of Defense made several critical recommendations to ensure that this technology is not being misused. Have any of these recommendations been implemented and, if not, why not?

- *The rampant use of racial profiling.* Passengers have been denied the right to fly on aircraft, religious institutions have been subjected to FBI surveillance, and Justice Department statistics clearly show that routine traffic stops, and their outcomes, are often connected to the race of the driver.

- *The panoply of abuses at Guantanamo.* These include the use of what are euphemistically referred to as "harsh interrogation techniques" against prisoners detained by the Defense Department; the imprisonment of hundreds of individuals for years at Guantanamo without meaningful due process as to the reasons or bases for their captivity; restricting Guantanamo detainees from having meaningful access to counsel. As a result of public pressure, some of these abuses have been mitigated somewhat, but not enough.

- *Allegations that our government is using the Material Witness Statute for unlawful purposes as part of our Nation's antiterrorism efforts.* According to the ACLU and Human Rights Watch, at least 70 men -- all were Muslim except for one -- were arrested using such material witness warrants as part of terrorism investigations after the attacks on September 11, 2001. The Act, enacted in 1984, allows the government to arrest persons who are needed as witnesses in ongoing cases and who it argues might not comply with a conventional subpoena. Of those detained, only 28 people were eventually charged with a crime, according to the Associated Press -- most of them unrelated to terrorism. The ACLU says that the

Justice Department's unlawful use of the Material Witness Statute "is perhaps the most extreme but least well-known of the government's post-September 11 abuses."

- *Repeated instances where federal agencies have lost personal data about our Nation's citizens thereby placing them at risk of being victims of identity theft.* In May 2006, for example, the Department of Veterans Affairs lost an unsecured laptop containing the health records and other sensitive personal information on approximately 26.5 million veterans and their spouses. In April of this year, the Department of Agriculture acknowledged that it posted personally identifiable information for 63,000 grant recipients on its website. And, in May of this year, the Transportation Security Administration reported that personal and financial records of 100,000 of its employees were lost, exposing the Department of Homeland Security to national risks as well as making these employees potential identity theft victims.

The 9/11 Commission, which was established to guide us in the Congress as to how to strengthen our terrorism detection abilities, stressed the need for balance. The Commission

warned that as we protect our homeland, Americans "should be mindful of threats to vital personal and civil liberties" and that this "shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."

In response to the Commission's sage advice, Congress established the Privacy and Civil Liberties Oversight Board in the Executive Office of the President. In addition, Department of Homeland Security Privacy Office, largely at the instigation of the Commercial and Administrative Law Subcommittee, was created in 2004 as the first statutorily-mandated privacy office in the federal government.

Today, we're fortunate to have representatives on behalf of both the Board and the DHS Privacy Office. Accordingly, I very much look forward to hearing how they are safeguarding the privacy and civil liberties of our Nation's citizens.

Ms. SÁNCHEZ. I thank the gentleman for his statement.

Mr. CANNON. Madam Chair, may I ask unanimous consent to include in the record at this point a story from *The Washington Post* dated November 28, 2006, regarding the Department of Justice inspector general announcing an examination of NSA wiretaps? It is an interesting article because it quotes Mr. Davis extensively, and I will leave it for the record, except to say that he was pleasantly surprised.

Just one quote: "I am astonished at the extent to which they are all concerned about the legal and civil liberties and privacy implications of what they are doing," Davis said. And he ties that back to the prior Administration. So this really is an area that does transcend partisan politics.

And so, I would ask unanimous consent that that be included in the record.

Ms. SÁNCHEZ. Without objection, so ordered.

[The article follows:]

The Washington Post

November 28, 2006 Tuesday
Final Edition

Justice Dept. to Examine Its Use of NSA Wiretaps; Review Won't Address Program's Legality

BYLINE: Dan Eggen, Washington Post Staff Writer

SECTION: A Section; A10

LENGTH: 696 words

The Justice Department's inspector general yesterday announced an investigation into the department's connections to the government's controversial warrantless surveillance program, but officials said the probe will not examine whether the National Security Agency is violating the Constitution or federal statutes.

In a letter to House lawmakers, Inspector General Glenn A. Fine said his office decided to open the probe after conducting "initial inquiries" into the program. Under the initiative, the NSA monitors phone calls and e-mails between people in the United States and others overseas without court oversight if one of the targets is suspected of ties to terrorism.

The "program review" will examine how the Justice Department has used information obtained from the NSA program, as well as whether Justice lawyers complied with the "legal requirements" that govern it, according to Fine's letter. Officials said the review will not examine whether the program itself is legal.

The announcement signals a new level of scrutiny for the NSA program, which was launched shortly after the Sept. 11, 2001, attacks and revealed in news reports in December 2005. The program has been ruled unconstitutional by one federal judge, but Bush and other administration officials have strongly defended it as a legal and efficient way to protect the nation from terrorist attacks.

The probe comes amid a dramatically changed political environment. Democrats who have been sharply critical of the surveillance program will soon control the Judiciary and intelligence committees, which oversee Justice and the NSA. Rep. John Conyers Jr. (D-Mich.), the incoming chairman of the House Judiciary Committee, called Fine's investigation "long overdue."

Several other House Democrats said the inquiry should be broadened to include the questions of whether the program violated federal laws and how it was approved. Rep. Maurice D. Hinchey (D-N.Y.) also said he is "skeptical about the timing" of the announcement.

"I wonder whether this reversal is only coming now after the election as an attempt to appease Democrats in Congress who have been critical of the NSA program and will soon be in control and armed with subpoena power," Hinchey said in a news release.

Fine has previously declined requests from lawmakers to conduct a broader probe into the legality of the NSA program, arguing that such an inquiry is beyond his jurisdiction. Those requests were referred to the Justice Department's Office of Professional Responsibility, which was forced to abandon its effort after President Bush refused to grant security clearances to lawyers who needed them.

Fine wrote in his letter to lawmakers yesterday that the White House has promised the security clearances necessary to conduct the new investigation. White House spokeswoman Dana Perino declined to comment.

Justice spokesman Brian Roehrkasse said Fine's review "will assist Justice Department personnel in ensuring that the department's activities comply with the legal requirements that govern operation of the program."

The probe comes as a newly active presidential civil liberties board received its first detailed briefing about the NSA program. The Privacy and Civil Liberties Oversight Board, which was established by Congress and whose five members were appointed by Bush, was provided details about the workings of the NSA program last week.

One member, Lanny J. Davis, a White House lawyer in the Clinton administration, said in an interview that he was "pleasantly surprised" by the privacy protections built into the program. He declined to discuss the program in detail because of secrecy restrictions.

"I was astonished at the extent to which they are all concerned about the legal and civil liberties and privacy implications of what they were doing," **Davis** said. "It was a constant theme of concern, awareness and training way beyond what I expected."

Davis said the briefings convinced him that the program had been carefully constructed from the start. "It was clear that as they thought about it, they put it together in a way that minimized problems to the best extent that they could," he said.

Ms. SÁNCHEZ. And without objection, other Members' opening statements will be included in the record.

Without objection, the Chair will be authorized to declare a recess of the hearing at any point.

I am now pleased to introduce the witnesses for today's hearing.

Our first witness is Hugo Teufel, chief privacy officer of the U.S. Department of Homeland Security. Mr. Teufel was appointed chief privacy officer by Secretary Chertoff on July 23, 2006, and has primary responsibility for privacy policy at the Department of Homeland Security. He also serves as the department's chief Freedom of Information Act officer.

Our second witness is Linda Koontz, who is the director of GAO's information and management issues division. In that capacity, she is responsible for issues regarding the collection, use and dissemination of government information. Ms. Koontz has led GAO's investigations into the government's data-mining activities as well as E-Government Initiatives. She is also board member of the Association for Information and Image Management Standards.

Our third witness is Lanny Davis. Mr. Davis is a partner at the firm of Orrick, Harrington & Sutcliffe, LLP, and advises clients on a wide range of legal and governmental issues. In June 2005, President Bush appointed Mr. Davis to serve on the Privacy and Civil Liberties Oversight Board, and on May 14, 2007, he resigned from the board. Mr. Davis served as special counsel to the President during the Clinton administration.

And our final witness is Alan Charles Raul, vice chairman of the Privacy and Civil Liberties Oversight Board. Appointed by President Bush to the board, Mr. Raul was confirmed by the Senate on February 17 of 2006 and also served in the White House as associate counsel to the President and general counsel to the Office of Management and Budget under President Reagan and as general counsel of the U.S. Department of Agriculture under President George H.W. Bush.

I want to thank you all for your willingness to participate in today's hearing.

Without objection, your written statements will be placed in their entirety into the record, and we would ask that you please limit your oral remarks to 5 minutes.

You will note that we have a lighting system that starts at the beginning of your time with a green light. After 4 minutes, it will turn orange, which is a warning to you that you have 1 minute to wrap up your oral testimony. When the light turns red, that is an indication that your time has expired. If you are mid-sentence, we would ask that you just finish your thought and wrap up your testimony in that way so that each witness will have an opportunity to give their testimony.

After each witness has presented his or her testimony, Subcommittee Members will be permitted to ask questions subject to a 5-minute limit.

Okay. We are going to switch the order of the witnesses, as I am noticing the seating order. So we are actually going to begin with Mr. Raul.

Mr. Raul, will you please begin your testimony?

TESTIMONY OF ALAN CHARLES RAUL, ESQ., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, THE WHITE HOUSE, WASHINGTON, DC

Mr. RAUL. Okay. Thank you, Chairman Sánchez, Ranking Member Cannon, Chairman Conyers, Mr. Feeney, and other Members of the Subcommittee.

On behalf of Chairman Carol Dinkins and members Ted Olson and Frank Taylor, I want to thank you for the opportunity to testify this afternoon regarding the Privacy and Civil Liberties Oversight Board.

The board recently discussed its mission, activities, and accomplishments in its first annual report to Congress issued in April, and it is available on the board's Web site at www.privacyboard.gov.

I appreciate the Subcommittee's interest in the board and its mission.

Before discussing some of the board's activities, accomplishments and plans for the year ahead, I believe it is important to address the legislation currently pending in both Houses of Congress that would dramatically affect the board's future, as Mr. Cannon indicated. It is significant that the pending legislation was passed by both Houses without any hearing or testimony on the subject of the board's operations.

I should note, however, that I would like to correct a statement in my written testimony that no relevant information was requested of the board. There have, in fact, been a number of informal meetings with Members and staff regarding the board's operations during its existence.

In any event, I respectfully submit that Congress would have been well-served to hold formal hearings before adopting significant legislative changes, such as the ones currently proposed and in the conference committee.

While the request for today's testimony did not mention or arise in the context of the pending legislation, I will seek to provide some perspective on this subject. I will also discuss a number of the board's principal activities in the past 16 months, specifically our review of the terrorist surveillance program conducted by the NSA, both before and after the FISA court orders authorizing the program, and the FBI's serious mishandling of that agency's authority to issue national security letters, or NSLs.

While we found the NSA compliance procedures to be highly regimented and well-controlled, we were dismayed at the FBI's lack of adequate compliance procedures to assure that NSLs were issued and used in accordance with legal requirements.

As you know, Congress created the board as part of the Intelligence Reform and Terrorism Prevention Act of 2004, which placed it in the Executive Office of the President. The board's mandate is to provide advice and oversight to help ensure that privacy and civil liberties are appropriately considered in the development and implementation of laws, regulations and policies related to the executive branch's efforts to protect the Nation against terrorists.

The board is, of course, fully aware that both the House of Representatives and the Senate have passed separate legislation that, if enacted in substantially the form of the House bill, would dras-

tically alter the present construct of the board. In fact, whether intended or not, if so enacted, the changes would result in the termination of the present board, elimination of the current staff and closure of the existing office.

The House bill H.R. 1 would establish the board as a new independent entity with subpoena authority. In effect, the House bill would create an institution potentially resembling certain data protection authorities found within the European Union member countries; namely, independent privacy czars that are effectively disconnected from the policymaking and implementing processes in the executive branch and are thus able to second-guess policy without necessarily understanding the consequences or alternatives.

This is potentially unwise for a number of reasons. I believe removing the board from the Executive Office of the President would deprive the board of some of its greatest assets and tools, namely, the access, influence and authority that comes from working directly in the Executive Office for the President. The board has, in fact, benefited from unparalleled access to the relevant policymakers and program managers.

Given the ongoing need for vigilance regarding privacy and civil liberties in the war against terrorism, it would be constitutionally and democratically preferable, in my opinion, for Congress to take the lead in providing fully independent oversight of the executive branch rather than subcontracting out this fundamental role to a free-floating body. Congress's independent oversight of these crucial and delicate national security policy matters should not be delegated to an unaccountable, independent agency.

Turning to the accomplishments during the board's existence and the year ahead, our first annual report to Congress noted in considerable detail what the board has been doing since our first meeting in March of 2006.

We have undertaken a substantive review of existing programs and policies, including the NSA surveillance program, Terrorist Finance Tracking Program, the Department of Defense's Counterintelligence Field Activities and other programs, including the Watch List Memorandum of Understanding regarding the traveler redress program for individuals who find that they are on the no-fly or selectee list, and we have been integrated into the implementation and drafting of the information-sharing guidelines.

With that, my time is up, and I will look forward to answering any questions that the Committee may have.

[The prepared statement of Mr. Raul follows:]

PREPARED STATEMENT OF ALAN CHARLES RAUL, ESQ.

Testimony of Alan Charles Raul
Vice Chairman, Privacy and Civil Liberties Oversight Board
Before the House Judiciary Subcommittee on Commercial and Administrative Law
July 24, 2007

Chairman Sanchez, Ranking Member Cannon and Members of the Subcommittee:

On behalf of Chairman Carol Dinkins and Members Ted Olson and Frank Taylor, I want to thank you for the opportunity to testify this afternoon regarding the Privacy and Civil Liberties Oversight Board. The Board recently discussed its mission, activities and accomplishments in its first Annual Report to Congress, issued in April and available on the Board's website at www.privacyboard.gov. I appreciate the Subcommittee's interest in the Board and its mission.

Before discussing some of the Board's activities, accomplishments and plans for the year ahead, I believe it is important to address certain structural issues that are relevant to legislation currently pending in both Houses of Congress that would dramatically affect the Board's future. It is significant that the pending legislation was passed by both Houses without any hearing or testimony on the subject of the Board's operations, or any relevant information having been requested of the Board. I respectfully submit that Congress would have been well served to hear from the Board before adopting possible legislative changes. Accordingly, while the request for today's testimony did not mention or arise in the context of the pending legislation, I will seek to provide some perspective on this subject. I will conclude with some suggestions I would recommend for strengthening the role of the current Board.

I. Background on the Board

As you know, Congress created the Board as part of the Intelligence Reform and Terrorism Prevention Act of 2004, which placed it in the Executive Office of the President. Among other things, the Intelligence Reform Act implemented the recommendations of the 9/11 Commission. In its report, the Commission acknowledged that many of its recommendations "call[ed] for the government to increase its presence in our lives – for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies." THE 9/11 COMMISSION REPORT, 393-94 (2004). However, the Commission also noted that "[t]he choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home." *Id.* at 395. Consequently, the Commission also recommended the creation of "a board within the Executive Branch to oversee . . . the commitment the government makes to defend our civil liberties." *Id.*

The President appointed the five Members of the Board, and Chairman Dinkins and I were confirmed by the Senate. Congress appropriated funds for the Board directly to the White House Office, rather than to the Board as a separate entity within the Executive Office of the President.

The Board's mandate is to provide advice and oversight to help ensure that privacy and civil liberties are appropriately considered in the development and implementation of laws, regulations, and policies related to the Executive Branch's efforts to protect the Nation against terrorism. In carrying out this mandate, the Board has two primary tasks. *First*, it must "*advise* the President and the head of any department or agency of the Executive Branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation," *id.* § 1061(c)(1)(C) (emphasis added), of "laws, regulations, and executive branch policies related to efforts to protect the Nation from terrorism." *Id.* § 1061(c)(1)(B). *Second*, it must exercise *oversight* by "continually review[ing] regulations, executive branch policies, and procedures . . . and other actions by the executive branch related to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected." *Id.* § 1061(c)(2)(A). The statute also expressly requires the Board to advise and oversee the creation and implementation of the Information Sharing Environment (ISE). *Id.* §§ 1061(c)(2)(B), (d)(2).

As shown in the Board's location, assigned roles, and authority, IRTPA did not create an independent watchdog entity in the nature of an inspector general. Rather, the statute created a Board that operates *within* the Executive Office of the President and ultimately reports *to* the President. The statute requires the Board to produce an annual report to Congress "on [its] major activities" – not on all of its internal deliberations and recommendations. *Id.* § 1061(c)(4). The statute expressly places the Board within the Executive Office of the President (EOP), an office whose sole purpose is to support the Executive. Consistent with that placement and with the goal of offering candid advice, the President has located the Board even more closely to him by placing it within the White House Office (WHO). Congress acknowledged this placement by earmarking certain WHO appropriated funds for Board use rather than appropriating funds to a specific EOP entity. As the statute explicitly acknowledges, all five Board Members (like other EOP and WHO employees) serve at the pleasure of the President. *Id.* § 1061(e)(1)(E). By empowering the Board with broad access to records, IRTPA has created a Board that can offer a distinctly independent perspective to the President, along with oversight of Executive agencies.

The Board acts in concert with a robust and developing privacy and civil liberties (PCL) infrastructure that is already operating throughout every major anti-terrorism agency, including the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Office of the Director of National Intelligence (ODNI). In most cases, these PCL offices are headed by officials with direct access to their agency heads. They are primarily staffed by diligent career civil servants who focus on and provide an additional degree of continuity regarding the appropriate consideration of privacy and civil liberties. As discussed below, the Board intends to provide a coordinating role for these PCL offices and will also assist in addressing unique problems that require government-wide coordination or specific White House involvement.

II. Pending Legislation

As I mentioned earlier, the Board is of course fully aware that both the House of Representatives and the Senate have passed separate legislation that if enacted in substantially the form of the House bill would drastically alter the present construct of the Board. In fact, whether intended or not, if so enacted, the changes would result in the termination of the present

Board, elimination of the current staff, and closure of the existing office. At the very least, this would be highly inefficient and would require lengthy new selection, confirmation and security clearance processes that would leave the Executive Branch without any privacy board for perhaps the duration of the current Administration.

The Senate bill, S.4, leaves the Board within the Executive Office of the President, but requires that the position of chairman be full time. It requires Senate confirmation to be staggered with six year terms for all Members.

The House bill, H.R. 1, would impose the same appointment restrictions, but would also establish the Board as a new independent entity with subpoena authority. In effect, the House bill would create an institution potentially resembling certain data protection authorities found within European Union member Countries: namely, independent privacy czars that are effectively disconnected from the policymaking and implementing process in the Executive Branch, and are thus able to second guess policy without understanding the consequences and/or alternatives.

This is potentially unwise for a number of reasons. First, it should be recognized that the 9/11 Commission itself did not recommend creating an independent agency; rather, the Commission's Report said "there should be a board within the executive branch to oversee adherence to the [counterterrorism] guidelines . . . we recommended and the commitment the government makes to defend our civil liberties." Thus, in the Intelligence Reform Act, Congress expressly placed the Board in the Executive Office of the President, and stipulated that the Board "shall perform its functions within the executive branch and under the general supervision of the President." Second, removing the Board from the Executive Office of the President would deprive the Board of some of its greatest assets and tools, namely the access, influence and authority that comes from working directly in the Executive Office of the President. The Board has in fact benefited from unparalleled access to the relevant policy makers and program managers. Third, an independent agency may not be operational before the end of the present Administration, and the learning curve for its members will be significant.

An independent agency – designed to operate like an Inspector General – will inevitably experience a different level of access than the current Board has enjoyed. But most importantly, an independent agency may not be brought into sensitive programs before, or even *while*, they are being developed and executed. To the contrary, it would be more realistic to expect that an independent agency will be engaged after the fact – that is, once programs have been fully implemented programs. Of course, an independent agency, no matter how well intentioned or how distinguished its members, will not have the access or clout of Congress itself to judge whether programs have been devised and conducted in a satisfactory manner. Thus, a new independent agency will not be able to (and should not) perform Congress' oversight function, and will also not be able to operate as an influential adviser of the Executive Branch.

The provisions of the legislation requiring all five Members to be confirmed by the Senate also produce what may be an unintended consequence. By applying the Freedom of Information Act (FOIA) *and* requiring confirmation of all five Members, the Board would have to meet publicly unless it satisfied logistical procedures of the Sunshine in Government Act. 5 U.S.C. § 552b. Inhibiting the agency from meeting together frequently and informally would not

be desirable. The better approach, we believe, is to stay with the current structure, with the Chairman and Vice Chairman subject to Senate confirmation. If the current Board remains in place, we are fully committed to holding public sessions throughout the coming year and inviting public comments and concerns regarding relevant government policies. We held our first public hearing last December, which we thought was very successful in stimulating debate.

Indeed, I question whether Congress is well served to establish an independent review agency that would tend to supplant or duplicate Congress' own role – but with less authority to do so effectively. Congress should not create an agency that would be free to criticize the Administration (presumably the next one, given how long it will take to start up a new Board) on the most sensitive national security matters, but without any accountability. If the independent agency does not work for and report to the President, then the Executive Branch would not be responsible or accountable for the new agency. If the independent agency were not an arm of Congress, then the new agency would be free to question the counterterrorism, privacy and civil liberties judgments of the Executive Branch without any accountability to either Branch. This is not the type of system of checks and balances that the Constitution envisions. Freestanding commissions are useful for conducting particular investigations (e.g., 9/11 Commission, WMD Commission, etc.), or addressing discrete issues (e.g., Social Security, Budget, etc.), with a finite lifespan and defined work product. However, with respect to the ongoing need for vigilance regarding privacy and civil liberties in the war against terrorism, it would be constitutionally and democratically preferable, in my opinion, for Congress to take the lead in providing fully independent oversight of the Executive Branch rather than to sub-contract out this fundamental role to a free-floating body.

In short, Congress' independent oversight of these crucial – and delicate – national security policy matters should not be delegated to an unaccountable, independent agency.

III. Accomplishments and the Year Ahead

As our first annual report to Congress notes in considerable detail, the present Board has accomplished a great deal since its first meeting in March, 2006. We have established the means and infrastructure necessary to support our statutory mission. We have engaged in discussion with policy officials and experts both within the government and in the private, academic and non-profit sectors. Finally, we have undertaken a substantive review of existing programs and policies. For example, the Board has evaluated, among others, National Security Agency surveillance programs, the Treasury Department's Terrorist Finance Tracking Program, the Department of Defense's Counterintelligence Field Activities Threat and Local Observation Notices program, the State Department's e-Passport initiative, and the National Counterterrorism Center's National Implementation Plan. It has helped coordinate the drafting and inter-agency approval of a Memorandum of Understanding to standardize and improve procedures for obtaining redress for watch list grievances. The Board has also been integrated into the drafting and implementation of the Information Sharing Environment guidelines. Significantly, the Board has also delved deeply into the FBI's use of National Security Letters. We issued a highly critical preliminary assessment, in conjunction with the Board's annual report, in which we set forth the Board's concerns about the Bureau's lack of compliance with legal requirements in using NSLs.

A. Establishing Necessary Infrastructure

In carrying out its substantive statutory mandates, the Board has formally met thirty-five times since March 2006. All meetings took place in or around Washington, DC – within the White House complex, at various departments and agencies, and one meeting at Georgetown University. To place the activity of the Board's part-time membership in perspective, the Board has formally met an average of about once every two weeks. Members always remain in near-constant communication with each other and the staff through e-mail and telephone. In the first few months of operation, the Board adopted a number of formative procedures and policies, including issue prioritization, everyday operations, public communications, and analytical methodologies.

As an initial matter, the Board adopted its first annual agenda. The agenda functioned as a business plan by allocating responsibility for tasks among staff and setting expectations regarding how the Board would function. It also served as a substantive agenda by laying out an initial list of issues on which the Board agreed to focus its energies. As part of a comprehensive communications plan, the Board approved the creation of a web site – www.privacyboard.gov – to discuss the Board's history, mission, and activities and provide the public access to Board Member biographies, Board statements, and other related documents. The web site also serves as a means by which the public may contact the Board.

The Board also developed a series of preliminary processes, procedures, and methods by which it could fulfill its advice and oversight responsibilities to the President and Executive Branch agency heads. Of greatest importance, it agreed upon a methodology for analyzing and evaluating proposed programs. It established both a regular means for Board staff to report their activities to the Members and a means of discussing issues and offering possible actions for the Board to take.

In construing the mandate contained in IRTPA, the Board has initially determined that it will focus its efforts on issues concerning U.S. Persons or occurring on American soil. A "U.S. person" is defined, *inter alia*, as a United States citizen and a lawful permanent resident alien. *See, e.g.,* 50 U.S.C. § 1801(i); Executive Order 12333 § 3.4(i). As a result, it will not evaluate specific issues associated with the uniformed services' efforts against terrorism or activities directed against non-U.S. persons abroad. IRTPA instructs the Board to ensure the consideration and protection of "privacy and civil liberties" but neither defines this phrase nor guides the Board in determining whose privacy and civil liberties should warrant the Board's attention. In order to maximize the Board's effectiveness and to prevent the diffusion of its limited resources across too many programs, the Board has elected to concentrate on the United States and U.S. Persons. The Board reserves the right to revisit this determination as circumstances or events may warrant.

In addition to determining the general reach of its mandate, the Board established a standardized means to evaluate how well privacy and civil liberties have been considered in the development and implementation of anti-terrorism policies and programs. To that end, the Board has developed an "issues and process analysis methodology" that will bring full and consistent consideration of all issues that come before it. This methodology allows the Board to

consider separate substantive questions and the extent to which privacy and civil liberty officers within the relevant agency have meaningfully participated in the development and implementation of the policy or program. The Board wishes to acknowledge and thank Jim Harper, Director of Information Policy Studies at the Cato Institute, and the Department of Homeland Security Data Privacy and Integrity Advisory Committee, on which Mr. Harper sits, for their guidance and earlier work product, upon which much of this is based. The methodology takes into account five large issues, as well as a number of subsidiary questions. The larger questions include: The scope of the program; the program's legal basis; how the program supports efforts to protect the Nation against terrorism from the perspective of managing risk to privacy or to survival; the extent to which officials within the relevant department or agency analyzed the privacy and civil liberties interests implicated by the policy, program or issue; and processes employed by the government to review privacy and civil liberties interests.

B. Engaging Policymakers and Interested Parties

In order to obtain the most complete, real-time access to information regarding proposed and operational anti-terror programs, the Board agreed that it must establish trust and credibility between itself and the relevant members of the Executive Branch. To that end, the Board has developed a sound, regular, and productive working relationship with the President's most senior advisors tasked with anti-terrorism responsibilities. This relationship has put the Board in a position to integrate itself into the policymaking process and obtain the necessary support from the Administration to offer meaningful advice.

The Board has met personally with numerous principal senior White House officials, including: the current and previous Chiefs of Staff; the National Security Advisor; the Homeland Security and Counterterrorism Advisor; current and previous Counsel to the President; Staff Secretary; Chairman of the Intelligence Oversight Board and a member of the President's Foreign Intelligence Advisory Board.

These meetings have allowed the Board to forge strong working relationships with agencies within the Executive Office of the President, including the National Security Council, Homeland Security Council, Office of Management and Budget, Office of the Counsel to the President, and the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board, among others. Additionally, the Board's professional staff meets weekly with an EOP working group which consists of commissioned officer representatives from the Office of the White House Chief of Staff, the National Security Council, the Homeland Security Council, the Office of the Counsel to the President, the Office of Legislative Affairs, the Office of Communications, and the Office of Management and Budget.

The Board has also met with senior administration officials throughout the Executive Branch who have responsibilities for developing and implementing war-on-terrorism policies and strategies. These officials include: the Attorney General, Deputy Attorney General, Assistant Attorney General for Legal Policy, Assistant Attorney General for National Security, and Acting-Assistant Attorney General for Legal Counsel; FBI Director; Secretary for Homeland Security; Department of the Treasury Under Secretary for Terrorism and Financial Intelligence Stuart Levey, as well as the Assistant Secretary for Intelligence and Analysis; the current and

previous Director of National Intelligence, the previous Deputy DNI, the ODNI General Counsel, and Information Sharing Environment (ISE) Program Manager; Director and senior supporting staff of the National Security Agency; and Director and senior staff of the Director of the National Counterterrorism Center.

The Board and its staff have made repeated visits to a number of government facilities to observe how those agencies operate, develop anti-terror policies, and train their employees to protect privacy and civil liberties. On-site visits also tend to promote a high-quality dialogue between Board Members and advisors. Consequently, the Board has personally visited the Department of Justice, the Department of Homeland Security, the National Security Agency, the National Counterterrorism Center, the Terrorist Screening Center, the Federal Bureau of Investigation, and the Department of Defense Counterintelligence Field Activity Office.

Perhaps most importantly, the Board has established strong working relationships with the developing privacy and civil liberties offices within the government's anti-terror agencies. These offices and officers advance privacy and civil liberties at the ground level and generally have the greatest practical impact on the development and implementation of policies within their respective agencies. The privacy and civil liberties offices with which the Board works most closely include those at the Department of Justice, the Department of Homeland Security, and the Office of the Director of National Intelligence. These officials have likewise developed lines of communication and authority within their organizations' structure. These relationships allow the Board to encourage the sharing of information and best practices among those offices. The relationships have also allowed the Board to coordinate and offer assistance when the privacy or civil liberties officers encounter problems. The Board has helped and will continue to help coordinate and foster the development of a privacy and civil liberties infrastructure throughout the Executive Branch.

Board Members have also reached out to Senators and Representatives to brief them on the Board's mission, priorities, and activities, as appropriate. The Chairman and Vice Chairman have responded to all Congressional requests for testimony. The Board has also authorized its Executive Director to ensure that appropriate lines of communication and information exist between it and Congress.

The Board has set as a high priority engaging in a productive and ongoing dialogue with privacy, non-profit, and academic organizations within the privacy and civil liberties community. These conversations have helped identify issues important to the community, exchange ideas regarding how to craft anti-terrorism policies and procedures, and establish trust between the Board and the community. For example, the Board has strived to communicate regularly with the co-chairs of the 9/11 Commission, Governor Thomas Kean and Congressman Lee Hamilton. Chairman Dinkins and I met collectively with Governor Kean and Congressman Hamilton and apprised them of the Board's major activities. They have also held individual telephone conferences with Governor Kean and Congressman Hamilton. Following the December telephone conference, Congressman Hamilton requested the Board's executive director to contact him every 60 days with additional updates on the Board's efforts. In addition, the Board's executive director has met with then-State Department Counselor and former Commission executive director Philip D. Zelikow and Commission General Counsel Daniel

Marcus. The Board is dedicated to meeting the letter and spirit of the 9/11 Commission's recommendations, consistent with its statutory authority, and looks forward to continued contact with the Commission's co-chairs.

Additionally, the Chairman and Vice Chairman met with representatives from the American Civil Liberties Union and the Center for Democracy and Technology within the first two months of the Board's operation. The Board also has held meetings with: the American Conservative Union; the Center for Strategic and International Studies; the Electronic Privacy Information Center and the Privacy Coalition; the Markle Foundation; Cato Institute; the Heritage Foundation; the Liberty Coalition; and the National Institute of Standards and Technology. Board representatives have appeared at the Progress and Freedom Foundation's Annual Aspen Summit, the U.S. Army Judge Advocate General's School Advanced Intelligence Law Conference, and the Intelink and the Information Sharing Conference and Technology Exposition.

C. Reviewing Critical National Security Programs and Policies

The Board has begun its efforts to review some of the Federal government's most sensitive and far-reaching surveillance programs. As discussed below in greater detail, these programs include National Security Agency surveillance programs (such as the former Terrorist Surveillance Program (TSP) and the current program governed by the Foreign Intelligence Surveillance Court) and the Terrorist Finance Tracking Program (TFTP). The Board also conducted a review of the National Implementation Plan (NIP).

In each briefing, Board members were free to engage in a probing inquiry and ask unfettered questions, all of which were answered. Following each briefing, the Board met to consider further areas of inquiry, additional issues associated with these specific programs, and underlying documents to review.

i. Anti-Terrorist Surveillance

The Board devoted substantial time and focus in its first year of operation to reviewing anti-terrorist surveillance conducted by the National Security Agency (NSA) and the Terrorist Surveillance Program (TSP) described by the President on December 17, 2005. The TSP involved surveillance of communications where one party to the communication is outside the United States and the government has probable cause to believe that at least one party to the communication is a member or agent of al Qaeda, or an affiliated terrorist organization.

The Board's review of the NSA's surveillance activities was conducted in the course of various briefings by senior NSA personnel, including the Director, and through briefings, questioning, and other interaction with analysts and program operators. Board members repeatedly visited NSA and observed the physical operations where the relevant surveillance is conducted. In particular, the Board reviewed material supporting the government's determination that there was probable cause to believe that at least one of the parties to a surveilled communication was a member or agent of al Qaeda, or an associated terrorist organization.

The Board also received briefings and had opportunities to question NSA lawyers from the Office of General Counsel, Inspector General officials, and other knowledgeable personnel. The Board discussed TSP with the Attorney General, the Acting Assistant Attorney General for the Office of Legal Counsel, and the current and former Counsel to the President, among other knowledgeable officials in the Executive Branch.

The Board was briefed on the multiple levels of review, approval and oversight for conducting this surveillance. At the NSA, operators must carefully justify tasking requests, and multiple levels of review and approval are required to initiate collection. Ongoing audits and legal reviews are conducted by the NSA's Office of Inspector General, General Counsel and Signals Intelligence Directorate Office of Oversight and Compliance. No surveillance may be conducted without leaving a reviewable audit trail that can be and routinely is subject to extensive continuing examination by Inspector General and Compliance staff.

In addition, the members of the Board reviewed U.S. Signals Intelligence Directive 18 (USSID 18), which reflects the classified guidelines established by the NSA and approved by the Attorney General pursuant to Executive Order 12333 to ensure that information about U.S. Persons is protected from improper or excessive collection, dissemination and distribution. The NSA requires all of its personnel holding security clearances authorizing access to certain information to participate in extensive USSID 18 training upon the initiation of access and every two years during which they continue to have access. The Vice Chairman and Executive Director participated in the full USSID 18 training received by NSA personnel in order to examine the extent and quality of the training, and to assess awareness of the need to protect the privacy and civil liberties interests of U.S. Persons among NSA personnel with access to sensitive information.

On January 17, 2007, the Attorney General notified Senators Leahy and Specter that a Judge of the Foreign Intelligence Surveillance Court (FISC) had issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (FISC Orders). As a result of the FISC Orders, any electronic surveillance that was conducted under the TSP is now conducted subject to the approval of the FISC. After the FISC Orders were issued, the Board was extensively briefed by both the Department of Justice and NSA regarding this development. Members of the Board also have studied the classified FISC Orders themselves and closely reviewed the classified material submitted to the FISC in connection with the Orders, including the applications, legal memoranda, and supporting declarations.

While the details of the FISC Orders remain classified, we can report in an unclassified format that as a result of the Orders the relevant surveillance is now subject both to extensive ongoing Department of Justice review and to the approval of the FISA Court. The Department of Justice's responsibilities for implementing the Orders are carried out by the new National Security Division in the Department of Justice headed by Assistant Attorney General Kenneth Wainstein, who has briefed the Board.

Based upon its review, the Board has concluded that the Executive Branch's conduct of these surveillance activities appropriately considers and reasonably protects the privacy and civil liberties of U.S. Persons. As a result of the new FISA Court Orders, the highly regimented Executive Branch process of justification, review, approval, and auditing has been further augmented by court supervision. This provides reasonable assurance that national security and privacy and civil liberties interests are appropriately balanced. The Board found no evidence or reasonable basis to believe that the privacy and civil liberties of U.S. Persons are improperly threatened or impinged under the surveillance conducted by the Executive Branch, either under the TSP or subsequently under the new FISC Orders. In the opinion of the Board, it appears that the officials and personnel who were involved in conducting the TSP, and who now are responsible for implementing surveillance under the FISC Orders, are significantly aware and respectful of U.S. Constitutional and legal rights and protections for U.S. Persons, and that they are actively committed to protecting privacy and civil liberties of U.S. Persons in conducting such surveillance.

The Board notes that it was not involved in and has taken no position on the original design or legal authorization of the TSP. The Board believes that it is appropriate for it to provide continuing advice and oversight with respect to NSA's surveillance activities.

ii. National Implementation Plan

The National Implementation Plan was approved by the President in June, 2006, and is intended to coordinate and integrate all instruments of national power in a unified effort to protect the Nation against terrorism. Toward that end, it assigns hundreds of specific tasks to various Federal departments and agencies. Participating departments and agencies are now adopting and implementing their own supporting plans, and an annual strategic review of the entire NIP is in progress. The Board has reviewed the entire NIP and has had the opportunity to direct additional questions to the appropriate White House and Intelligence Community officials. The Board is also working with the National Counterterrorism Center to ensure that it has access to NIP tasks and activities that could raise privacy or civil liberties concerns.

iii. Terrorist Finance Tracking Program

Additionally, the Board was briefed on the Terrorist Finance Tracking Program (TFTP) by the Treasury Under Secretary for Terrorism and Financial Intelligence and Assistant Secretary for Intelligence and Analysis. Under this program, intelligence analysts review records acquired through administrative subpoenas from the Society for Worldwide Interbank Financial Telecommunication to locate financial connections to known or suspected terrorists. This program also predates the Board's existence.

The Board has also examined or begun to examine privacy concerns connected to other programs and issues, including CIFA TALON, the Department of State E-Passport Program, Passenger Name Recognition data, US-VISIT, and the reauthorized PATRIOT Act. Comments regarding these programs are located on pages 30-32 of the Board's 2007 Report to Congress.

D. Becoming Involved in Policy Development and Implementation

i. Watchlist Redress

At the request of the Board, I have undertaken the coordination of efforts among the various relevant Federal departments and agencies to establish a formalized, unified, and simplified redress procedure for individuals with adverse experiences with the government's watch list or during screening processes. Both government officials and non-governmental advocacy experts repeatedly raised this issue as an area where the Board could bring focus, organization and prioritization.

The Terrorist Screening Center (TSC) is charged with maintaining the U.S. government's consolidated terrorist watch list, which contains the identifying information of all known or appropriately suspected terrorists. Thirteen months after the Center began operations, it established a formal watch list redress process. The process allowed agencies that used the consolidated terrorist watch list data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appeared those complaints were watch list related. The goal of the redress process is to provide timely and fair review of individuals' complaints, and to identify and correct any data errors, including errors in the terrorist watch list itself.

TSC's redress process consists of a procedure to receive, track, and research watch list-related complaints and to correct the watch list or other data that caused an individual unwarranted hardship or difficulty during a screening process. Throughout 2005, TSC worked closely with screening agencies to establish a standardized process for referral of and response to public redress complaints. In the fall of 2005, TSC undertook to document formally the participating agencies' mutual understanding of their obligations and responsibilities arising out of the watch list redress process. Competing priorities within participating agencies, however, slowed progress.

On June 20, 2006, I convened a meeting of all relevant agencies and called for a renewed effort to prioritize this project. In attendance were representatives from TSC, the Departments of State, Defense, Treasury, Justice, and Homeland Security, the Office of the Director of National Intelligence, the FBI, the CIA and the National Counterterrorism Center. The resulting draft Memorandum of Understanding (MOU) is a constructive and positive step intended to secure a commitment from these agencies that participate in the watch list process actively to engage in and support the redress process. The MOU resulted from a six-month period of negotiations between the agencies mentioned previously. I convened a final working group meeting on November 30, 2006; in January 2007, a final draft of the MOU was approved and submitted for the signature of the heads of these agencies.

The MOU sets forth the existing multi-agency redress process in significant detail, from receipt of an individual's complaint to the response sent by the screening agency. Among other things, the MOU establishes obligations for all parties to secure personal information, update and correct their own record systems, and share information to ensure redress complaints are resolved appropriately. Each participating agency must also commit to providing appropriate staff and other resources to make sure the redress process functions in a timely and efficient

manner. Finally, each agency must designate a senior official that is responsible for ensuring the agency's full participation in the redress process and overall compliance with the MOU. Once the MOU has been executed and implemented, the Board intends to continue efforts to bring all possible transparency and public understanding to this process.

ii. Information Sharing Environment

Pursuant to IRTPA, the Board has also participated in the drafting of elements of the Information Sharing Environment (ISE). The ISE is an approach that facilitates the sharing of information relating to terrorism by putting in place the processes, protocols, and technology that enable the sharing of this information among Federal, State, local, tribal and private sector entities, and foreign partners. The ISE brings together, aligns and builds upon existing information sharing policies, business processes and technologies (systems), and promotes a culture of information sharing through increased collaboration. IRTPA also established the Program Manager for the Information Sharing Environment with government-wide authority to plan, oversee, and manage the ISE. The Program Manager assists the President and government agencies in the development and operation of the ISE and monitors and assesses its progress.

To guide efforts to establish the ISE and implement the requirements of IRTPA, on December 16, 2005, President Bush issued a Memorandum to the Heads of Executive Departments and Agencies. This Memorandum delineated two requirements and five guidelines which prioritize efforts that the President believes are most critical to the development of the ISE and assigns Cabinet officials responsibility for resolving some of the more complicated issues associated with information sharing. The five guidelines are: (1) Set Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE; (2) Create Common Framework for Sharing Information Between and Among Federal Agencies and State, Local and Tribal Governments, Law Enforcements Agencies and the Private Sector; (3) Standardize Procedures for Sensitive But Unclassified Information; (4) Facilitate Information Sharing with Foreign Partners; and (5) Protect the Information Privacy Rights and Other Legal Rights of Americans.

IRTPA required that these guidelines be drafted and implemented in consultation with the Board. With regard to all five sets of guidelines, the Board's Executive Director is a member of the White House Information Sharing Policy Coordination Committee which sits above all the working groups and directly below the Deputies and Principals Committees.

The ISE Privacy Guidelines are based on a set of core principles that requires agencies to: identify any privacy-protected information to be shared; enable other agencies to determine the nature of the information and whether it contains information about U.S. Persons; assess and document applicable legal and policy rules and restrictions; put in place accountability and audit mechanisms; implement data quality and, where appropriate, redress procedures; and identify an ISE Privacy Official to ensure compliance with the guidelines.

The ISE Privacy Guidelines also provide for an ISE Privacy Guidelines Committee, consisting of the ISE Privacy Officials of the departments and agencies comprising the Information Sharing

Council (ISC), and chaired by a senior official designated by the Program Manager. Working closely with the Privacy and Civil Liberties Oversight Board as it exercises its oversight mission, the committee will seek to ensure consistency and standardization in implementation, as well as serve as a forum to share best practices and resolve inter-agency issues. The Program Manager has designated Alex Joel and Jane Horvath to serve as co-chairs of this ISE Privacy Guidelines Committee, which will include the Board's Executive Director as a member. The Board instructed its staff to meet with the Program Manager and provide options concerning its on-going oversight role and how that role can be most effectively and efficiently exercised.

E. Examining National Security Letters

Recently, the Board began a substantive review of the FBI's use of National Security Letters. The Board chose to undertake this review at the invitation of the Attorney General and immediately prior to the release of the Department of Justice Inspector General's report on this subject. *See A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Report of the Inspector General (March 2007). The report described a number of troubling deficiencies in the use and management of NSLs and NSL-derived information. Such deficiencies included issuing letters without complying with appropriate statutory and internal regulations, failing adequately to document and track information provided in response to NSLs, and issuing "exigent letters" that contained inaccurate information. The Board and its staff have met with the Inspector General, the Director of the FBI and other senior officials, senior DOJ officials within the National Security Division, and representatives from privacy advocacy organizations. The Board has asked follow-up questions of those officials and has reviewed Bureau guidance and internal memoranda regarding possible corrective actions. The Board will shortly deliver recommendations regarding this program to the Attorney General.

This project is a good example of the value the present Board brings to promoting consideration of privacy and civil liberties. Prior to the release of the Inspector General's report, the Attorney General invited Board review of FBI procedures. The Board had full access to all individuals and materials needed for a comprehensive review. Our discussions, observations, and suggestions along the way have been incorporated into the FBI and DOJ remedial actions. We believe that DOJ and FBI officials take our mission seriously and will fully consider the findings and recommendations of our final report.

F. Planning the Year Ahead

The Board has laid out an ambitious and aggressive agenda for the year ahead, building on our organizational and educational efforts of the past year. As required by statute, we will stay involved in the development of the Information Sharing Environment. We are continuing to look into government surveillance operations and terrorist watch list redress issues. Other areas of interest include:

- *USA PATRIOT Act and National Security Letters (NSLs)*. The 2006 reauthorization included over thirty new civil liberties protections. The Board will work with the Department of Justice to monitor implementation of these protections.

- *Federal data analysis and management issues.* Board Members intend to enhance significantly their understanding of issues associated with data mining activities, data sharing practices, and governmental use of commercial databases. This level of understanding will assist the Board in its review of many Federal anti-terrorism programs. Toward this end, the Board will follow up on recommendations of the March, 2004 report of the Technology and Privacy Advisory Committee (TAPAC) to the Secretary of Defense, *Safeguarding Privacy in the Fight Against Terrorism.*

- *U.S. Persons Guidelines.* These guidelines limit the government's ability to collect, retain, and distribute intelligence information regarding U.S. Persons. These guidelines are applicable to agencies in the intelligence community pursuant to Executive Orders 12333 and 13284. As was noted in the 2005 report to the President on Weapons of Mass Destruction, these rules are complicated, subject to varying interpretations, and substantially different from one agency to another. The Attorney General and the Director of National Intelligence have established a staff level working group to review these guidelines and propose appropriate reforms. The Board intends to participate in this process.

- *State and local fusion centers.* State and local law enforcement entities are establishing joint centers where they share information and data of value to their common missions. Federal agencies are developing partnerships with these centers. The Board will review these sharing practices to ensure that privacy rights and civil liberties concerns are taken into appropriate consideration.

- *National Implementation Plan.* The Board will continue to monitor those tasks and activities that might raise privacy or civil liberties concerns.

- *Department of Homeland Security Automated Targeting System (ATS).* ATS is a decision support tool used by Customs and Border Protection to assist in making a threshold assessment in advance of arrival into the U.S. based on information that DHS would otherwise collect at the point of entry. The Board intends to review this system.

- *Material Witness Statute.* As a result of concerns raised at its December 5, 2006 Georgetown University forum, the Board will investigate public expressions of concern over how this statute is being used in Federal anti-terrorism efforts. The Board will meet with senior Department of Justice officials to gain an understanding of the statute's use and to ask questions regarding its possible abuse.

IV. Possible Areas of Improvement

Finally, I would like to propose a few suggestions going forward that Congress and the Administration could consider if the current Board is not essentially terminated by new legislation. As we enter the mid-point of our second year in existence, I would expect the Board to begin hiring additional staff and bring on detailees as soon as possible. We would engage even more actively with the public over counterterrorism policies and programs. In addition, the

Board would benefit from an enhanced stature within the Executive Office of the President, with its Executive Director holding a position of program authority comparable to the counterparts he works with on a daily basis. Moreover, additional opportunities should be sought to further institutionalize the Board's role and responsibilities within the Executive Branch,

I would also recommend that the Board obtain both periodic and ad hoc written reports from policy and legal officials from all the relevant agencies documenting their consideration of privacy and civil liberties considerations. And finally, the existing, very strong relationship between the Board and the privacy and civil liberties officers in place throughout the Executive Branch should be further strengthened and institutionalized by requiring periodic formal reporting from those officials to the Board.

Of course, whether the present Board continues in existence is out of our hands at this point. Should Congress pass legislation creating a new independent agency, and it becomes law, my colleagues on the Board and I stand ready to assist fully in the transition in order to ensure that privacy and civil liberties continue to be appropriately considered and protected in the country's efforts to combat terrorism. Should a new Board take our place, we will cooperate with it to help promote our shared mission.

Again, thank you for the opportunity to speak with you today, and I look forward to answering any questions you may have.

Ms. SÁNCHEZ. Thank you, Mr. Raul. We appreciate your testimony.

At this time, we would like to hear from Mr. Davis.

Mr. Davis, you may begin your testimony.

TESTIMONY OF LANNY J. DAVIS, ESQ., ORRICK, HERRINGTON & SUTCLIFFE, LLP, WASHINGTON, DC

Mr. DAVIS. Thank you, Madam Chairwoman and Mr. Feeney.

I would like to say first to Mr. Conyers, somebody who has been a political hero of mine since I was much, much younger and during the Clinton days was especially heroic, and it is nice to see you, sir.

And to Congressman Cannon, proving the words of Alexander Hamilton in the congressman's opening remarks that there are occasions where left and right not only come together but even in adversity become friends. And I appreciate it, Congressman Cannon, even when we sometimes disagreed on television. So nice to see you, sir.

And to directly respond to your comments about my resignation, first of all, my colleague, Alan Raul, the staff of the Privacy Board on which I served and to President Bush who appointed me and especially to Fred Fielding, the White House counsel, I only have memories of honor and legitimate disagreement that led to my resignation, no suggestion whatsoever of bad faith or even partisan motives that led to our disagreement.

The reason that I resigned was finally reaching the conclusion that the construct of the board was simply a square peg in a round hole. Congress tried to compromise between an independent board that would have oversight and a board within the White House that would have to have oversight of the very institution within which it resided. And while we all saw a contradiction and even a tension, as members of the board, we all thought we could work that out. And I thought that to a great extent we did have access, we were treated very well, and we were listened to. And I only have great memories of my service.

What led to my final conclusion—and it was reluctant, and it was painful—was that it simply was not possible to have independent oversight while being treated as if we were a part of the White House staff.

And the report to Congress led me to the conclusion that even if it were so, Congressman Cannon, that the red lines were only typographical errors and technical corrections—and that is not the case—the White House assumed that it had a right to take a report of our body, which was supposed to, under the statute, issue an annual report, edit it, review it, put it through OMG, circulate it, and send it back to us 2 days before submission with extensive redlining without even telling us that that was going to happen.

Now, in fact, the substance of what happened—I would never have resigned if it was just typographic errors—were significant deletions of substantive parts of our report, especially relating to what we wanted to look at in the year ahead.

For example, we wanted to look into the material witness statute which we had learned during one of our public hearings had civil liberties implications, and we had not ever looked at that. We re-

ceived back the red line where that provision was deleted, as were other deletions.

The material witness deletion, it was explained to us, was deleted not for substantive reasons and not for reasons of classified or sensitive information. We were told that it should be deleted because it might be confused with the U.S. attorneys controversy issue—in other words, an essentially political reason.

So, without casting aspersions, I recognized that the White House was doing its job in staffing us out just as if we were part of the White House, which we were. And so I changed my mind and decided that the better way would be to have an independent agency where the White House would not feel it needed to vet, edit and review the work product of a board that was supposed to be doing oversight.

But, again, having said that, everybody acted with correct motives, everybody did what they believed was right, and, most importantly, Fred Fielding was able to support the efforts of Alan Raul and myself and others to return to the original language that we had adopted, the very deletions that had caused me great concern.

I chose not to continue, notwithstanding Fred Fielding's support of my viewpoint, because I did not want every week or every other week to go back to Fred Fielding to ask him to intervene. I thought that the board needed fundamentally to be restructured, and that is why I reluctantly chose to resign.

Ms. SÁNCHEZ. Thank you, Mr. Davis. We appreciate your testimony.

Mr. CANNON. Madam Chair, may I ask unanimous consent to speak out of order for 1 minute?

Ms. SÁNCHEZ. Without objection, so ordered.

Mr. CANNON. Thank you.

Mr. Davis and I have disagreed in the past, as he indicated. From my point of view, he is an eloquent speaker.

And I just wanted to say to Mr. Davis, thank you for expressing those thoughts with such clarity and with such insight into the complexity of government and the jobs that each of us have as individuals and in describing your role as working on this board and the nature of the disagreement. I think that was remarkable. I appreciate it, and I just wanted to say that on the record.

And, Madam Chair, I yield back.

Mr. DAVIS. Thank you, sir.

Ms. SÁNCHEZ. Thank you.

Mr. Teufel?

TESTIMONY OF HUGO TEUFEL III, ESQ., U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. TEUFEL. Good afternoon, and thank you, Madam Chairwoman. Ranking Member Cannon, Chairman Conyers, Mr. Feeney, Mr. Franks, it is an honor to testify before you here today on the progress of the privacy office at the Department of Homeland Security and to review the findings and recommendations of the recent review of our office by the Government Accountability Office.

I would like to thank Representatives Watt and Cannon for requesting this review, the recommendations of which were useful, and I believe some of GAO's observations confirm progress in areas

that we have worked hard to improve. Oversight is a good thing. It fosters transparency and accountability, two of the Fair Information Practice principles that undergird the Privacy Act of 1974.

I would also like to thank Linda Koontz and her team for the work that they have done on the GAO report and on privacy oversight generally. While we do not always agree on issues, I respect her greatly and enjoy immensely working with her.

I was gratified to see GAO acknowledge the privacy office has made substantial progress both in the number and significantly the quality of Privacy Impact Assessments issued by our office. I attribute this to the hard work of my compliance staff and to our ongoing efforts to update our PIA guidance. We recently released a new version of the guidance and held a PIA workshop attended by over 100 people.

The next PIA workshop will be offered at the DHS Annual Security Awareness Training Conference in late summer 2007, and I am confident that these efforts will support the trend of simultaneous increases in the number and quality of PIAs issued by the department.

I was equally pleased to see in the GAO report that the privacy office has taken steps to integrate privacy into DHS decision-making. We call this important goal operationalizing privacy. To achieve this, the privacy office forms close relationships with system owners and program managers, along with I.T. security officials and senior DHS officials.

By placing privacy into the program development and decision-making processes of the department, we can ensure that DHS not only meets its legal requirements and improves the effectiveness of the department's programs, but stands as a model of how privacy can complement and work with law enforcement and intelligence agencies.

I also want to mention that the privacy office report of the Science and Technology Directorate's program, known as ADVISE, was released to the public yesterday. I know there is much interest in this report, and I understand that our Office of Legislative Affairs has provided electronic copies in PDF format to staff Members of the Committee. It is also available on our public Web site, dhs.gov/privacy.

This report took longer than I had anticipated, but it is a thorough report covering a number of uses of the tool in various stages of development and use throughout a number of DHS components. The extra time will make the report much more informative and useful to the public, Members of Congress and the department programs planning to use ADVISE in the future.

I thank the Subcommittee for this opportunity to testify about the accomplishments of the privacy office, and we look forward to demonstrating continued improvement in our efforts to ensure privacy is protected throughout the Department of Homeland Security.

I look forward to answering your questions.

[The prepared statement of Mr. Teufel follows:]

PREPARED STATEMENT OF HUGO TEUFEL III

WRITTEN STATEMENT

OF

HUGO TEUFEL III
CHIEF PRIVACY OFFICER
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

FOR A HEARING ENTITLED,

"OVERSIGHT HEARING ON THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICER"

JULY 24, 2007

Introduction

Chairman Sánchez, Ranking Member Cannon, and Members of the Subcommittee, it is an honor to testify before you today on the progress of the Privacy Office at the Department of Homeland Security (DHS) and to review the findings and recommendations of the recent review of our office by the Government Accountability Office (GAO). I am particularly pleased to be testifying at a hearing with Alan Raul from the Privacy and Civil Liberties Oversight Board (PCLOB). I have known Alan for a number of years and my office works closely with PCLOB on privacy issues.

Because this is my first time appearing before the Subcommittee, I would like to introduce myself. I was appointed Chief Privacy Officer of the U.S. Department of Homeland Security by Secretary Michael Chertoff on July 23, 2006. In this capacity and pursuant to Section 222 of the Homeland Security Act of 2002, 6 U.S.C. § 142, my office has primary responsibility for privacy policy at the Department, to include: assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; assuring that the Department complies with fair information practices as set out in the Privacy Act of 1974; conducting privacy impact assessments of proposed rules at the Department; evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; coordinating with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and

procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner, and Congress receives appropriate reports on such programs, policies, and procedures; and preparing an annual report to Congress on the activities of the Department that affect privacy. Additionally, I am responsible for overseeing DHS' implementation of privacy-related regulations and policies.

I also serve as the Department's Chief Freedom of Information Act (FOIA) Officer. In this role, I assure consistent and appropriate Department-wide statutory compliance and harmonized program and policy implementation.

The GAO Audit

In April 2007, the GAO issued a report entitled, "DHS PRIVACY OFFICE: Progress Made but Challenges Remain in Notifying and Reporting to the Public." This review constituted GAO's first-ever review of the DHS Privacy Office following the creation of the Department. When the Privacy Office stood up four years ago, it took on the unprecedented responsibility of a systematic review of both nearly 300 systems of records and many hundreds of information technology systems that were either part of the legacy agencies or incorporated into new components. Since starting with two people, the Privacy Office has grown in size and, through investment in personnel and hard work, created a comprehensive process to ensure privacy is protected when personally identifiable information (PII) is used or disclosed by DHS.

"Significant" and "Substantial" Progress

I was gratified to see that GAO acknowledged the Privacy Office has made "significant progress" in reviewing and approving Privacy Impact Assessments (PIAs). PIAs are required for certain systems under the E-Government Act, and are an invaluable

tool programs use to understand how their use of information impacts privacy. They are so useful, in fact, that we made a policy decision to complete a PIA for many programs under the authority of Section 222 of the Homeland Security Act, even when one is not required under the E-Government Act. In addition to helping programs identify and mitigate privacy concerns, PIAs also enhance the confidence the public has in the steps DHS takes to protect privacy; PIAs required by the E-Government Act are available for review on the Privacy Office's public facing website, www.dhs.gov/privacy.

I am pleased to report that our office is increasing its capacity to conduct PIAs. In FY05, the Privacy Office conducted approximately 17 PIAs; in FY06, that number rose to 25; and in the current fiscal year, we've already conducted 42 PIAs. While this marked increase is cause for satisfaction, it must be noted that the quality of PIAs increased significantly over this time as well. So reported GAO; and on this point, we concur.

This high standard is the result of regular refinement of the Privacy Office's PIA Guidance. In its report, GAO mentioned two updates to the PIA Guidance. In May 2007, after GAO published its report, the Privacy Office issued a new version of the PIA Guidance. The Privacy Office's Director of Compliance introduced these changes at a PIA workshop attended by more than 100 individuals. The next PIA workshop will be offered together with training for privacy incidents involving PII at the DHS annual Security Awareness Training conference in late summer 2007. I am confident that these efforts will support the trend of simultaneous increases in the number and quality of PIAs issued by the Department.

I was equally pleased to see in the GAO report that the Privacy Office has taken steps to integrate privacy into DHS decision-making. We term this important goal "operationalizing privacy." To achieve this, the Privacy Office forms close relationships with system owners and program managers, along with IT security officials, and senior DHS officials. By placing privacy into the program development and decision-making processes of the Department, we can ensure that DHS not only meets its legal requirements and improves the effectiveness of the Department's programs, but stands as a model of how privacy can complement and work with law enforcement and intelligence agencies.

As part of our ongoing operations, our Compliance group works with IT security, budgeting, procurement, financial, and program professionals Department-wide to complete Privacy Threshold Analyses (PTAs), PIAs, system of records notices (SORNS), and other privacy documentation relevant to and required for DHS' systems and programs.

GAO Recommendations

GAO made four recommendations to improve the Privacy Office's effectiveness:

(1) Designate full time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

(2) Implement a department-wide process for the biennial review of system or record notices, as required by OMB.

(3) Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report developmental clearance.

(4) Ensure that the Privacy Office's Annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

GAO provided the Privacy Office with a draft of its report, and our reply appears as an attachment to their final report. While this is a matter of public record already, I will summarize our reply and review the steps the Privacy Office has taken to implement the recommendations.

Recommendation One – Designate full time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, U.S. Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

The Privacy Office recognizes a strong correlation between the designation of privacy officers at the component and program level, and the success of the Privacy Office's mission within those components and programs. Privacy officers at the Transportation Security Administration and the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program office, for instance, are an important factor ensuring privacy is operationalized. While GAO observed that the components with designated privacy officers have produced a majority of the PIAs issued to date, this is just one example of the important contribution these component privacy officers make in embedding privacy into departmental programs. These component privacy officers provide day-to-day privacy expertise within their components to programs at all stages of development, ensuring that privacy is considered from the design through the implementation phase of every program within their component.

This recommendation is consistent with DHS Privacy Act Compliance Management Directive (MD) No. 0470.2. Specifically, section V.B.1. of the MD directs Under Secretaries and all DHS Designated Officials to:

Appoint an individual with day-to-day responsibility for implementing the privacy provisions of the Privacy Act, and any other applicable statutory privacy requirement.

The Privacy Office will continue to press the importance of placing privacy officers within the components and work with the Department to develop position descriptions and provide necessary training to support this development. We are working with senior leadership of the Department to designate component privacy officers in components that make significant use of PII.

Recommendation Two - Implement a department-wide process for the biennial review of system-of-records notices, as required by OMB.

The Privacy Office concurs with this recommendation. The Privacy Office developed the PTA in order to understand which nascent systems at DHS handle or involve PII and, of those systems, which need PIAs. Based on the analysis of the PIA, the Privacy Office can then identify which systems need new or updated SORNs. The Privacy Office found that the most expedient process to ensure overall privacy compliance focuses first on the development of the PIA and then on any the corresponding SORN, because the PIA helps identify the appropriate purposes, routine uses for disseminating information, types of information, categories of individuals affected, and, if applicable and appropriate, exemptions from certain Privacy Act requirements for the system of records.

The Privacy Office developed a two prong approach to reviewing the legacy SORNs and updating them appropriately. As noted in the GAO report, the Privacy Office has a well-developed PIA compliance process. Part of that process identifies the legacy SORNs and determines whether an updated or new SORN must be published. Next, the component, the Privacy Office, and the DHS Office of the General Counsel

review the SORN to issue a DHS SORN that is updated appropriately to describe the program as it exists under DHS and its homeland security mission. Programs making operational enhancements may not implement any updates until DHS publishes the SORN in the *Federal Register* and the Privacy Office approves the PIA.

In the second prong of the SORN review, the Privacy Office is systematically reviewing, by component, the legacy SORNs in order to issue updated SORNs on a schedule that prioritizes those systems with the most sensitive PII.

As of July 2007, the Privacy Office holds 266 System of Records, of which 215 are legacy system of records. DHS has issued 55 notices for updates to system of records, new system of records, and retirement of existing system of records. DHS is actively reviewing its remaining legacy system of records.

By the end of FY 2007, the Privacy Office will issue an updated System of Records Notice Guide to help in the drafting process. The Privacy Office is also developing a library of acceptable routine uses that components can use to identify appropriate routine uses as they review and develop their own SORNs. This will likely reduce the time needed to review draft SORNs.

This two-pronged approach will permit the Privacy Office to work with DHS components to evaluate methodically, and in a timely fashion, all of the existing SORNs to determine if the need exists to re-issue, remove, or re-draft each notice. The Privacy Office has met with a number of components and will meet with all others to establish appropriate timelines to accomplish this goal, consistent with the Privacy Office's responsibilities under issued OMB guidance.

Recommendation 3 – Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report development including departmental clearance.

The Privacy Office concurs and fully acknowledges the need for the timely issuance of its reports, including its annual report, and applies full effort to meet any report deadlines. The Privacy Office will work those components and programs impacted by its reports to provide for both full collaboration and coordination within DHS and timely issuance of its reports. We are confident that our reports will be timelier in the future. Our next annual report will cover the period from July 2006 to July 2007, and will soon be completed and sent to Congress.

On July 6, 2007, The Privacy Office released our 2007 Data Mining Report. This is exactly one year from the date of release of our 2006 Data Mining Report. The recent effort was not merely an update to the earlier report, however. We first had to familiarize ourselves with a new definition of "data mining" supplied in House Report No. 109-699 – *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2007, and for Other Purposes*. Then we had to apply that definition against all existing programs and new programs instituted throughout the year.

The last report I will mention here is the Privacy Office's review of the Science and Technology Directorate's Program, "Analysis, Dissemination, Visualization, Insight and Semantic Enhancement" (ADVISE). This report was initiated by me under the authority of Section 222 of the Homeland Security Act, which designates the Chief Privacy Officer as the DHS senior official responsible for ensuring that PII is used in full compliance with the fair information practices of the Privacy Act of 1974 and for reporting on complaints of privacy violations. As such, there is no statutory due date for

this report. Nonetheless, as GAO stated, giving the public and Congress timely information about programs supports transparency and accountability, two of the fair information practices the Privacy Office promotes. Accordingly, we are committed to issuing reports as quickly as is consistent with creating a useful, quality product. On March 21, 2007, I testified before the Homeland Security Subcommittee of the U.S. House of Representatives Committee on Appropriations. At that time, I answered a question about our efforts to review the ADVISE program. I stated that our review would be completed in a matter of weeks and that the report would be issued soon.

It is now four months later, and I wish to say a word about the interim. As it becomes clear reading the report, the term ADVISE covers a number of tools in various stages of development and use within several DHS components. To make sense of these after our initial review, we divided our examination into the ADVISE Technology Framework and the ADVISE Deployments, and proceeded to examine the privacy implications of each. This took longer than I anticipated it would during my March 21st testimony. Nonetheless, I believe the extra time it took to fully understand what we mean when we say "ADVISE" and then flesh out the privacy concerns with each will make the report much more informative and useful to the public, Members of Congress, and the Department programs planning to use ADVISE in the future.

Recommendation 4 – Ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

While the Privacy Office acknowledges that Section 222 of the Homeland Security Act of 2002 requires the Privacy Office to include in its annual report to Congress a number of items of information, including "complaints of privacy violations,"

the Privacy Office interpreted this list as descriptive, rather than prescriptive, in terms of where this information appears in the report. As such, the last report noted the privacy complaints the Privacy Office received within the substantive discussion of the actions of the Privacy Office.

For example, in the section discussing the reports provided to Congress, the last annual report notes the *Report on the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties* and the 2006 *Data Mining Report*. Although both reports were completed in response to Congressional requests, they dealt with privacy issues that surrounded complaints received by the Department. Additionally, this annual report discussed the work on the *Secure Flight* and *MATRIX* reports, which have since been issued and were directly responsive to complaints received by the Privacy Office. Further, the annual report noted the work of the Privacy Office with regard to the Undertakings concerning Passenger Name Records (PNR) and REAL ID, issues that had generated a number of comments to the Privacy Office from privacy groups, if not specifically privacy complaints. Thus, throughout the last annual report, the Privacy Office noted issues of interest brought to its attention regarding privacy and DHS.

Nonetheless, the Privacy Office agrees that for the sake of clarity a consolidated reporting structure for privacy complaints within future annual reports will assist in assuring Congress and the public that the Privacy Office is addressing the complaints that it receives.

External, Interagency, and International Outreach

The Privacy Office mission extends beyond operationalizing privacy within DHS. We also undertake a number of outreach initiatives in order to enhance transparency with

the general public and increase understanding of what the Department does to protect privacy, share best practices, adhere to privacy law, and respect the fair information practices. I was pleased to see that many of our outreach initiatives were also favorably reported by GAO.

The Data Privacy and Integrity Advisory Committee

The DHS Privacy and Integrity Advisory Committee (DPIAC) is chartered to offer advice and guidance to the Secretary and the Chief Privacy Officer on programmatic, policy, operational, and technological issues within DHS that relate to PII, as well as data integrity and other privacy-related matters.

The DPIAC was formed under the Federal Advisory Committee Act (FACA) in 2004. Members come from large and small companies, academia, and the non-profit sector, and are selected because of their expertise, education, training, and experience in the fields of data protection, privacy, and/or emerging technologies. DPIAC meetings are open to the public, and generally they are well attended.

Since its first meeting in 2005, the DPIAC has issued six reports with a total of 36 recommendations to enhance privacy protection within the Department. The advisory committee has met three times in FY07, and at its last meeting issued a report entitled "Comments Regarding the Notice of Proposed Rulemaking for Implementation of the REAL ID Act." This report has been shared with the Department's REAL ID governance committee and is assisting the Privacy Office to evaluate the privacy issues related to the drafting and implementation of the final rule. Of course, this report and all other DPIAC reports are available on the Privacy Office's public website.

The next meeting of the DPIAC will be held in September in Washington, DC.

White House Privacy and Civil Liberties Oversight Board

The Privacy Office continues to have a close working relationship with the President's Privacy and Civil Liberties Oversight Board (PCLOB). The executive director, Mark Robbins, appeared before the DPIAC at its meeting on September 20, 2006 and provided a summary of the board's activities since its inception. He described the mission of the board, articulating three charges: to participate in the development, implementation, and review of the guidelines for the information sharing environment (ISE); to release an annual report to Congress; and to advise the President and senior executive branch officials on how to ensure privacy and civil liberties interests based on current law, regulations, and policies. He also answered a number of questions from the DPIAC members, making it an informative and useful session. I am pleased to tell you that my colleague, Dan Sutherland, Civil Rights and Civil Liberties Officer at the Department, and I meet and converse regularly with Mark and our privacy and civil liberties colleagues at other agencies. As well, the Secretary and I have briefed the Board on occasion as requested by the Board.

Information Sharing Environment

Section 1016 of Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required the federal government to put into operation a recommendation of the 9-11 Commission to create a new means and methodology to share terrorism information across the entirety of the federal government as well as state, local, tribal, and foreign governments and private sector entities. Furthermore, the statute created the Program Manager's Office (PM/ISE) for the development and implementation of the ISE.

The DHS Privacy Office participated in all ISE Coordinating Group activities, providing necessary privacy leadership and supporting Departmental goals, and coordinated with other parts of the Department, including the Office of Security, the Office of the Chief Information Officer, and the Information Sharing & Collaboration Office. The output of these Coordinating Groups was used by the PM/ISE to respond to the President's direction, set out in a Presidential Memorandum dated December 15, 2005, setting forth specific guidelines and requesting recommendations for development of the ISE.

Out of these guidelines, specific working groups were developed with specified agency leads to provide specific guidance. The Privacy Office participated on a number of groups, including the Privacy group (Guideline 5), the Controlled Unclassified Information (CUI) group (Guideline 3), Foreign Government Information (FGI) group (Guideline 4), and participates in the State, Local, Tribal, and Private Sector group.

Privacy and Civil Liberties Committee

The Privacy Office participates in the interagency Privacy and Civil Liberties Committee co-chaired by OMB and the Department of Justice. This quarterly forum allows privacy personnel from all Federal agencies to exchange views and information on issues of mutual concern and discuss privacy best practices government-wide.

President's Identity Theft Task Force

Through Executive Order 13402, issued on May 10, 2006, the President established an Identity Theft Task Force comprised of 17 federal agencies, including DHS. The mission of the Task Force was to develop a comprehensive national strategy to combat identity theft. In the Executive Order, the President specifically directed the

Task Force to make recommendations on steps the federal government can take to reduce the likelihood of identity theft.

The Task Force recommended that OMB and DHS outline best practices in the arena of automated tools, training processes, and standards that would enable agencies to improve their security and privacy programs. In response to this recommendation, OMB and DHS developed a paper, titled "Common Risks Impeding the Adequate Protection of Government Information," which identifies common risks, or "mistakes," impeding agencies from adequately protecting government information. Agencies may refer to this paper, which is posted on the web sites for the Chief Information Officer (CIO) Council and the National Institute of Standards and Technology (NIST), when considering steps necessary for administering agency information security and privacy programs as required by law, policy, and guidance.

International Outreach

The Privacy Office provides crucial policy and programmatic guidance to the Secretary, Directorates and component agencies on international privacy matters. Over the past year, the Privacy Office has continued to expand both in its reach and in its effectiveness within the Department and with its partners abroad. The office expects this to continue throughout 2007 with more high profile cross-border data sharing issues facing the Department.

When the United States – European Union (U.S.–EU) Agreement on Passenger Name Records (PNR), in effect since 2004, was overturned by the European Court of Justice in May 2006, the DHS Policy Office led the negotiation of an interim agreement

and continues discussions with the European Commission. Because of the Privacy Office's expertise on international privacy frameworks, it became an important resource to the DHS negotiating team that successfully concluded a new PNR agreement.

In the last twelve months, the Privacy Office represented the U.S. government and DHS privacy policies at the following international forums: The International Conference of Data Protection and Privacy Commissioners in London, England; The Organization for Economic Cooperation and Development (OECD); and the International Association of Privacy Professionals (IAPP) meeting in Ontario, Canada.

In September 2006, the Privacy Office made a presentation to the Asian-Pacific Economic Cooperation (APEC) E-Commerce Steering Group on the DHS development of Privacy Impact Assessments. The Privacy Office also led the drafting of privacy provisions in the Regional Movement Alert System, a counter-terrorism initiative to share lost and stolen passport information with foreign partners. The resulting Memorandum of Understanding was adopted as a model by the APEC Business Mobility Group and endorsed by the APEC Ministers.

The Privacy Office co-hosted an International Conference on Biometrics and Ethics with US-VISIT and the DHS Biometric Coordination Group, in late 2006, in Washington, DC. This conference was held to promote understanding and international cooperation on the use of biometrics as its technologies evolve and impact individuals' privacy. The conference brought together approximately 80 experts from several countries to engage in an open discussion of the application and ethics of biometrics. Participants included representatives from academia, private industry, non-profit organizations and government, and hailed from Asia, Europe, the Middle East and North

America. In addition to DHS, representatives from the U.S. Departments of Defense, Justice and State also attended.

In January 2007, the Privacy Office participated in the APEC E-Commerce Steering Group's (ECSG) Data Privacy Subgroup (DPSG) meeting in Canberra, Australia where participants agreed upon a model for the commercial cross-border exchange of PII. The Privacy Office remains engaged in APEC activities to ensure that the scope of discussions does not jeopardize data sharing in the national security/law enforcement context.

Later in January, the Director of International Privacy Policy (who was recently selected to be the Deputy Chief Privacy Officer) attended a two day conference on Aviation Security in Singapore. More than 50 officials from the aviation security branches of Asian, Canadian and Middle Eastern governments attended, along with private representatives from the aviation industry. The Director presented an overview of DHS and its use of personal information relevant to aviation security. He also discussed developments in the EU and Asia Pacific region and suggested a global strategy for resolving impediments to the free flow of information for law enforcement and national security purposes. The Director's participation set the foundation for further contacts with Singapore data protection officials, who expressed a willingness to share developments in their privacy work.

Most recently, the Privacy Office's Director of International Privacy Policy and I traveled to Brussels to meet with members of the international and European media as well as E.U. government officials that included the European Data Protection Supervisor;

members of the Freedom, Security and Justice Directorate of the Commission; and members of the European Parliament.

The Privacy Office has endeavored to reach overseas audiences and increase understanding of USG privacy policy through publication of articles in the Bureau of National Affairs Privacy & Security Law. In *The Golden Rule of Privacy: A Proposal for a Global Privacy Policy On Government-to-Government Sharing of Personal Information*, the Director of International Privacy Policy suggests an approach based on the Fair Information Practices combined with the basic international principle of reciprocity. The Privacy Office has also prepared *Accountability and Oversight in the U.S. System*, as well as *Notice and Consent Principles in International Guidelines, Agreements and National Legislation*, which will be published later in 2007.

Conclusion

I thank the Subcommittee for this opportunity to testify about the significant efforts of the Privacy Office. I and my office look forward to demonstrating continued improvement in our efforts to ensure privacy is protected throughout the Department of Homeland Security.

Ms. SÁNCHEZ. Thank you, Mr. Teufel.
Ms. Koontz?

TESTIMONY OF LINDA KOONTZ, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Ms. KOONTZ. Madam Chairwoman and Members of the Subcommittee, I appreciate the opportunity to be here today to discuss progress made by the Department of Homeland Security's privacy office.

As you know, the Homeland Security Act of 2002 created at DHS, the first statutorily required senior privacy official at any Federal agency. The law mandated that this senior official assume primary responsibility for privacy policy, including assuring that the use of technology sustains and does not erode privacy protections relating to the use, collection and disclosure of personal information.

At this Subcommittee's and others' requests, we reviewed the progress the DHS privacy office has made since it was formally established in 2003. I would like to briefly summarize our results.

The privacy office has made significant progress in carrying out its statutory responsibilities under the Homeland Security Act and other laws. Specifically, the office has established processes for ensuring that the department complies with the E-Government Act requirement to conduct Privacy Impact Assessments before developing technology or initiating information collections that involve personal information. It has done this by developing a compliance framework including written guidance, a template for conducting the assessments, training and a process for identifying systems that require assessments.

These actions have led to increased attention to privacy requirements. It has also proved beneficial in identifying systems that require an assessment, from 46 identified in 2005 to a projected 188 in fiscal year 2007.

However, the resulting workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain key department components could help speed the processing of assessments, but DHS has not yet done this.

The office has also taken action to integrate privacy considerations into the departmental decision-making process by establishing a Federal advisory committee, conducting public workshops and participating in policy development for major departmental initiatives. These actions provide an opportunity for privacy concerns to be raised explicitly and early in the development of policies.

While substantial progress has been made in these areas, limited progress has been made in other important aspects of privacy protection. For example, the office has reviewed, approved and issued 56 new and revised public notices that are required under the Privacy Act.

However, little progress has been made in updating notices for legacy systems, older collections of records originally designated and maintained by other agencies prior to the creation of DHS. As a result, the department cannot be assured that the privacy implications of its many systems that process personal information have been fully and accurately disclosed to the public.

Further, the privacy officer has not been timely in issuing public reports. For example, the office has issued only two of the required annual reports to the Congress in the past 3 years. In addition, its reports on investigations that the office conducted were, in some cases, not publicly released until long after concerns had been addressed. Late issuance of reports has a number of consequences beyond failure to comply with the law. It potentially reduces the value of these reports and erodes the credibility of the privacy office.

Clearly, the DHS privacy office has made significant progress and has been a leader in the Federal Government. Nonetheless, much challenging work remains to be done.

That concludes my statement. I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Koontz follows:]

PREPARED STATEMENT OF LINDA KOONTZ

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EDT
Tuesday, July 24, 2007

HOMELAND SECURITY

DHS Privacy Office Has Made Progress but Faces Continuing Challenges

Statement of Linda Koontz
Director, Information Management Issues

GAO-07-1024T

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-1024T, a testimony before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

The Department of Homeland Security (DHS) Privacy Office was established with the appointment of the first Chief Privacy Officer in April 2003, as required by the Homeland Security Act of 2002. The Privacy Office's major responsibilities include: (1) reviewing and approving privacy impact assessments (PIA)—analyses of how personal information is managed in a federal system, (2) integrating privacy considerations into DHS decision making and ensuring compliance with the Privacy Act of 1974, and (3) preparing and issuing annual reports and reports on key privacy concerns.

GAO was asked to testify on its recent report examining progress made by the DHS Privacy Office in carrying out its statutory responsibilities. GAO compared statutory requirements with Privacy Office processes, documents, and activities.

What GAO Recommends

In its report, GAO recommended that the Secretary of Homeland Security take several actions including appointing privacy officers in key DHS components, implementing a process for reviewing Privacy Act notices, and establishing a schedule for timely issuance of Privacy Office reports.

DHS generally agreed with the report and described actions initiated to address GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-1024T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

HOMELAND SECURITY

DHS Privacy Office Has Made Progres but Faces Continuing Challenges

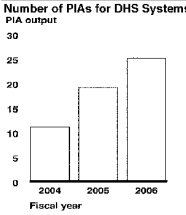
What GAO Found

The DHS Privacy Office has made significant progress in carrying out it statutory responsibilities under the Homeland Security Act and its relat role in ensuring compliance with the Privacy Act of 1974 and E-Governı Act of 2002, but more work remains to be accomplished. Specifically, tl Privacy Office has established a compliance framework for conducting which are required by the E-Gov Act. The framework includes formal w guidance, training sessions, and a process for identifying systems requi such assessments. The framework has contributed to an increase in the quality and number of PIAs issued (see fig.) as well as the identificatior many more affected systems. The resultant workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain DHS components could help speed processing of PIAs, but DHS not yet taken action to make these designations.

The Privacy Office has also taken actions to integrate privacy considera into the DHS decision-making process by establishing an advisory committee, holding public workshops, and participating in policy development. However, limited progress has been made in one aspect (ensuring compliance with the Privacy Act—updating public notices for systems of records that were in existence prior to the creation of DHS. These notices should identify, among other things, the type of data coll the types of individuals about whom information is collected, and the intended uses of the data. Until the notices are brought up-to-date, the department cannot assure the public that the notices reflect current use protections of personal information.

Further, the Privacy Office has generally not been timely in issuing pub reports. For example, a report on the Multi-state Anti-Terrorism Inform Exchange program—a pilot project for law enforcement sharing of pub records data—was not issued until long after the program had been terminated. Late issuance of reports has a number of negative conseque including a potential reduction in the reports' value and erosion of the office's credibility.

Number of PIAs for DHS Systems Published by Fiscal Year



Source: GAO analysis of published DHS PIAs.

Madam Chairwoman and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss progress made and challenges faced by the Department of Homeland Security's (DHS) Privacy Office. As you know, the Homeland Security Act of 2002 created the first statutorily required senior privacy official at any federal agency. This law mandated the appointment of a senior official at DHS to assume primary responsibility for privacy policy, including, among other things, assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information.[1]

As the federal government obtains and processes personal information[2] about its citizens and residents in increasingly diverse ways to better secure our homeland, it is important that this information be properly protected and the privacy rights of individuals respected. Advances in information technology make it easier than ever for DHS and other agencies to acquire data on individuals, analyze it for a variety of purposes, and share it with other governmental and nongovernmental entities. Further, the demands of the war on terror have led agencies to seek ways to extract as much value as possible from the information available to them, adding to the potential for compromising privacy. It is in this context that the DHS Privacy Officer is charged with ensuring that the privacy rights of individuals remain adequately addressed.

Formally established with the appointment of the first Chief Privacy Officer in April, 2003, the DHS Privacy Office is responsible for ensuring that the department is in compliance with federal laws that govern the use of personal information by the federal government. Among these laws are the Homeland Security Act of 2002 (as amended by the Intelligence Reform and Terrorism Prevention Act of 2004), the Privacy Act of 1974,

[1]Homeland Security Act of 2002, Sec. 222, Pub. L. No. 107-296 (Nov. 25, 2002).

[2]For purposes of this testimony, the term *personal information* encompasses all information associated with an individual, including *personally identifiable information*, which refers to any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

and the E-Government Act of 2002 (E-Gov Act).[3] The Privacy Office's major responsibilities can be summarized into four broad categories: (1) reviewing and approving privacy impact assessments (PIA) of the risks associated with information technology used to process personal information,[4] as required by the E-Government Act, (2) integrating privacy considerations into DHS decision making, (3) reviewing and approving public notices required by the Privacy Act, and (4) preparing and issuing reports.

My testimony today is based on a report that we recently issued.[5] In that report, we assessed progress made by the DHS Privacy Office in carrying out its responsibilities under federal privacy laws, including the Homeland Security Act and the E-Gov Act. In conducting work for that report, we compared statutory requirements with Privacy Office processes, documents, and activities. Our work was performed in accordance with generally accepted government auditing standards.

Today, after a brief summary and a discussion of the establishment of the DHS Privacy Office and its major responsibilities, my remarks will focus on the results of our review of the DHS Privacy Office.

Results in Brief

The DHS Privacy Office has made significant progress in carrying out its statutory responsibilities under the Homeland Security Act and its related role in ensuring E-Gov Act compliance, but more work remains to be accomplished. Specifically, the Privacy Office has established processes for ensuring departmental compliance with the PIA requirement in the E-Gov Act. It has done this by developing a compliance framework that includes formal written guidance, a template for conducting assessments, training sessions, a process for identifying systems that require assessments, and a process for reviewing and approving assessments. Instituting this framework has led to increased attention to privacy

[3]Section 222 of the Homeland Security Act, as amended by section 8305 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 (Dec. 17, 2004), 6 U.S.C. § 142; Privacy Act of 1974, 5 U.S.C. § 552a; section 208 of the E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[4]A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system to ensure that privacy requirements are addressed.

[5]GAO, *DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public*, GAO-07-522, (Washington, D.C.: Apr. 27, 2007).

requirements on the part of departmental components, contributing to an increase in the quality and number of PIAs issued. It has also proved beneficial in identifying systems that require an assessment, from 46 identified in fiscal year 2005 to a projected 188 in fiscal year 2007. However, the resulting increase in the workload is likely to prove difficult to process in a timely manner. Designating privacy officers in certain key DHS components could help speed processing of PIAs, but DHS has not yet done this.

The Privacy Office has taken actions to integrate privacy considerations into the DHS decision-making process through a variety of actions, including establishing a federal advisory committee, conducting a series of public workshops, and participating in policy development for several major departmental initiatives. These actions serve, in part, to address the mandate to assure that technologies sustain and do not erode privacy protections. The Privacy Office's participation in policy decisions provides an opportunity for privacy concerns to be raised explicitly and considered in the development of DHS policies. In addition, the office has taken steps to address its mandates to evaluate regulatory and legislative proposals involving personal information and to coordinate with the DHS Officer for Civil Rights and Civil Liberties.

While substantial progress has been made in these areas, limited progress has been made in other important aspects of privacy protection. For example, while the Privacy Office had reviewed, approved, and issued 56 new and revised Privacy Act public notices as of February 2007, little progress has been made in updating notices for "legacy" systems of records—older systems of records that were originally developed by other agencies prior to the creation of DHS. According to Privacy Office officials, they have focused their attention on reviewing and approving PIAs and developing notices for new systems and have given less priority to revising notices for legacy systems. However, because many of these notices are not up-to-date, the department cannot be assured that the privacy implications of its many systems that process and maintain personal information have been fully and accurately disclosed to the public.

Further, the Privacy Office has generally not been timely in issuing public reports, potentially limiting their value and impact. The Homeland Security Act requires that the Privacy Officer report annually to Congress on its activities, including complaints of privacy violations. However, the office has issued only two annual reports within the 3-year period since it was established in April 2003, and one of these did not include complaints of

privacy violations as required. In addition, other reports to Congress on several specific topics have been late. The office also initiated its own investigations of specific programs and produced reports on these reviews, but several of them were not publicly released until long after concerns had been addressed. Late issuance of reports has a number of negative consequences beyond failure to comply with mandated deadlines, including a potential reduction in the reports' value and erosion of the office's credibility.

We made recommendations to the Secretary of Homeland Security to designate component-level privacy officers at key components, ensure that Privacy Act notices reflect current DHS activities, and help the Privacy Office meet its obligations to issue reports in a timely manner. DHS generally agreed with our recommendations and described actions initiated to address them.

Background

The DHS Privacy Office was established with the appointment of the first Chief Privacy Officer in April 2003. The Chief Privacy Officer is appointed by the Secretary and reports directly to him. The Chief Privacy Officer serves as the designated senior agency official for privacy, as has been required by the Office of Management and Budget (OMB) of all major departments and agencies since 2005.[6] As a part of the DHS organizational structure, the Chief Privacy Officer has the ability to serve as a consultant on privacy issues to other departmental entities that may not have adequate expertise on privacy issues. In addition, there are also component-level and program-level privacy officers at the Transportation Security Administration (TSA), U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, and U.S. Citizenship and Immigration Services.

When the Privacy Office was initially established, it had 5 full-time employees, including the Chief Privacy Officer. Since then, the staff has expanded to 16 full-time employees. As of February 2007, the Privacy Office also had 9 full-time and 3 half-time contractor staff. The first Chief Privacy Officer served from April 2003 to September 2005, followed by an Acting Chief Privacy Officer who served through July 2006. In July 2006, the Secretary appointed a second permanent Chief Privacy Officer.

[6]Office of Management and Budget, *Designation of Senior Agency Officials for Privacy*, M-05-08 (Feb. 11, 2005).

Privacy Office Responsibilities

The Privacy Office is responsible for ensuring that DHS is in compliance with federal laws that govern the use of personal information by the federal government. Among these laws are the Homeland Security Act of 2002 (as amended by the Intelligence Reform and Terrorism Prevention Act of 2004), the Privacy Act of 1974, and the E-Gov Act of 2002. Based on these laws, the Privacy Office's major responsibilities can be summarized into these four broad categories:

1. reviewing and approving PIAs,
2. integrating privacy considerations into DHS decision making,
3. reviewing and approving public notices required by the Privacy Act, and
4. preparing and issuing reports.

Reviewing and approving PIAs

The Privacy Office is responsible for ensuring departmental compliance with the privacy provisions of the E-Gov Act. Specifically, section 208 of the E-Gov Act is designed to enhance protection of personally identifiable information in government information systems and information collections by requiring that agencies conduct PIAs. In addition, the Homeland Security Act requires the Chief Privacy Officer to conduct a PIA for proposed rules of the department on the privacy of personal information.

According to OMB guidance,[7] a PIA is an analysis of how information is handled: (1) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating personally identifiable information in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential risks to privacy.

Agencies must conduct PIAs before they (1) develop or procure information technology that collects, maintains, or disseminates personally identifiable information or (2) initiate any new data collections

[7]Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

of personal information that will be collected, maintained, or disseminated using information technology—if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available,[8] they provide explanations to the public about such things as what information will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

Integrating privacy considerations into the DHS decision-making process

Several of the Privacy Office's statutory responsibilities involve ensuring that the major decisions and operations of the department do not have an adverse impact on privacy. Specifically, the Homeland Security Act requires that the Privacy Office assure that the use of technologies by the department sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. The act further requires that the Privacy Office evaluate legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government. It also requires the office to coordinate with the DHS Officer for Civil Rights and Civil Liberties on those issues.

Reviewing and approving public notices required by the Privacy Act

The Privacy Office is required by the Homeland Security Act to assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974. The Privacy Act places limitations on agencies' collection, disclosure, and use of personally identifiable information that is maintained in their systems of records. The act defines a record as any item, collection, or grouping of information about an individual that is maintained by an agency and contains that individual's name or other personal identifier, such as a Social Security number. It defines "system-of-records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires agencies to notify the public, via a notice in the Federal Register, when they create or modify a system-of-records notice. This notice must include information such as the type of

[8]Section 208(b)(1)(B)(iii) of the E-Gov Act requires agencies, if practicable, to make PIAs publicly available through agency Web sites, publication in the *Federal Register*, or by other means. Pub. L. No. 107-347 (Dec. 17, 2002).

information collected, the types of individuals about whom information is collected, the intended "routine" uses of the information, and procedures that individuals can use to review and correct their personal information.[9] The act also requires agencies to define—and limit themselves to—specific purposes for collecting the information.[10]

Preparing and issuing reports

The Homeland Security Act requires the Privacy Office to prepare annual reports to Congress detailing the department's activities affecting privacy, including complaints of privacy violations and implementation of the Privacy Act of 1974. In addition to the reporting requirements under the Homeland Security Act, Congress has occasionally directed the Privacy Office to report on specific technologies and programs. For example, in the conference report for the DHS appropriations act for fiscal year 2005, Congress directed the Privacy Office to report on DHS's use of data mining technologies.[11] The Intelligence Reform and Terrorism Prevention Act of 2004 also required the Chief Privacy Officer to submit a report to Congress on the impact on privacy and civil liberties of the DHS-maintained Automatic Selectee and No-Fly lists, which contain names of potential airline passengers who are to be selected for secondary screening or not allowed to board aircraft. In addition, the Privacy Office can initiate its own investigations and produce reports under its Homeland Security Act authority to report on complaints of privacy violations and assure technologies sustain and do not erode privacy protections.

[9]Under the Privacy Act of 1974, the term routine use means (with respect to the disclosure of a record) the use of a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[10]Agencies are allowed to claim exemptions from provisions of the Privacy Act if the records are used for specific purposes, such as law enforcement. 5 U.S.C. § 552a(j) and (k).

[11]Conference Report on H.R. 4567, Department of Homeland Security Appropriations Act, 2005, House Report 108-774 (Oct. 9, 2004).

The Privacy Office Has Made Significant Progress in Reviewing and Approving PIAs, but Faces an Increasing Workload

One of the Privacy Office's primary responsibilities is to review and approve PIAs to ensure departmental compliance with the privacy provisions (section 208) of the E-Gov Act of 2002. The Privacy Office has established a PIA compliance framework to carry out this responsibility. The centerpiece of the Privacy Office's compliance framework is its written guidance on when a PIA must be conducted, how the associated analysis should be performed, and how the final document should be written. Although based on OMB's guidance,[12] the Privacy Office's guidance goes further in several areas. For example, the guidance does not exempt national security systems[13] and also clarifies that systems in the pilot testing phase are not exempt. The DHS guidance also provides more detailed instructions than OMB's guidance on the level of detail to be provided. For example, the DHS guidance requires a discussion of a system's data retention period, procedures for allowing individual access, redress, correction of information, and technologies used in the system, such as biometrics or radio frequency identification (RFID).

The Privacy Office has taken steps to continually improve its PIA guidance. Initially released in February 2004, the guidance has been updated each year since then. These updates have increased the emphasis on describing the privacy analysis that should take place in making system design decisions that affect privacy. For example, regarding information collection, the latest guidance requires program officials to explain how the collection supports the purpose(s) of the system or program and the mission of the organization. The guidance also reminds agencies that the information collected should be relevant and necessary to accomplish the stated purpose(s) and mission. To accompany its written guidance, the Privacy Office has also developed a PIA template and conducted a number of training sessions to further assist DHS personnel.

Our analysis of published DHS PIAs shows significant quality improvements in those completed recently compared with those from 2 or

[12]OMB, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

[13]A national security system is defined by the Clinger-Cohen Act as an information system operated by the federal government, the function, operation, or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons system, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management.

3 years ago. Overall, there is a greater emphasis on analysis of system development decisions that impact privacy, because the guidance now requires that such analysis be performed and described. For example, the most recent PIAs include assessments of planned uses of the system and information, plans for data retention, and the extent to which the information is to be shared outside of DHS. Earlier PIAs did not include any of these analyses.

The emphasis on analysis should allow the public to more easily understand a system and its impact on privacy. Further, our analysis found that use of the template has resulted in a more standardized structure, format, and content, making the PIAs more easily understandable to the general reader.

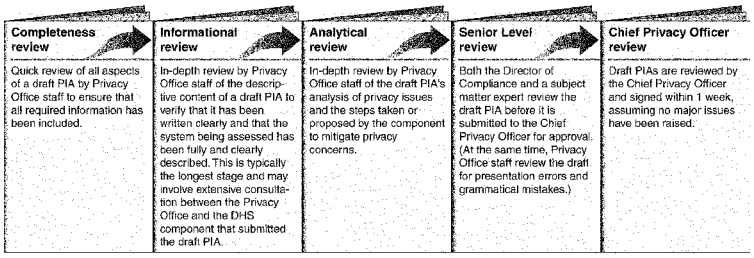
In addition to written guidance, the Privacy Office has also taken steps to integrate PIA development into the department's established operational processes. For example, the Privacy Office is using the OMB Exhibit 300 budget process[14] as an opportunity to ensure that systems containing personal information are identified and that PIAs are conducted when needed. OMB requires agencies to submit an Exhibit 300 Capital Asset Plan and Business Case for their major information technology systems in order to receive funding. The Exhibit 300 template asks whether a system has a PIA and if it is publicly available. Because the Privacy Office gives final departmental approval for all such assessments, it is able to use the Exhibit 300 process to ensure the assessments are completed. According to Privacy Office officials, the threat of losing funds has helped to encourage components to conduct PIAs. Integration of the PIA requirement into these management processes is beneficial in that it provides an opportunity to address privacy considerations during systems development, as envisioned by OMB's guidance.

Because of concerns expressed by component officials that the Privacy Office's review process takes a long time and is difficult to understand, the office has made efforts to improve the process and make it more transparent to DHS components. Specifically, the office has established a five-stage review process. Under this process, a PIA must satisfy all the requirements of a given stage before it can progress to the next one. The

[14]OMB Circular No. A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets* (Washington, D.C.: June 2006).

review process is intended to take 5 to 6 weeks, with each stage intended to take 1 week. Figure 1 illustrates the stages of the review process.

Figure 1: **The PIA Review Process**



Source: DHS.

Privacy Office Efforts Have Helped to Identify the Need for an Increasing Number of PIAs

Through efforts such as the compliance framework, the Privacy Office has steadily increased the number of PIAs it has approved and published each year.[16] Since 2004, PIA output by the Privacy Office has more than doubled. According to Privacy Office officials, the increase in output was aided by the development and implementation of the Privacy Office's structured guidance and review process. In addition, Privacy Office officials stated that as DHS components gain more experience, the output should continue to increase.

Because the Privacy Office has focused departmental attention on the development and review process and established a structured framework

[16]As of February 2007, the Privacy Office had approved and published a total of 71 PIAs. Of these, 46 were new, 20 were updates to preexisting documents, and 5 were PIAs for agency rules. Section 222 of the Homeland Security Act requires the Chief Privacy Officer to "[conduct] a privacy impact assessment of proposed rules for the department or that of the department on the privacy of personal information including the type of personal information collected and the number of people affected."

for identifying systems that need PIAs, the number of identified DHS systems requiring a PIA has increased dramatically. According to its annual Federal Information Security Management Act reports, DHS identified 46 systems as requiring a PIA in fiscal year 2005 and 143 systems in fiscal year 2006. Based on the privacy threshold analysis process, the Privacy Office estimates that 188 systems will require a PIA in fiscal year 2007.

Considering that only 25 were published in fiscal year 2006, it will likely be very difficult for DHS to expeditiously develop and issue PIAs for all of these systems because developing and approving them can be a lengthy process. According to estimates by Privacy Office officials, it takes approximately six months[16] to develop and approve a PIA, but the office is working to reduce this time.

The Privacy Office is examining several potential changes to the development process that would allow it to process an increased number of PIAs. One such option is to allow DHS components to quickly amend preexisting PIAs. An amendment would only need to contain information on changes to the system and would allow for quicker development and review. The Privacy Office is also considering developing standardized PIAs for commonly-used types of systems or uses. For example, such an assessment may be developed for local area networks. Systems intended to collect or use information outside what is specified in the standardized PIA would need approval from the Privacy Office.

The Privacy Office Has Taken Steps to Integrate Privacy Into DHS Decision Making

The Privacy Office has also taken steps to integrate privacy considerations in the DHS decision-making process. These actions are intended to address a number of statutory requirements, including that the Privacy Office assure that the use of technologies sustain, and do not erode, privacy protections; that it evaluate legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the federal government; and that it coordinate with the DHS Officer for Civil Rights and Civil Liberties.

For example, in 2004, the first Chief Privacy Officer established the DHS Data Privacy and Integrity Advisory Committee to advise her and the

[16]Although PIA development time is not formally tracked, DHS component-level officials reported it could take significantly longer than 6 months to develop a PIA.

Secretary on issues within the department that affect individual privacy, as well as data integrity, interoperability, and other privacy-related issues. The committee has examined a variety of privacy issues, produced reports, and made recommendations. In December 2006, the committee adopted two reports; one on the use of RFID for identity verification and another on the use of commercial data. According to Privacy Office officials, the additional instructions on the use of commercial data contained in the May 2007 PIA guidance update were based, in part, on the advisory committee's report on commercial data.

In addition to its reports, which are publicly available, the committee meets quarterly in Washington, D.C., and in other parts of the country where DHS programs operate. These meetings are open to the public and transcripts of the meetings are posted on the Privacy Office's Web site.[17] DHS officials from major programs and initiatives involving the use of personal data such as US-VISIT, Secure Flight, and the Western Hemisphere Travel Initiative, have testified before the committee. Private sector officials have also testified on topics such as data integrity, identity authentication, and RFID.

Because the committee is made up of experts from the private sector and the academic community, it brings an outside perspective to privacy issues through its reports and recommendations. In addition, because it was established as a federal advisory committee, its products and proceedings are publicly available and thus provide a public forum for the analysis of privacy issues that affect DHS operations.

The Privacy Office has also taken steps to raise awareness of privacy issues by holding a series of public workshops. The first workshop, on the use of commercial data for homeland security, was held in September 2005. Panel participants consisted of representatives from academia, the private sector, and government. In April 2006, a second workshop addressed the concept of public notices and freedom of information frameworks. In June 2006, a workshop was held on the policy, legal, and operational frameworks for PIAs and privacy threshold analyses and

[17]Reports produced by the DHS Data Privacy and Integrity Advisory Committee and transcripts of quarterly meetings can be found at http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm.

included a tutorial for conducting PIAs.[18] Hosting public workshops is beneficial in that it allows for communication between the Privacy Office and those who may be affected by DHS programs, including the privacy advocacy community and the general public.

Privacy Office Officials Have Participated in the DHS Decision-making Process

Another part of the Privacy Office's efforts to carry out its Homeland Security Act requirements is its participation in departmental policy development for initiatives that have a potential impact on privacy. The Privacy Office has been involved in policy discussions related to several major DHS initiatives and, according to department officials, the office has provided input on several privacy-related decisions. The following are major initiatives in which the Privacy Office has participated.

Passenger name record negotiations with the European Union

United States law requires airlines operating flights to or from the United States to provide the Bureau of Customs and Border Protection (CBP) with certain passenger reservation information for purposes of combating terrorism and other serious criminal offenses. In May 2004, an international agreement on the processing of this information was signed by DHS and the European Union.[19] Prior to the agreement, CBP established a set of terms for acquiring and protecting data on European Union citizens, referred to as the "Undertakings".[20] In September 2005, under the direction of the first Chief Privacy Officer, the Privacy Office issued a report on CBP's compliance with the Undertakings in which it provided guidance on necessary compliance measures and also required certain remediation steps. For example, the Privacy Office required CBP to review and delete data outside the 34 data elements permitted by the agreement. According to the report, the deletion of these extraneous elements was completed in August 2005 and was verified by the Privacy Office.

[18]In addition, in November 2006, the Privacy Office, US-VISIT program, and the DHS Biometrics Coordination Group sponsored a conference on privacy issues related to biometric technology; however, this conference was not open to the public or the media.

[19]The EU Data Protection Directive (Article 25(6) of Directive 95/46/EC) generally prohibits cross-border sharing with non-EU countries unless the receiving entity demonstrates that it has adequate data protection standards.

[20]DHS Privacy Office, *A Report Concerning Passenger Name Record Information Derived From Flights Between the U.S. and The European Union* (Washington, D.C.: Sept. 19, 2005).

In October 2006, DHS and the European Union completed negotiations on a new interim agreement concerning the transfer and processing of passenger reservation information. The Director of International Privacy Policy within the Privacy Office participated in these negotiations along with others from DHS in the Policy Office, Office of General Counsel, and CBP.

Western Hemisphere Travel Initiative

The Western Hemisphere Travel Initiative is a joint effort between DHS and the Department of State to implement new documentation requirements for certain U.S. citizens and nonimmigrant aliens entering the United States. DHS and State have proposed the creation of a special identification card that would serve as an alternative to a traditional passport for use by U.S. citizens who cross land borders or travel by sea between the United States, Canada, Mexico, the Caribbean, or Bermuda.[31] The card is to use a technology called vicinity RFID to transmit information on travelers to CBP officers at land and sea ports of entry. Advocacy groups have raised concerns about the proposed use of vicinity RFID because of privacy and security risks due primarily to the ability to read information from these cards from distances of up to 20 feet. The Privacy Office was consulted on the choice of identification technology for the cards. According to the DHS Policy Office, Privacy Office input led to a decision not to store or transmit personally identifiable information on the RFID chip on the card. Instead, DHS is planning on transmitting a randomly-generated identifier for individuals, which is to be used by DHS to retrieve information about the individual from a centralized database.

REAL ID Act of 2005

Among other things, the REAL ID Act[32] requires DHS to consult with the Department of Transportation and the states in issuing regulations that set minimum standards for state-issued REAL ID drivers' licenses and identification cards to be accepted for official purposes after May 11, 2008. Advocacy groups have raised a number of privacy concerns about REAL ID, chiefly that it creates a de facto national ID that could be used in the future for privacy-infringing purposes and that it puts individuals at

[31] 71 *Federal Register* 60928-60932 (Oct. 17, 2006).

[32] Division B, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13 (May 11, 2005).

increased risk of identity theft. The DHS Policy Office reported that it included Privacy Office officials, as well as officials from the Office of Civil Rights and Civil Liberties, in developing its implementing rule for REAL ID.[23] The Privacy Office's participation in REAL ID also served to address its requirement to evaluate legislative and regulatory proposals concerning the collection, use, and disclosure of personal information by the federal government.[24] According to its November 2006 annual report, the Privacy Office championed the need for privacy protections regarding the collection and use of the personal information that will be stored on the REAL ID drivers' licenses. Further, the office reported that it funded a contract to examine the creation of a state federation to implement the information sharing required by the act in a privacy-sensitive manner.

Use of commercial data

As we have previously reported, DHS has used personal information obtained from commercial data providers for immigration, fraud detection, and border screening programs but, like other agencies, does not have policies in place concerning its uses of these data.[25] Accordingly, we recommended that DHS, as well as other agencies, develop such policies. In response to the concerns raised in our report and by privacy advocacy groups, Privacy Office officials said they were drafting a departmentwide policy on the use of commercial data. Once drafted by the Privacy Office, this policy is to undergo a departmental review process (including review by the Policy Office, General Counsel, and Office of the Secretary), followed by a review by OMB prior to adoption.

These examples demonstrate specific involvement of the Privacy Office in major DHS initiatives. However, Privacy Office input is only one factor that DHS officials consider in formulating decisions about major programs, and Privacy Office participation does not guarantee that privacy

[23]The Intelligence Reform Act of 2004 requires the DHS Privacy Officer to coordinate activities with the DHS Officer for Civil Rights and Civil Liberties. Participation in this working group is one example of coordination between the two offices.

[24]Privacy Office officials reported that they use the OMB legislative review process and the publication of rules in the *Federal Register* as mechanisms for reviewing emerging rules and legislation. In addition, the Privacy Office recently created a Director of Legislative and Regulatory Affairs position to coordinate, among other things, review of proposed privacy legislation and rulemakings. This position was filled in February 2007.

[25]GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

concerns will be fully addressed. For example, our previous work has highlighted problems in implementing privacy protections in specific DHS programs, including Secure Flight[26] and the ADVISE program.[27] Nevertheless, the Privacy Office's participation in policy decisions provides an opportunity for privacy concerns to be raised explicitly and considered in the development of DHS policies.

The Privacy Office Has Coordinated Activities with the DHS Officer for Civil Rights and Civil Liberties

The Privacy Office has also taken steps to address its mandate to coordinate with the DHS Officer for Civil Rights and Civil Liberties on programs, policies, and procedures that involve civil rights, civil liberties, and privacy considerations, and ensure that Congress receives appropriate reports. The DHS Officer for Civil Rights and Civil Liberties cited three specific instances where the offices have collaborated. First, as stated previously, both offices have participated in the working group involved in drafting the implementing regulations for REAL ID. Second, the two offices coordinated in preparing the Privacy Office's report to Congress assessing the privacy and civil liberties impact of the No-Fly and Selectee lists used by DHS for passenger prescreening. Third, the two offices coordinated on providing input for the "One-Stop Redress" initiative, a joint initiative between the Department of State and DHS to implement a streamlined redress center for travelers who have concerns about their treatment in the screening process.

[26]GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R (Washington, D.C.: July 22, 2005).

[27]GAO, *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*, GAO-07-293 (Washington, D.C.: Feb. 28, 2007).

Although Privacy Act Processes Have Been Established, Little Progress Has Been Made in Updating Public Notices for DHS Legacy Systems-of-Records

The DHS Privacy Office is responsible for reviewing and approving DHS system-of-records notices to ensure that the department complies with the Privacy Act of 1974. Specifically, the Homeland Security Act requires the Privacy Office to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." The Privacy Act requires that federal agencies publish notices in the *Federal Register* on the establishment or revision of systems of records. These notices must describe the nature of a system-of-records and the information it maintains. Additionally, OMB has issued various guidance documents for implementing the Privacy Act. OMB Circular A-130, for example, outlines agency responsibilities for maintaining records on individuals and directs government agencies to conduct biennial reviews of each system-of-records notice to ensure that it accurately describes the system-of-records.[28]

The Privacy Office has taken steps to establish a departmental process for complying with the Privacy Act. It issued a management directive that outlines its own responsibilities as well as those of component-level officials. Under this policy, the Privacy Office is to act as the department's representative for matters relating to the Privacy Act. The Privacy Office is to issue and revise, as needed, departmental regulations implementing the Privacy Act and approve all system-of-records notices before they are published in the Federal Register. DHS components are responsible for drafting system-of-records notices and submitting them to the Privacy Office for review and approval. The management directive was in addition to system-of-records notice guidance published by the Privacy Office in August 2005. The guidance discusses the requirements of the Privacy Act and provides instructions on how to prepare system-of-records notices by listing key elements and explaining how they must be addressed. The guidance also lists common routine uses and provides standard language that DHS components may incorporate into their notices. As of February 2007, the Privacy Office had approved and published 56 system-of-records notices, including updates and revisions as well as new documents.

However, the Privacy Office has not yet established a process for conducting a biennial review of system-of-records notices, as required by OMB. OMB Circular A-130 directs federal agencies to review their notices

[28]OMB, *Management of Federal Information Resources*, Circular A-130, Appendix I (Nov. 28, 2000).

biennially to ensure that they accurately describe all systems of records. Where changes are needed, the agencies are to publish amended notices in the Federal Register.[29]

The establishment of DHS involved the consolidation of a number of preexisting agencies, thus, there are a substantial number of systems that are operating under preexisting, or "legacy," system-of-records notices—218, as of February 2007.[30] These documents may not reflect changes that have occurred since they were prepared. For example, the system-of-records notice for the Treasury Enforcement and Communication System has not been updated to reflect changes in how personal information is used that has occurred since the system was taken over by DHS from the Department of the Treasury.

The Privacy Office acknowledges that identifying, coordinating, and updating legacy system-of-records notices is the biggest challenge it faces in ensuring DHS compliance with the Privacy Act. Because it focused its initial efforts on PIAs and gave priority to DHS systems of records that were not covered by preexisting notices, the office did not give the same priority to performing a comprehensive review of existing notices. According to Privacy Office officials, the office is encouraging DHS components to update legacy system-of-records notices and is developing new guidance intended to be more closely integrated with its PIA guidance. However, no significant reduction has yet been made in the number of legacy system-of-records notices that need to be updated.

By not reviewing notices biennially, the department is not in compliance with OMB direction. Further, by not keeping its notices up-to-date, DHS hinders the public's ability to understand the nature of DHS systems-of-records notices and how their personal information is being used and protected. Inaccurate system-of-records notices may make it difficult for individuals to determine whether their information is being used in a way that is incompatible with the purpose for which it was originally collected.

[29]OMB gives agencies the option to publish one annual comprehensive publication consolidating minor changes.

[30]These DHS system-of-records are covered by preexisting notices through the operation of a savings provision in the Homeland Security Act of 2002. 6 U.S.C. § 552.

Privacy Office Has Generally Not Issued Reports in a Timely Fashion

Section 222 of the Homeland Security Act requires that the Privacy Officer report annually to Congress on "activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters." The act does not prescribe a deadline for submission of these reports; however, the requirement to report "on an annual basis" suggests that each report should cover a 1-year time period and that subsequent annual reports should be provided to Congress 1 year after the previous report was submitted. Congress has also required that the Privacy Office report on specific departmental activities and programs, including data mining and passenger prescreening programs. In addition, the first Chief Privacy Officer initiated several investigations and prepared reports on them to address requirements to report on complaints of privacy violations and to assure that technologies sustain and do not erode privacy protections.

In addition to satisfying legal requirements, the issuance of timely public reports helps in adhering to the fair information practices, which the Privacy Office has pledged to support. Public reports address openness—the principle that the public should be informed about privacy policies and practices and that individuals should have a ready means of learning about the use of personal information—and the accountability principle—that individuals controlling the collection or use of personal information should be accountable for taking steps to ensure implementation of the fair information principles.

The Privacy Office has not been timely and in one case has been incomplete in addressing its requirement to report annually to Congress. The Privacy Office's first annual report, issued in February 2005, covered 14 months from April 2003 through June 2004. A second annual report, for the next 12 months, was never issued. Instead, information about that period was combined with information about the next 12-month period, and a single report was issued in November 2006 covering the office's activities from July 2004 through July 2006. While this report generally addressed the content specified by the Homeland Security Act, it did not include the required description of complaints of privacy violations.

Other reports produced by the Privacy Office have not met statutory deadlines or have been issued long after privacy concerns had been addressed. For example, although Congress required a report on the privacy and civil liberties effects of the No-Fly and Automatic Selectee

Lists[31] by June 2005, the report was not issued until April 2006, nearly a year late. In addition, although required by December 2005, the Privacy Office's report on DHS data mining activities was not provided to Congress until July 2006 and was not made available to the public on the Privacy Office Web site until November 2006.

In addition, the first Chief Privacy Officer initiated four investigations of specific programs and produced reports on these reviews. Although two of the four reports were issued in a relatively timely fashion, the other two reports were issued long after privacy concerns had been raised and addressed. For example, a report on the Multi-state Anti-Terrorism Information Exchange program, initiated in response to a complaint by the American Civil Liberties Union submitted in May 2004, was not issued until two and a half years later, long after the program had been terminated. As another example, although drafts of the recommendations contained in the Secure Flight report were shared with TSA staff as early as summer 2005, the report was not released until December 2006, nearly a year and a half later.

According to Privacy Office officials, there are a number of factors contributing to the delayed release of its reports, including time required to consult with affected DHS components as well as the departmental clearance process, which includes the Policy Office, the Office of General Counsel, and the Office of the Secretary. After that, drafts must be sent to OMB for further review. In addition, the Privacy Office did not establish schedules for completing these reports that took into account the time needed for coordination with components or departmental and OMB review.

Regarding the omission of complaints of privacy violations in the latest annual report, Privacy Office officials noted that the report cites previous reports on Secure Flight and the Multi-state Anti-Terrorism Information Exchange program, which were initiated in response to alleged privacy violations, and that during the time period in question there were no additional complaints of privacy violations. However, the report itself provides no specific statements about the status of privacy complaints; it does not state that there were no privacy complaints received.

[31]These lists are used by TSA and CBP for screening airline and cruise line passengers. Individuals on the lists may be denied boarding or selected for additional screening.

Late issuance of reports has a number of negative consequences beyond noncompliance with mandated deadlines. First, the value these reports are intended to provide is reduced when the information contained is no longer timely or relevant. In addition, since these reports serve as a critical window into the operations of the Privacy Office and on DHS programs that make use of personal information, not issuing them in a timely fashion diminishes the office's credibility and can raise questions about the extent to which the office is receiving executive-level attention. For example, delays in releasing the most recent annual report led a number of privacy advocates to question whether the Privacy Office had adequate authority and executive-level support. Congress also voiced this concern in passing the Department of Homeland Security Appropriations Act of 2007, which states that none of the funds made available in the act may be used by any person other than the Privacy Officer to "alter, direct that changes be made to, delay, or prohibit the transmission to Congress" of its annual report.[32] In addition, on January 5, 2007, legislation was introduced entitled "Privacy Officer with Enhanced Rights Act of 2007". This bill, among other things, would provide the Privacy Officer with the authority to report directly to Congress without prior comment or amendment by either OMB or DHS officials who are outside the Privacy Office.[33] Until its reports are issued in a timely fashion, questions about the credibility and authority of the Privacy Office will likely remain.

[32]Section 522, Department of Homeland Security Appropriations Act, 2007 (Pub. L. No. 109-295). The President's signing statement to that act stated, among other things, "the executive branch shall construe section 522 of the act, relating to privacy officer reports, in a manner consistent with the President's constitutional authority to supervise the unitary executive branch."

[33]The Privacy Officer with Enhanced Rights Act was introduced as Subtitle B of Title VIII of H.R. 1, "Implementing the 9/11 Commission Recommendations Act of 2007," introduced on January 5, 2007. This bill would also grant the Privacy Officer investigative authority, including subpoena power.

Implementation of GAO Recommendations Would Lead to Improvements in Privacy Office Operations

In order to ensure that Privacy Act notices reflect current DHS activities and to help the Privacy Office meet its obligations and issue reports in a timely manner, in our report we recommended that the Secretary of Homeland Security take the following four actions:

1. Designate full-time privacy officers at key DHS components, such as Customs and Border Protection, the U.S. Coast Guard, Immigration and Customs Enforcement, and the Federal Emergency Management Agency.

2. Implement a department-wide process for the biennial review of system-of-records notices, as required by OMB.

3. Establish a schedule for the timely issuance of Privacy Office reports (including annual reports), which appropriately consider all aspects of report development, including departmental clearance.

4. Ensure that the Privacy Office's annual reports to Congress contain a specific discussion of complaints of privacy violations, as required by law.

Concerning our recommendation that it designate full-time privacy officers in key departmental components, DHS noted in comments on a draft of our report that the recommendation was consistent with a departmental management directive on compliance with the Privacy Act and stated that it would take the recommendation "under advisement." However, according to Privacy Office officials, as of July 2007, no such designations have been made. Until DHS appoints such officers, the Privacy Office will not benefit from their potential to help speed the processing of PIAs, nor will component programs be in a position to benefit from the privacy expertise these officials could provide.

DHS concurred with the other three recommendations and noted actions initiated to address them. Specifically, regarding our recommendation that DHS implement a process for the biennial review of system-of-records notices required by OMB, DHS noted that it is systematically reviewing legacy system-of-records notices in order to issue updated notices on a schedule that gives priority to systems with the most sensitive personally identifiable information. DHS also noted that the Privacy Office is to issue an updated system-of-records notice guide by the end of fiscal year 2007. As of July 2007, DHS officials reported that they have 215 legacy SORNs that need to be reviewed and either revised or retired. Until DHS reviews and updates all of its legacy notices as required by federal guidance, it

cannot assure the public that its notices reflect current uses and protections of personal information.

Concerning our recommendations related to timely reporting, DHS stated that the Privacy Office will work with necessary components and programs affected by its reports to provide for both full collaboration and coordination within DHS. Finally, regarding our recommendation that the Privacy Office's annual reports contain a specific discussion of privacy complaints, as required by law, DHS agreed that a consolidated reporting structure for privacy complaints within the annual report would assist in assuring Congress and the public that the Privacy Office is addressing the complaints that it receives.

In summary, the DHS Privacy Office has made significant progress in implementing its statutory responsibilities under the Homeland Security Act; however, more work remains to be accomplished. The office has made great strides in implementing a process for developing PIAs, contributing to greater output over time and higher quality assessments. The Privacy Office has also provided the opportunity for privacy to be considered at key stages in systems development by incorporating PIA requirements into existing management processes. The office faces continuing challenges in reducing its backlog of systems requiring PIAs, ensuring that system-of-records notices are kept up to date, and in issuing reports in a timely fashion.

Mr. Chairman, this concludes my testimony today. I would be happy to answer any questions you or other members of the subcommittee may have.

Contacts and Acknowledgments

If you have any questions concerning this testimony, please contact Linda Koontz, Director, Information Management, at (202) 512-6240, or koontzl@gao.gov. Other individuals who made key contributions include John de Ferrari, Nancy Glover, Anthony Molet, David Plocher, and Jamie Pressman.

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Ms. SÁNCHEZ. Thank you, Ms. Koontz.

We will now proceed to our first round of questioning. Members will have 5 minutes to ask witnesses questions. We ask that you remain mindful of the time constraints that we are working under.

I will begin by recognizing myself for 5 minutes.

Mr. Davis, I am interested in your testimony because you were very clear about people working with correct motives in terms of the work the board was trying to accomplish, and yet you also mentioned an instance in which there were deletions made in the report for what you termed political reasons.

How can you reconcile the two statements that you just made because it sort of seems inherent that if deletions were made for political reasons, there perhaps weren't always the purest of motives?

Mr. DAVIS. Well, I worked in the Clinton White House, and if an office of the Clinton White House were putting something out on its own without getting permission from the chief of staff or the press secretary and it happened to be a message that was out of political sync with what the Clinton White House wanted, the White House office would not be permitted to do that.

It would have to go through the press secretary, the Office of Management and Budget, the White House chief of staff. The White House is an organization that has a hierarchy, so one doesn't just put out public statements that may be out of sync with what the President or the White House's critical message is. That is perfectly appropriate.

That is what happened. Our report was viewed as simply an expression of a White House agency that needed to be cleared by various political substantive and bureaucratic methods that are very, very consistent with being treated as a White House office.

When I accepted the job, I understood there was a hybrid trying to be accomplished, putting us in the White House as an office of the President, but trying to give us independent oversight authority. And I recognized ultimately the-square-peg-in-the-round-hole concept simply did not work, and that is why I resigned.

Ms. SÁNCHEZ. Okay. I am interested in knowing then what you think that Congress could do to address the inherent tension involved in the somewhat questionable independence of the board when it provides oversight of the executive branch, while at the same time being part of the Executive Office of the President.

Mr. DAVIS. Well, I changed my mind on this. I agreed with Alan, and we spoke to Senator Lieberman and Senator Collins and recommended that the office be kept within the White House but be granted investigative special independent powers, and that was our hope.

When I saw what happened to our report and I recognized the bureaucratic, political and institutional pressures of being part of the White House, it was just too much to ask the White House not to act like the White House and treat us as an office of the White House.

At one point, we did send a memo to the President, or tried to, in which we asked the President to issue an executive order that basically could be summarized by three words, "Leave them alone." And that memo to the President and that executive order was never issued.

I do believe the new approach does better guarantee independence. I hope that Alan Raul and his concerns and others' concerns, including myself, can be overcome by allowing the independent agency that would be the result of the legislation that I now understand is being considered to have the same access that we did, which was phenomenal access and which did lead me to some of the positive conclusions, for example, about the surveillance program in its execution that Congressman Cannon referred to.

I had doubts, Congressman, which I would like to get into about the constitutional and legal validity of that program, which I now feel better about, now that they have FISA court approval. But the execution of the program and the people at the NSA executing it impressed me greatly as sensitive to civil liberties and privacy rights.

Ms. SÁNCHEZ. Let me ask you this. I am interested in having you explain why the brief statement on the national security letter abuses by the FBI was relegated to the cover letter of the board's first annual report to Congress and not included in the extensive discussion of that report. It seems to me that that is a pretty significant issue that——

Mr. DAVIS. I have a terrific personal angst about that topic, especially the man I am sitting next to who backed me up and also believed that the national security letter violations were egregious, of great concern, and to this day to me reflected an FBI out of control that had officers in the field violating the law with no effective oversight and to this day have great concern.

For reasons that were beyond my comprehension, we set a date for March 1 of that report, and the I.G. report on the NSL letters came out in the middle of March. I wanted to include our critical comments about the national security letter abuses since it was so critical in our report, since it wasn't due to the end of the month, and we had great resistance to doing that.

The compromise, thanks to Alan's support of my position and my support of Alan's position, was to put it in the cover letter to the report where we were critical, but not in the report itself, something that to this day I still have never been able to understand.

Ms. SÁNCHEZ. Well, thank you for your frankness.

And at this time, my time has expired. I would like to recognize Mr. Cannon for 5 minutes of questioning.

Mr. CANNON. Thank you, Madam Chair.

Mr. Raul, do you agree with how Mr. Davis characterized your views to be?

Mr. RAUL. Yes, for the most part. We had extensive discussions over the substance of the violations by the FBI not complying with the legal requirements for issuance of national security letters. We also, I think, were relatively congruent in our views about the importance of publicizing that in an important forum.

So the question really became: Was it going to be in the body of the report, in the cover letter, or in an independent statement that would be issued to the press and on our Web site? The key point, though, is that we did make the substantive criticisms publicly.

Mr. CANNON. And it seems to me that the cover letter would be really the place to do that.

Mr. RAUL. It had a prominence in the cover letter that it might have lost if it was in the body of it, but all the members of the board were agreed that it was important for the board to make a statement on this very important sensitive and not well-handled matter by the Federal Bureau of Investigation.

Mr. CANNON. The important thing is how we make this office work or this board work better in the future.

But can I just clarify one thing, Mr. Davis? In the final report, the piece that you objected to on the material witnesses was actually included in the report. I take it that is because you objected and then it went back in.

Mr. DAVIS. Yes, that and a number of other deletions that were in the section called "the year ahead." And it was thanks to Fred Fielding and my going to Fred Fielding and his backing me up and I must say Alan Raul's support for returning those deletions that they were put back in. Most of them were put back in, not all.

Mr. CANNON. I am personally a big fan of Fred Fielding.

Mr. DAVIS. Me, too.

Mr. CANNON. One of the bright stars out there.

Let me just talk a little bit about your function and our function here, and then I want to take it back to the two of you to talk about where we should go, what we need to do, and this is where I have been out of sync with Republicans for the 10 or the 12 years they were in the majority.

I think that Congress has an obligation to oversee. When Republicans took over, they had this idea that we would show the world that we could cut our own budget and, therefore, the rest of the agencies can do it as well, and we actually in fact cut spending. We did not cut the rate of growth of spending. We actually cut spending in 1996, the next cycle that the first Republican majority was in charge of, and that was a remarkable thing and I think the foundation for the huge growth we have had in our economy.

I think that is very important, but at the same time, what we did was cut our budget by eliminating the oversight folks. Now the vast majority of what the Administration does, it does based upon laws and mandates, and there is very little discretion on the part of the President. But, on the other hand, when something goes wrong, the President of whichever party gets all the blame, and I think that is actually very counterproductive in our society.

So I think—and I express this to my colleagues here—that we ought to be much more robust in oversight, in part because we have given mandates to the Administration. We ought to be making sure those happen, and whether that conflicts with the President, whether we are critical of even a political appointee or otherwise, ultimately, the country is better served by that sort of thing.

Now you have spoken eloquently, Mr. Davis, about the square peg in the round hole and how this doesn't work, and, on the other hand, it may have been fixed with an executive order saying, "Let them be."

And I take it, Mr. Raul, you would like to see this remain in the White House because of the kind of access it gets. Would you mind talking a little bit about what you think of where it appears we are headed on the board?

And then, Mr. Davis, if you would respond?

And then, Mr. Raul, if you would follow up and——

Mr. RAUL. Yes, Mr. Cannon, thank you. I would love to address that.

Let me preface my remarks here with what my views on this are for myself. I am a member of a collegial board of four members now, so I will express my views and not necessarily those of the chair or the full board.

There is a distinction between the Executive Office of the President and the White House office. Colloquially, we refer to them the same, but the Executive Office of the President is a broader constellation of units that work directly for the President and serve the presidency but are not within the immediate staff of the White House. So the Executive Office of the President has, in addition to the White House office, OMB, the U.S. Trade Representative's office, and, you know, other offices, Council on Environmental Quality and so on.

The original legislation, the Intelligence Reform and Terrorism Prevention Act, established the privacy board in the Executive Office of the President. Congress then proceeded to appropriate funds for the board to the White House office. So there was a bit of a mismatch that occurred right then and there.

As part of the Executive Office of the President, we have had access to anybody that we have sought access to with an ability to obtain information and exchange views on the most candid, free-flowing basis. Really, I think it is fair to say almost without any reservations or inhibitions.

If the board, as it appears will be the case, is taken out of the Executive Office of the President, put at arm's length from the executive branch, although part of the executive branch, we will have an inspector general type situation in contrast with the privacy and civil liberties officer type situation.

We have heard Ms. Koontz in her testimony say that one of the positive attributes of Mr. Teufel's office is that it is increasingly able, as I heard her say and as I understand it, to become involved in the development of policy early. That is different from a function that the inspector general plays and different from the function that Congress and its oversight function would play in judging whether the Administration has carried out the laws faithfully.

Ms. SÁNCHEZ. The time of the gentleman has expired.

At this time, I would like to recognize Mr. Conyers for 5 minutes.

Mr. CONYERS. Thank you, Madam Chairman.

I appreciate the witnesses' testimony.

I am so glad that we have talked about the national security letters. The head of the Federal Bureau of Investigation, Mr. Mueller, will be before us in 2 days, and we have the same concerns that you have already expressed, and so I thank you both for raising that.

And I compliment Attorney Raul for working as closely as he did in many instances with Lanny Davis.

Mr. RAUL. Thank you.

Mr. CONYERS. That gives me hope.

Now, just to get one matter out of the way, Mr. Teufel, we received this report. It came into the staff's office at about 9:30 this morning.

Mr. TEUFEL. Yes, sir.

Mr. CONYERS. As far as I know, nobody has been able to read it. We don't know what is inside it. And you knew you were going to be a witness. Couldn't this have arrived maybe 24 hours earlier?

Mr. TEUFEL. It could have, sir, and I would be happy to come and speak with you and your staff about the report and all the time that you would like to talk about it, sir.

Mr. CONYERS. And if we held another hearing for that, would you come to that?

Mr. TEUFEL. Absolutely, sir. At your convenience.

Mr. CONYERS. Well, my convenience would have been that you delivered it a day earlier.

Mr. TEUFEL. Yes, sir.

Mr. CONYERS. We could do it here.

Mr. TEUFEL. Yes, sir.

Mr. CONYERS. I mean, we are holding a hearing right now.

Mr. TEUFEL. Yes, sir.

Mr. CONYERS. So what is in the report, just real quickly? I mean, what can you say about the report in a sentence or two?

Mr. TEUFEL. Well, in a sentence or two, sir, ADVISE is a tool that the Science and Technology Directorate came up with. It is a tool for making clearer links between data or among data.

Mr. CONYERS. Okay, stop.

Mr. TEUFEL. Yes, sir.

Mr. CONYERS. I can see under the 5-minute rule that we are not going to get very far down the line here.

Now, Lanny Davis, I would like to know what you think of the situation that exists right now. We have a whole string of problems inside the United States that deal with constitutional discretion, abuses of the executive power. We can hardly get anything here.

We actually had the Republican National Committee raising executive privilege as a reason they could not give us documents. They dropped it. It was too ludicrous. I guess nobody could take that, a political party claiming presidential privilege.

But we have a whole string of problems here, and I would like you to comment on whether you see them as serious and as complicated that it would lead me and Chris Cannon both to quote Alexander Hamilton.

Mr. DAVIS. I tried to be consistent with how I felt in the Clinton White House when I felt congressional oversight and subpoenas were being abused for political purposes, and the assertion of executive privilege to us made sense when we thought that Congress was abusing its investigatory powers for partisan purposes.

So there is an institutional perspective from a separate branch of government called the White House and executive branch when Congress appears to be overly intrusive.

Mr. CONYERS. Whoa. You——

Mr. DAVIS. On the other hand, I have great concerns that this Administration and this White House have so far gone in the other direction that they appear to define executive power as completely regardless of congressional oversight responsibilities, to the point where I believe that the NSA program itself was launched and implemented, and several years later, somebody finally caught up in

the Justice Department that we need legal authority to do what we are doing.

And they got the legal authority in a very creative and, I thought, legally correct fashion, but why 3 or 4 years after beginning the surveillance program? Why not do it right away? And I think that flows from an assumption among some people in this particular White House that there is something called the unitary presidency. Whatever that means, it means we are the only branch of government that counts.

So the pendulum appeared to me, while I was there in the White House, to have swung too far in one direction of congressional abuse of investigatory oversight authority. Now appears to have swung too far in the direction of ignoring congressional legitimate oversight—subpoenas, requests for documents, requests for testimony.

If the Clinton White House had ever said, with all due respect, to Congressman Burton, "You can interview us, but not under oath, no transcript, and we are not going to appear in front of you," my good friend, Congressman Chris Cannon, on "Crossfire" that night would have killed me. You have to be kidding me? Not under oath, no transcript, and you expect that to satisfy congressional oversight?

And the deafening silence of this particular Congress, Republican and Democratic, to the notion that somebody should be interviewed by the Congress and no transcript, put aside not under oath, to me strikes me as the pendulum going too far.

But I do hope that Democrats will be intellectually consistent and grant that there is a proper assertion of executive privilege when the subpoena power and congressional investigations go too far.

Ms. SÁNCHEZ. The time of the gentleman has expired.

Mr. DAVIS. Sorry to speak so long.

Mr. CONYERS. No, I thank you. And I don't have any time for questions, but I want to assure you that the 7 months of this Committee's existence, the Judiciary Committee, we have been very careful about politicizing or turning into a partisan endeavor or some wide search for information far beyond our oversight capacity. And so I thank you for your comments.

Ms. SÁNCHEZ. I thank the gentleman.

The gentleman from Arizona, Mr. Franks, is recognized for 5 minutes for questioning.

Mr. FRANKS. Thank you, Madam Chair.

I thank all of you for coming here.

Again, I would like to express my personal appreciation, Mr. Davis, too. It is not so often that someone is so eloquent in what seems to be a genuine attitude of bipartisanship and a commitment to——

Mr. DAVIS. Thank you.

Mr. FRANKS [continuing]. Saying what they believe in an unbiased fashion, even if there might be some of us that take issue with some of it.

Mr. Teufel, how would you characterize the interaction between your office and the Privacy and Civil Liberties Oversight Board?

And do you think that relationship would improve or deteriorate if the board was taken out of the White House?

Mr. TEUFEL. Well, sir, I would describe the relationship as a very good one. The relationship is on two levels.

First is at the working level, and by that I mean that my colleague at the department, Dan Sutherland, the civil rights and civil liberties officer, and I regularly meet with Mark Robbins, who is executive director for the Privacy and Civil Liberties Oversight Board; Alex Joel who is the privacy and civil liberties officer at OD&I; and Jane Horvath at Department of Justice; and other privacy officers. And so we meet and talk fairly regularly about issues.

And then also in the more formal sense that my office interacts with the Privacy and Civil Liberties Oversight Board, the secretary and I have spoken to the board on a couple of occasions, and we routinely make available information to the board at its request whenever it wants to know something about what we are doing or what the department is doing. So we have a very good relationship.

I am not sure what the differences would be if the office were moved outside of the White House. I think my concern would probably be that there might be a change, and it might be a more adversarial relationship generally between the new office and the executive branch. But, sir, I just cannot tell you. I don't know.

Mr. FRANKS. If you were to point to the greatest single achievement that your office has had and perhaps even go further and tell us what you think the best way to improve the office would be in just an overall fashion, I might pose that to some of the other members as well.

Mr. TEUFEL. Well, sir, the best thing to improve the office would be within the President's budget, there is a request for funding for additional slots within the office. My office is responsible for Freedom of Information and also Privacy Act compliance, System of Records Notices and Privacy Impact Assessments, and the President's budget asks for additional folks to assist in those areas. I have 211 legacy agency System of Records Notices that I have, and I am determined before I leave to review and get up to date, and we could use the help.

In terms of what I have done so far, it is further infusing the culture of privacy within the department and helping to regularize our approach to work product. We still, as Chairman Conyers noted, have a long ways to go with respect to reports, but we are making great improvements in terms of getting out reports.

I just looked at our draft annual report for this last year, July to July, and read through it, gave my comments to my staff, and we are going to get it through the review process and get it out and up to Congress in September.

So that is what I would say in answer to your question, sir.

Mr. FRANKS. You know, as a political appointee, when an Administration's in its last couple of years, I think you have 18 months left. It is always kind of a challenging question, I know, but what do you plan to do with the remaining 18 months that you have in office?

Mr. TEUFEL. Work on the recommendations of the GAO report, get the remaining 211 legacy agency System of Records Notices up to date, continue to do the good work of the department, and I have

no plans over the next 18 months. Unless the National Guard deploys me, I will be here at the job, sir.

Mr. FRANKS. Would anyone else on the panel like to take a shot at what do you think would be the most significant thing that could be done to improve the office and its function?

Yes, ma'am?

Ms. KOONTZ. I would just like to underscore a couple of our recommendations.

Two of the biggest challenges that the privacy office faces is, number one, the reporting issue. The reports have taken a long time for them to be finalized, although there seems to be some improvement more recently, and I think that putting some more discipline around that review process could help speed up the issuance of those reports, and it sounds like some of the things that Mr. Teufel is doing may help in that regard.

I would think secondly the public notices that are supposed to be issued on the Privacy Act, they have a huge workload ahead of them, and one of the things that we thought would help that, actually, the privacy office originally recommended as well, and that is establishing privacy officers in certain of the key components in DHS to help speed along this process.

So I look forward to working with them on implementing those recommendations.

Mr. FRANKS. Thank you, all.

Thank you, Madam Chair.

Ms. SÁNCHEZ. The time of the gentleman has expired.

The gentleman from North Carolina, Mr. Watt, is recognized for 5 minutes.

Mr. WATT. Thank you, Madam Chair.

And let me first apologize to the witnesses for not being present to hear their testimony. Unfortunately, I had, as we often do, two or three different places, all important, to be in at the same time.

And I especially want to apologize to my good friend and former classmate, Lanny Davis—we go back a long way—and applaud, as he has already been applauded, his willingness to speak appropriate positions that he believes in, regardless of which way they cut politically.

It is that point that I would like to focus on first and maybe then pick up a second point if we can get this one, and that is the distinction between what our Committee has been pursuing with this Administration and the way in which some of the oversight was done in the last Administration.

Am I correct that it got to a point with the last Administration that Congress was or at least one of the Committees was actually issuing subpoenas before they even contacted the agencies to request certain information?

Mr. DAVIS. Yes. At the Clinton White House, we were accustomed to receiving subpoenas even before a request for documents and a negotiation, which is traditionally the way it is done, and we were accustomed at times to try to negotiate something short of the subpoena because they were usually very broad and sometimes would require emptying all the file cabinets of the White House for fear that if you missed one piece of paper, you would be in an obstruction of justice charge.

So we were frequently concerned about the premature issuance of subpoenas, but we never would have conceived of defying one. We frequently fantasized about it, but we never actually did it.

Mr. WATT. What are some of the other distinctions that you would draw? I am not trying to draw you into an endorsement of our process versus what was happening in the last Administration with congressional oversight, but what are some of the other distinctions that we might be alert to in trying to make sure that we stay far from the line where we appear to be being on some partisan endeavor as opposed to the genuine business of oversight?

Mr. DAVIS. I think conversations and communications between staff and the President would be something, whether I am a Democrat or a Republican, I would be very sensitive to, even if it is a politically attractive issue. And I am referring to the U.S. attorneys issue, which I think there really is serious potential wrongdoing that causes me concern, and congressional oversight, I think, is necessary.

Still, communications between individuals and the President would, to me, be a line to draw.

Mr. WATT. But if there are people on record as saying that the President had no involvement with a particular issue, would that seem to be a sufficient basis for discounting that as a major factor?

Mr. DAVIS. I think the Justice Department has an obligation to disclose everything there is to be disclosed about communications between the Justice Department and the White House on that issue because there is serious possible impropriety.

I draw the line about White House staff communicating with the President. We were very sensitive to those requests for documents for testimony involving communications with the President, but, having said that, Congressman Watt, we ultimately surrendered and after fighting a while, we ended up saying to ourselves, "Why fight if we are going to give up? This is a transparent process we are in. Congress is going to continue to insist that we do this." And we ended up giving it up.

Mr. WATT. Before my red light goes off, let me see if I can shift to the second area because it strikes me that the Privacy and Civil Liberties Oversight Board is kind of to the executive branch the equivalent of what a privacy office would be in a particular agency.

Is that an accurate assessment, and if so, how have the agencies themselves avoided the same kind of potential conflicts that gave rise to your resignation?

Mr. DAVIS. The big difference—and it goes back to Congressman Cannon and I in our conversation—is we were a creation of the Congress and the word "oversight" was put into our name and the legislative history required us to report to Congress and to do oversight.

The privacy officers are supposed to be internal as watchdogs within the agency, but the word "oversight," to me at least and I believe to my colleagues, meant that we could be critical and a public critic, if necessary, to the Congress as a public entity, not a private agency as staff to the President, but a public accountability doing oversight, and that is where the square-peg-and-the-round-hole problem occurred.

Ms. SÁNCHEZ. The time of the gentleman has expired.

Mr. WATT. Thank you, Madam Chair.

Ms. SÁNCHEZ. Thank you.

I have been informed that we have a couple of outstanding questions, so I am going to ask unanimous consent that I be allowed 2 more minutes for questioning.

And, without objection, so ordered.

Mr. WATT. Can I reserve the right to object just long enough to inquire, does that mean that we are doing another round of 2 minutes each?

Ms. SÁNCHEZ. We were trying to avoid doing a second round of 5 minutes each. I have a very brief question I would like to ask.

Mr. WATT. What about 2 minutes each?

Ms. SÁNCHEZ. If there is no objection.

Mr. CANNON. I would have no objection to the gentleman taking an additional 2 minutes.

Ms. SÁNCHEZ. We will do them all. Does that satisfy the gentleman from North Carolina?

Mr. WATT. Yes, Madam Chair.

Ms. SÁNCHEZ. Okay.

Mr. Raul, page 22 of the board's first annual report to Congress states that, "In order to maximize the board's effectiveness and to prevent the diffusion of its limited resources across too many programs, the board has elected to concentrate on the United States and U.S. persons." Footnote 46 on page 22 of the report, however, notes that the board may revisit that determination.

Is the reason that the board chooses to limit its scope because of funding or because of some other reason? Do you know?

Mr. RAUL. It was our view that nothing in the statute, Intelligence Reform and Terrorism Prevention Act, or legislative history or any of the comments of the 9/11 Commission, which was one of the entities that recommended the creation of a board like ours, had focused on extraterritorial impacts. The focus was on the American way of life, privacy and civil liberties for Americans. So I think that we had a robust debate internally after substantial legal analysis as to what was required and what was permitted.

Speaking for myself of what my view of both the law is and of our decision on this point, we felt that it was not entirely clear that the board was authorized or precluded from considering international or non-domestic issues, as privacy and civil liberties might affect non-U.S. persons. So we thought that it was possible that we had the authority to go in that direction, but not required.

Ms. SÁNCHEZ. Do you think it would make sense if Congress wanted to, for example, review civil liberties questions raised by detainees at Guantanamo and to meet the mission and mandate of the Intelligence Reform and Terrorism Prevention Act of 2004 that it should express a legislative mandate for the board to review those areas? Would that help clarify some of the confusion?

Mr. RAUL. Well, that would certainly clarify the confusion. Whether it would be prudent to do so is a question that I leave to you, and if it gets to the President, the President. Obviously, where you trench upon commander in chief and foreign affairs responsibilities, a different set of constitutional considerations come into play, but I would certainly agree with you, Madam Chairwoman, that it would clarify the confusion or uncertainty.

Mr. DAVIS. Could I just add 30 seconds? There was a good debate on this issue, and my personal opinion was that when an American citizen under the power of our government snatches somebody in a rendition and puts them in prison in Syria and tortures them, it doesn't matter to me whether that individual is an American citizen or a non-American citizen. That is a matter that our American values have been compromised, and the board should be looking into that.

So we had a disagreement on that, Guantanamo and other issues, and the sentence you just read was the compromise that we focus on the word "priorities," but there was serious disagreement about whether Congress intended us to be worried about American government officials doing that to non-American citizens, and we did—I think Alan is right—think the Congress should have been much clearer in mandating whether they wanted us to do that.

Ms. SÁNCHEZ. Thank you, Mr. Davis.

I understand that the gentleman from Michigan seeks to be recognized.

Mr. CONYERS. Yes, I ask unanimous consent to proceed for a few minutes.

Ms. SÁNCHEZ. Without objection, so ordered.

Mr. CONYERS. Thank you.

I am so glad that this issue was raised by yourself, Chairwoman Sánchez, because I wanted to put in the record an examination of the President's executive order of last Friday in which he issued an executive order supposedly clearing up the question of the condemnation of torture in this country. As David Cole points, it was full of loopholes and cleared up little or nothing. And I ask unanimous consent to put it in the record.

Ms. SÁNCHEZ. Without objection, so ordered.

[The information referred to follows:]

- War Room
WEEKLY
- Ask the Pilot
- Beyond the Multiplex
- Sidney Blumenthal

Join Salon.com today | Help Benefits of membership

salon.com

Site Pass

SITE PRESENTED BY WITHOUT PREJUDICE?

Search Go! Salon The Web powered by YAHOO! SEARCH

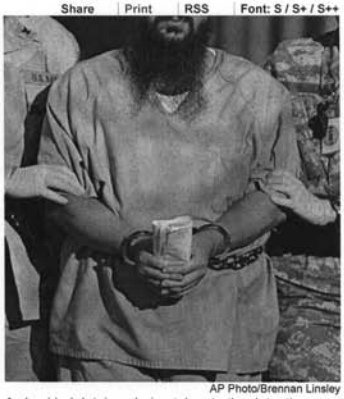
A&E Books Comics Community Life Movies News & Politics Opinion Sports Tech & Business

Bush's torture ban is full of loopholes

The president has issued an executive order to stop the CIA from using torture, but the ban is unenforceable.

By David Cole

Share | Print | RSS | Font: S / S+ / S++



AP Photo/Brennan Linsley

A shackled detainee being taken to the detention center at Guantánamo Bay, Cuba, Dec. 6, 2006.

July 23, 2007 | Once upon a time, a U.S. official's condemnation of torture was a statement of moral principle. Today, it is an opportunity for obfuscation. We have learned that when President Bush says, "We don't torture," it's important to read the fine print. So it was once again on July 20, when Bush issued a long-awaited executive order purporting to regulate interrogation tactics used by the CIA in the "war on terror." According to a White House press release, the order provides "clear rules" to implement the Geneva Conventions governing treatment of detainees in wartime -- rules the administration insisted did not even apply to the "war on terror" until the Supreme Court ruled otherwise last summer. But while the new rules reflect a significant retreat by the administration from its initial torture policies, they are anything but "clear," come far too late in the day, and in any event are unenforceable.

The executive order prohibits the CIA from using torture and cruel, inhuman and degrading treatment, sexual abuse, denigration of religion and serious "acts of violence" in its interrogations. While one might have thought that the

impermissibility of such tactics in official U.S. interrogations would go without saying, it has not been so since 9/11. This is an administration that narrowly defined "torture" to permit the use of sexual abuse, stress positions, injecting suspects with intravenous fluids until they urinate on themselves, prolonged sleep deprivation, exposure to extreme heat and cold and "waterboarding," i.e., simulated drowning. This is an administration that adopted as official legal policy the counterintuitive and deeply immoral position that international law's ban on "cruel, inhuman and degrading treatment" did not apply to foreigners held by the U.S. outside U.S. borders. And this is an administration that opined that the president could order torture itself if he so chose as a way of "engaging the enemy," notwithstanding a federal criminal statute and ratified treaty banning torture under all circumstances, including war.

In light of that history, an executive order that categorically bans torture and cruel, inhuman and degrading treatment is a significant step in the right direction. And make no mistake -- the administration would never have taken this step of its own accord. President Bush was forced to act by a combination of the Abu Ghraib photographs, international and domestic condemnation of the administration's torture tactics, Congress' overwhelming and veto-proof repudiation of the administration's interpretation of "cruel, inhuman and degrading treatment," and the Supreme Court's rejection of the contention that the Geneva Conventions do not apply to the conflict with al-Qaida.

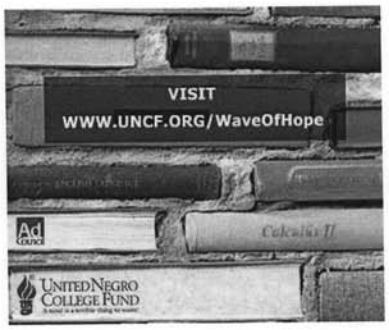
But how much of a step the administration has really taken remains a serious question. The actual tactics the CIA is authorized to use remain classified, based on the bogus claim that agency interrogators need to keep detainees guessing about how far they can go in order to interrogate effectively. The Army, by contrast, has set forth for the world to see the specific tactics its interrogators can employ -- in the Army Field Manual. And of course, it is black-letter law that no use or threat of physical force is permissible for state and federal police interrogations. Yet both the Army and domestic police obtain useful information from interrogations every day. The limits do not need to be secret for interrogation to be effective.

While the executive order flatly forbids torture and cruel, inhuman and degrading treatment, its failure to specify permissible and impermissible techniques seems designed to leave the CIA wiggle room. A prohibition on "acts of violence," for example, applies only to those violent acts "serious enough to be considered comparable to murder, torture, mutilation, and cruel or inhuman treatment," as defined by the Military Commissions Act. The MCA, in turn, limits "cruel and inhuman treatment" to the infliction of bodily injury that entails: "(i) a substantial risk of death; (ii) extreme physical pain; (iii) a burn or physical disfigurement of a serious nature (other than cuts, abrasions, or bruises); or (iv) significant loss or impairment of the function of a bodily member, organ, or mental faculty." In other words, the president's order appears to permit cutting or bruising a suspect so long as the injury does not risk death, significant functional impairment or "extreme physical pain," an entirely subjective term.

Similarly, the order prohibits "willful and outrageous acts of personal abuse done for the purpose of humiliation or degrading the individuals in a manner so

serious that any reasonable person, considering the circumstances, would deem the acts to be beyond the bounds of human decency." But this implies that it is permissible to inflict any abuse that is willful but not outrageous, or that is done for a purpose other than humiliation or degradation, or that a single reasonable person might consider within the bounds of decency under the circumstances. Whatever else one might say, these are hardly "clear rules."

The executive order's most revealing words come at the end. Its final section states that the order creates no rights enforceable by any victim against the United States or its employees, while expressly offering CIA employees a defense against any attempt to hold them liable for abuse. The ultimate purpose of the law, in other words, is to protect the potential perpetrators, not the potential victims.



Nor is there any mechanism for enforcement *outside* the courts. The International Committee for the Red Cross ordinarily monitors treatment of detainees, and this oversight has historically been a critical safeguard against abuse. But this order applies to interrogation at CIA "black sites," secret prisons into which suspects are "disappeared" for years at a time, and from which the United States has barred the Red Cross or any other outside monitor. "Disappearances" are themselves a fundamental violation of international human rights, in large part because they facilitate abuse, yet this order allows that practice to continue unabated.

With a different administration and a different history, one might be less inclined to read President Bush's latest executive order so skeptically. But this administration has shown repeatedly that it approaches the prohibitions on coercive interrogation the way a particularly creative tax lawyer might treat the tax code. Instead of striving to uphold what we thought were our country's moral principles, the Bush administration seeks to exploit every loophole it can find or manufacture. As a result, the administration has lost the trust of the nation and of the rest of the world. Executive orders like this one are not likely to win it back.

Share | Print | RSS | Font: S / S+ / S++

POST A LETTER ABOUT THIS ARTICLE

Read all letters on this article (8)

Read Editor's Choice letters on this article (4)

Mr. CONYERS. The main question, though, is to our GAO representative, Ms. Koontz. What are these four recommendations that you boiled your testimony down, plus the observation that the privacy office hasn't been timely in issuing public reports, potentially limiting their value and impact.

If you are not well-read in this kind of language, it seems like administrative, you know, "Let's be neat, let's be on time, fellows." But I suspect there is something far more serious in why you put together a lengthy report that comes to these conclusions.

Ms. KOONTZ. I had hoped our report sounded more powerful than that, but I will give you an example.

There was a report down on the multistate antiterrorism exchange. It was started in 2004 based on an ACLU complaint. It was not issued until 2006. I would say another example would be a data-mining report that was asked under Appropriations Act. It was due in December 2005. It wasn't completed until July 2006, but then not made public until late in that year.

I think in some of these cases, especially in the first one I mentioned, the program had already been terminated well before the report was issued. Our point was that it is not so much bean counting as it was that this was no longer a useful communication with the public, and a large amount of privacy is being transparent with the public, saying what you are doing with citizens' personal information.

Mr. CONYERS. So stalling is a way of obfuscation?

Ms. KOONTZ. It could be.

Ms. SÁNCHEZ. The time of the gentleman has expired.

Mr. WATT. Madam Chair, I ask unanimous consent for a modicum less than a few minutes.

Ms. SÁNCHEZ. You will be granted 2 additional minutes, Mr. Watt.

Mr. WATT. Okay. Well, I was thinking that I would not dare ask for what the Chair of the full Committee asked for, but if I asked for something less than that, I will get it.

Mr. Teufel, just in follow-up to the question that I raised with Mr. Davis, have there been situations in the Homeland Security privacy setting where you have felt either that the people above you in Homeland Security or the Administration have sought to compromise your findings and your efforts to do what you are charged to do?

Mr. TEUFEL. No, sir, I have not. And with respect to reports, I have a very senior career official within my office, and whenever we get ready to issue a report, that senior career official takes the pen. She is incorruptible, she has career protections, and she decides what goes into a report and what doesn't go into a report when we send it around for review. So I have not seen that, and we have not had those issues, sir.

Mr. WATT. The second question I wanted to ask: we spent a lot of time when we were putting this system together debating whether the authority to issue subpoenas was important. What, if anything, have you found on that? I don't know. I mean, I am not trying the program, but for future reference, it would be helpful to know, Mr. Raul, for planning.

Mr. RAUL. Mr. Watt, on the subpoena authority, this is not something that the board has requested or really to date found necessary. As I understand it, the pending legislation——

Mr. WATT. Not that this Administration would honor any of them anyway.

Mr. RAUL. Well, you see, but this is the irony. The subpoena authority that is under discussion, as I understand it, is whether the privacy board can issue subpoenas, and if so, are the subpoenas to be issued to private parties or to other government agencies.

I believe that the language that was in H.R. 1 would have authorized the board to issue subpoenas to private entities and not to the government. That is the way the inspector general statutes were.

I am not sure how essential the issuance of subpoenas to private parties for the executive branch Privacy and Civil Liberties Oversight Board really is, so I think that the issue is perhaps a bit of a tangent for us. We have not found it a problem not to have it. If we had subpoena authority for private entities, I am not sure that there would be a serious constitutional issue there, so I think the issue is a bit of a tangent.

Mr. WATT. I thank the gentlelady. These were just follow-ups to some concerns I had. I wasn't trying to prolong this, and I appreciate the extra time.

Ms. SÁNCHEZ. Thank you, Mr. Watt. I appreciate the questions.

Mr. Franks?

Mr. FRANKS. Thank you, Madam Chair.

Madam Chair, I will be very brief, just to comment related to Mr. Davis and Chairman Conyers.

Ms. SÁNCHEZ. Without objection, you will be granted 1 minute.

Mr. CONYERS. I ask unanimous consent for 2 minutes.

Mr. FRANKS. I will do 1. That will be fine.

Ms. SÁNCHEZ. Mr. Franks has told us he could be significantly briefer than both of you. So he has only requested 1. [Laughter.]

One additional minute.

Mr. FRANKS. Thank you, Madam Chair.

Related to any torture policy of the United States, being on the Armed Services Committee, it is my conviction that the policy nor the practice of this country has been to torture. In fact, the penalty for torture is 20 years in prison, and if the person tortured dies, the death penalty is appropriate, according to our policy.

So I don't think that policy has been diminished in any way under this Administration, and I just wanted to make sure that that is on the record.

Thank you, Madam Chair.

Mr. WATT. Will the gentleman yield?

Mr. FRANKS. Sure. You have 20 seconds here.

Mr. WATT. Does that apply if the torture takes place in another country after somebody has been rendered to someplace else?

Mr. FRANKS. Madam Chair, I just answered the gentleman's question. I do not believe that is the policy nor the practice of this Administration to torture anybody in this country or otherwise. The Abu Ghraib situation was abuse. But torture is very well-defined.

Mr. WATT. The gentleman may have misunderstood the question I was asking. Do the criminal penalties apply if we render somebody to another country and the torture takes place where we have not been active participants in the torture?

Mr. FRANKS. Madam Chair, the gentleman probably is asking whether or not the prisoners are under the constitution or the laws of the United States, and, no, I don't think they are. They would be under the Military Code of Justice.

Ms. SÁNCHEZ. The time of the gentleman has expired.

And that will conclude our rounds of questioning.

I want to thank the witnesses again for their testimony today and for making yourselves available for questions.

Without objection, Members will have 5 legislative days to submit any additional written questions, which we will forward to the witnesses and ask that you answer as promptly as you can so that they can be made a part of this record.

Without objection, the record will remain open for 5 legislative days for the submission of any additional materials.

I want to thank everybody for their time and their patience, and the hearing of the Subcommittee on Commercial and Administrative Law is adjourned.

Mr. DAVIS. Thank you.

[Whereupon, at 3:11 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Redline version of the Privacy and Civil Liberties Oversight Board, 2007 Report to Congress with edits by The White House, submitted by the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Chairwoman, Subcommittee on Commercial and Administrative Law

LANNY J. DAVIS, ESQ.
SENIOR PARTNER
ORRICK, HERRINGTON & SUTCLIFFE

JULY 24, 2007

"Oversight Hearing on the Privacy and Civil Liberties Oversight Board and the Department of Homeland Security Privacy Officer"

PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

2007 REPORT TO CONGRESS

I. INTRODUCTION
II. HISTORY AND MISSION 1
III. ORGANIZATION, ADMINISTRATION AND PROCESS 4
A. Necessary Administrative Actions and Budget 9
B. Substantive Actions to Fulfill Statutory Mandate 9
IV. OUTREACH AND EDUCATION 11
A. The White House and Executive Office of the President 13
B. Executive Branch 13
C. Congress 14
D. Media 18
E. Private Sector, Non-profit, Academic, and Advocacy Groups and Experts 19
F. International Forums 20
V. ISSUE IDENTIFICATION, PRIORITIZATION, AND DISCUSSION 21
A. Scope and Process 22
B. Specific Issues, Policies, Procedures, and Regulations 23
1. Oversight of Existing Federal Anti-terrorism Policies and Programs 26
2. Examples Where the Board Has Offered Advice Regarding the Development of a Policy, Program, Regulation, or Statute 27
3. Information Sharing 34
VI. THE YEAR AHEAD 36
VII. CONCLUSION 40
42

Deleted: 18
Deleted: 18
Deleted: 1817
Field Code Changed
Deleted: 19
Deleted: 19
Deleted: 1918
Deleted: 19
Deleted: 21
Deleted: 21
Deleted: 2120
Deleted: 22
Deleted: 22
Deleted: 2221
Deleted: 23
Deleted: 23
Deleted: 2322
Deleted: 26
Deleted: 26
Deleted: 2625
Deleted: 27
Deleted: 27
Deleted: 2726
Deleted: 34
Deleted: 33
Deleted: 3332
Deleted: 37
Deleted: 36
Deleted: 3635
Deleted: 40
Deleted: 39
Deleted: 3938
Deleted: 42
Deleted: 42
Deleted: 4241

DRAFT

I. INTRODUCTION

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which created the Privacy and Civil Liberties Oversight Board (Board), requires that "[n]ot less frequently than annually, the Board shall prepare a report to Congress, unclassified to the greatest extent possible . . . on the Board's major activities during the preceding period."[1] This report discusses the Board's activities from its first meeting on March 14, 2006, at which the Members were sworn in and an Executive Director was appointed, through March 1, 2007. This report contains no classified information.

Unlike other boards and commissions charged with addressing an issue, making recommendations, issuing a report and then disbanding, this Board embodies a permanent commitment to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations and executive branch policies related to efforts to protect the Nation against terrorism."[2] As the Federal government works to prevent acts of terror against the Nation, its citizens, and its interests, it must do so in compliance with the law, protective of the rights and liberties guaranteed by the Constitution, and consistent with the values we share as Americans. The Board's statutory mandate and fundamental purpose is to further those objectives.

During its first year, the Board met approximately twice a month. The Board dedicated itself to organization, staffing, and substantive background briefings on significant Executive Branch anti-terrorism programs affecting privacy rights and civil liberties and meeting with interested members of the privacy and civil liberties community. These included meetings with the Director of National Intelligence, and the heads of the National Security Agency, the National Counterterrorism Center, the Federal Bureau of Investigation, and the Terrorist Screening Center as well as the National Security Advisor, the Homeland Security Advisor, the Secretary of Homeland Security, the Attorney General, the White House Chief of Staff, the White House Counsel, and the Information Sharing Environment Program Manager. The Board has been fully briefed at the highest level of classification on the NSA's surveillance programs, the Treasury Department's Terrorist Finance Tracking Program, and the National Counterterrorism Center's National Implementation Plan on the War on Terror. While the Board was unable in its first year to spend as much time on evaluating and providing oversight of programs most affecting privacy rights and civil liberties as it would have liked, as this Report describes in Section VI (The Year Ahead), the Board now has the appropriate foundation to provide the advice and oversight required by IRTPA.

Deleted:

Deleted: ,

Deleted: Terrorist S

Deleted: P

Deleted: Program

Deleted: Therefore, during

Deleted: , the Board was unable to spend

Comment [SMW1]: DPC suggests this is a good thing – not warranting the apology. OLA says we should characterize as organizational.

Deleted: . However,

Formatted: Font: Times New

Formatted: Font: Times New Roman, 12 pt

Formatted: Font: Times New Roman, 12 pt.

Formatted: Space After: 6 pt

Formatted: Font: Times New Roman, 12 pt, Italic

Formatted: Font: Times New Roman, 12 pt

[1] Pub. L. 108-458, §1061(c)(4) (Dec. 17, 2004).

[2] *Id.* § 1061(c)(1)(C).

DRAFT

In order to stand up its operation during the first year, the Board allocated its resources among three core areas, discussed below, to build a foundation on which to offer substantive advice and oversight. Activities in these areas have helped the Board establish its viability, subject matter expertise, and credibility. The Board unanimously identified substantive accomplishments in these three areas at the outset as necessary prerequisites for long term success and included them in its first annual agenda, adopted in June, 2006. This first report to Congress outlines the Board's activities in these areas:

Organization, Administration and Process. The Board understood that, due to its part-time Membership, it had to establish the means and infrastructure necessary to help it accomplish its statutory mission. Toward that end, it has hired a professional staff, reached agreement with the Director of National Intelligence on the scope and logistics of detailing additional staff from within the intelligence community, acquired the necessary security clearances, built out appropriate office space with secured facilities for classified information, and developed a web site for communication with the public. Due to its position within the White House Office, the Board receives additional administrative support from White House staff.

Education and Outreach. The Board has engaged policy officials and experts within the Executive Branch, Congress, the public, and private, non-profit, and academic institutions. It has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism by meeting with senior officials, examining their missions and legal authorities, learning of their specific programs, and reviewing their operational methodologies and privacy and civil liberties training, reporting, and auditing programs. For example, the Board has met personally, among others, with the Attorney General, the Secretary of the Department of Homeland Security, the Director of National Intelligence, the Directors of the National Counterterrorism Center and National Security Agency, the Information Sharing Environment Program Manager, the Undersecretary of the Treasury for Terrorism and Financial Intelligence, and the President's senior staff. Among other non-governmental experts and advocacy groups, it has met with representatives from the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Markle Foundation, and the American Conservative Union. It also held its first public forum at Georgetown University on December 5, 2006.

As a part of this education and outreach effort, the Board has made it a priority to work with a new and growing network of Executive Branch homeland security professionals specifically dedicated to consideration of privacy and civil liberties issues. The Board considers one of its fundamental responsibilities fostering a sense of community among these new professional privacy and civil liberties officers and members of the relevant professions that have existed within the Federal government for decades, including attorneys, inspectors general, and relevant program policy officials.

The Board intends to continue providing these offices with the necessary support to enable them better to accomplish their own responsibilities.

Issue Prioritization. The Board's statutory authority is broad. The Board has focused on those issues that could provide the most value for the American people, the President, and the Executive Branch. Policies and programs warranting the Board's attention will evolve over time. Identification of these priorities will necessarily change as new initiatives are considered, developed, and implemented. This report outlines the process and consideration undertaken by the Board in developing and reviewing those issues.

With these foundational accomplishments behind it, the Board stands at the beginning of its second year well equipped to further address the substantive issues of its statutory mandate.

II. HISTORY AND MISSION

Following the attacks of September 11, 2001, Congress and the President established the National Commission on Terrorist Attacks on the United States (9/11 Commission or Commission), a bipartisan panel charged with investigating the events of 9/11 and offering "recommendations designed to guard against future attacks."[3] As the Commission acknowledged, many of its recommendations "call[ed] for the government to increase its presence in our lives – for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies."[4] However, the Commission also noted that "[t]he choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home."[5] Consequently, the Commission also recommended the creation of "a board within the Executive Branch to oversee . . . the commitment the government makes to defend our civil liberties."[6] In order to implement the Commission's numerous recommendations, Congress passed, and President Bush signed, the Intelligence Reform and Terrorism Prevention Act of 2004.[7] Among other actions – including reshaping the intelligence community under one Director of National Intelligence[8] – IRTPA authorized the creation of the Privacy and Civil Liberties Oversight Board.

Deleted: —

IRTPA requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism."[9] In carrying out this mandate, the Board has two primary tasks. *First*, it must "*advise* the President and the head of any department or agency of the Executive Branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation"[10] of "laws, regulations, and executive branch policies related to efforts to protect the Nation from terrorism."[11] *Second*, it must exercise *oversight* by

[3] *National Commission on Terrorist Attacks on the United States*, *available at* http://www.9-11commission.gov/about/index.htm (last accessed Nov. 1, 2006).

[4] THE 9/11 COMMISSION REPORT, 393-94 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf (last accessed Nov. 1, 2006).

[5] *Id.* at 395.

[6] *Id.*

[7] Pub. L. 108-458 (Dec. 17, 2004).

[8] *Id.* § 1001 *et seq.*

Deleted: Most notably, IRTPA dramatically reshaped the intelligence community by consolidating intelligence officials under one Director of National Intelligence.

[9] *Id.* § 1061(c)(3).

[10] *Id.* § 1061(c)(1)(C) (emphasis added).

[11] *Id.* § 1061(c)(1)(B).

"continually review[ing] regulations, executive branch policies, and procedures . . . and other actions by the executive branch related to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected."[12] The statute expressly requires the Board to advise[13] and oversee[14] the creation and implementation of the Information Sharing Environment (ISE).

In order to offer informed advice and oversight, the Board may access "from any department or agency of the executive branch, or any Federal officer or employee of any such department or agency[,] all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law."[15] And to allow Board Members timely access to classified materials to carry out their mandate, the statute requires "appropriate departments and agencies of the executive branch [to] cooperate with the Board to expeditiously provide Board members and staff with appropriate security clearances."[16] The Board may also demand that persons other than departments, agencies, and elements of the Executive Branch provide "relevant information, documents, reports, answers, records, accounts, papers, and other documentary and testimonial evidence."[17] If a Federal agency, official, or other relevant persons choose not to produce information requested by the Board, the Board may pursue a remedy by notifying the Attorney General or the head of the relevant agency. The Attorney General may then "take such steps as appropriate to ensure compliance" with the Board's request, including issuing subpoenas.[18] Although the Board may have general access to "materials necessary to carry out its responsibilities,"[19] materials may be withheld if "the National Intelligence Director, in consultation with the Attorney General, determines that it is necessary . . . to protect the national security interests of the United States"[20] or if the Attorney General determines that it is necessary to withhold information "to protect sensitive law enforcement or counterterrorism information or ongoing operations."[21]

---

[12] *Id.* § 1061(c)(2)(A).

[13] *Id.* § 1061(d)(2).

Deleted: 1

[14] *Id.* 1061(c)(2)(B).

[15] *Id.* § 1061(d)(1)(A).

[16] *Id.* § 1061(h).

[17] *Id.* § 1061(d)(1)(D)(i).

[18] *Id.* § 1061(d)(2)(B).

[19] *Id.* § 1061(d)(1).

[20] *Id.* § 1061(d)(4)(A).

[21] *Id.* § 1061(d)(4)(B).

DRAFT

As shown in the Board's location, assigned roles, and authority, IRTPA did not create an independent watchdog entity in the nature of an inspector general.[22] Rather, the statute created a Board that operates *within* the Executive Office of the President and ultimately reports to the President. The statute requires the Board to produce an annual report to Congress only "on [its] major activities"[23] – not on all of its internal deliberations and recommendations. The statute expressly places the Board within the Executive Office of the President (EOP), an office whose sole purpose is to support the Executive. Consistent with that placement and with the goal of offering candid advice,[24] the President has located the Board even more closely to him by placing it within the White House Office (WHO). Congress acknowledged this placement by earmarking certain WHO appropriated funds for Board use rather than appropriating funds to a specific EOP entity. As the statute explicitly acknowledges, all five Board Members (like other EOP and WHO employees) serve at the pleasure of the President.[25] By empowering the Board with broad access to records, IRTPA has created a Board that can offer a distinctly independent perspective to the President, along with oversight of executive agencies.

Deleted: Branch

Comment [SMW2]: OMB – delete; under discussion re level of detail

Formatted: Font: Times New

The Board acts in concert with a robust and developing privacy and civil liberties (PCL) infrastructure that is already operating throughout every major anti-terrorism agency, including the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Office of the Director of National Intelligence (ODNI).[26] In most cases, these PCL offices are headed by officials with direct access to their agency heads. They are primarily staffed by diligent career civil servants who focus on and provide an additional degree of continuity regarding the appropriate consideration of privacy and civil liberties. As discussed below, the Board intends to provide a coordinating role for these PCL offices and will also assist in addressing unique problems that require government-wide coordination or specific White House involvement.[27]

---

[22] *See, e.g.*, the Federal Inspector General Act of 1978, 5 U.S.C. Appx § 1 *et seq.*

[23] IRTPA § 1061(c)(4).

[24] Although the statute subjects the Board to the Freedom of Information Act (FOIA), *see id.* § 1061(i)(2), the regular exemptions to FOIA disclosure still apply. *See* 5 U.S.C. § 552(b).

[25] IRTPA § 1061(e)(1)(E) ("The chairman, vice chairman, and other members of the Board shall each serve at the pleasure of the President.").

[26] In IRTPA, Congress expressed its sense "that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." *Id.* § 1062.

[27] *Infra* Part V.B.2.

DRAFT

IRTPA also sets the qualifications of the Board's Members. The President must appoint as Members "trustworthy and distinguished citizens outside the Federal Government who are qualified on the basis of achievement, experience, and independence."[28] Both the Chairman and Vice Chairman of the Board also require Senate confirmation.[29] To these ends, President Bush appointed the following individuals as Members:

- ***Carol E. Dinkins, Chairman*** – Formerly served as Deputy Attorney General and Assistant Attorney General in charge of the Department of Justice's Environment and Natural Resources Division. She is a partner with Vinson & Elkins, L.L.P. in its Houston, TX office.

- ***Alan Charles Raul, Vice Chairman*** – Former General Counsel of both the U.S. Department of Agriculture and the Office of Management and Budget as well as Associate White House Counsel to President Reagan. He is a noted expert and author on privacy, data protection, and information security. He is a partner in Sidley Austin's Washington, DC office.

- ***Lanny J. Davis*** – Served as Special Counsel to President Bill Clinton and is a noted author and frequent television commentator. He is a partner in Orrick, Herrington and Sutcliffe's Washington, DC office.

- ***Theodore B. Olson*** – Served as U.S. Solicitor General from 2001-2004 and as Assistant Attorney General for the Office of Legal Counsel from 1981-1984. Mr. Olson is one of the Nation's premier appellate and Supreme Court advocates and is a partner in Gibson, Dunn and Crutcher's Washington, DC office.

- ***Francis X. Taylor*** – A retired Brigadier General with the U.S. Air Force and former Commander of the Air Force Office of Special Investigation. He also served as Assistant Secretary of State for Diplomatic Security and U.S. Ambassador at Large for Counterterrorism. He is presently the Chief Security Officer for the General Electric Company.

Deleted:

On February 17, 2006, the Senate confirmed Chairman Dinkins and Vice Chairman Raul. All five Members were sworn into office and held their first meeting on March 14, 2006. In taking office, the Board effectively took the place of the President's Board on Safeguarding Americans' Civil Liberties (President's Board), which the President created by executive order in 2004.[30] The President's Board was chaired by the

[28] IRTPA § 1061(e)(1)(C).

[29] *Id.* § 1061(e)(1)(B).

[30] *See* EO 13353 (Aug. 27, 2004).

Deputy Attorney General and consisted of twenty-two representatives from the Departments of State, Defense, Justice, Treasury, Health and Human Services, and Homeland Security, the Intelligence Community, and the Office of Management and Budget.[31] Following the enactment of IRPTA and the creation of the Board, the President's Board disbanded itself and transferred its papers to Board staff.

In addition to IRTPA, the Board works within the legal framework that guides all efforts to protect the Nation against terrorism.[32] Consequently, the Board has gathered and familiarized itself with relevant seminal documents and authorities that impact its mission.[33]

[31] The President's Board met as a full group six times and organized itself into six subcommittees. The six subcommittees included Investigative Legal Authorities, Redress Systems, Data Collection and Sharing Standards, Engagement with Arab-American Communities, Public Outreach, and Policies and Procedures.

Deleted: ;

[32] *See, e.g.*, IRTPA § 1061(d)(1) (allowing the Board to obtain documents subject to the statute's restrictions and "to the extent permitted by law").

[33] This list includes, but is not necessarily limited to: U.S. CONSTITUTION; BILL OF RIGHTS; Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 *et seq.*; *Strengthening the Sharing of Terrorism Information to Protect Americans*, EO 13388, 70 Fed. Reg. 62023 (Oct. 27, 2005); *Strengthening the Sharing of Terrorism Information to Protect Americans*, EO 13356 (Aug. 27, 2004), 69 Fed. Reg. 53599 (Sept. 1, 2004); *Strengthened Management of the Intelligence Community*, EO 13355 (Aug. 27, 2004), 69 Fed. Reg. 53593 (Sept. 1, 2004); *National Counterterrorism Center*, EO 13354 (Aug. 27, 2004), 69 Fed. Reg. 53589 (Sept. 1, 2004); *Establishing the President's Board on Safeguarding Americans' Civil Liberties*, EO 13353 (Aug. 27, 2004), 69 Fed. Reg. 53585 (Sept. 1, 2004); *Conduct of Intelligence Activities*, EO 12333, 46 Fed. Reg. 59941 (1981); *Memoranda from the President to Congress and Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* (Dec. 16, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html (last accessed Jan. 4, 2006); THE 9/11 COMMISSION REPORT; COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION: REPORT TO THE PRESIDENT OF THE UNITED STATES (March 31, 2005).

Formatted: Space After: 6 pt

Deleted: 36

DRAFT

III. ORGANIZATION, ADMINISTRATION AND PROCESS

The Board has established and instituted the means and infrastructure to support it in accomplishing its statutory mission. As mentioned previously, the Board operates within the White House Office, a unit within the Executive Office of the President. Given this placement, the Board follows established White House Office policies in carrying out its administrative and budgetary responsibilities.

A. Necessary Administrative Actions and Budget

In order to manage its everyday affairs, the Board has hired a full-time staff. As an initial matter, it hired an Executive Director – Mark A. Robbins, who previously served as General Counsel of the U.S. Office of Personnel Management. Shortly thereafter, it hired a Deputy Executive Director and Counsel, Seth M. Wood, and a Staff Assistant, John V. Coghlan. The Board's staff communicates on a daily basis with all Members and regularly reports its activities to the Board. Staff – in conjunction with the Office of Government Ethics[34] and ethics counsel within the White House Counsel's office – have identified and clarified the relevant legal, ethical, and financial rules and guidelines applicable to special government employees,[35] as defined by law. The Members have entered into ethics agreements which ensure that their activities on behalf of clients and employers do not conflict with their service on the Board.

Deleted: al

The Board has also begun the process of securing detailees from other agencies.[36] Then-Director of National Intelligence John Negroponte determined that a detail assignment to the Board for a period of one year will fulfill the "joint duty" requirement for professional advancement within the intelligence community and requested that each of the 16 intelligence agencies reporting to ODNI propose candidates for such a detail assignment.[37] The Board is not responsible for reimbursing host agencies for detailees under the provisions of IRTPA.

Deleted: billing

---

[34] Members and staff have held two formal meetings with the Office of Government Ethics and have sought informal advice as needed.

Deleted: al

[35] Due to their part-time status, Board Members are classified as special government employees. 18 U.S.C. § 202(a) (defining a "special government employee" as one "who is retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days"). In order to determine a Member's employment status, staff has established a process for reporting and recording the time Members spend on Board activity.

[36] IRTPA § 1061(g)(2).

[37] IRTPA also authorizes the Board to hire the services of consultants as necessary.

DRAFT

As a WHO unit, the Board did not have to hire separate staff dedicated to press and communications, legislative affairs, administration, or information technology but instead has utilized the services of the relevant components of the White House Office. The Board's administrative support staff has been integrated into the regular operations of the WHO and attends regularly-scheduled meetings with the White House Office of Management and Administration.

IRTPA requires the Board to adopt rules and procedures for physical, communications, computer, document, personnel, and other security in relation to the work of the Board. As a WHO unit, the Board adopted the existing rules and procedures of the EOP.

Staff has carried out other necessary duties to allow Board Members full access to the potentially classified and sensitive documents necessary to complete their statutory obligations. For example, working with the relevant Executive authorities, Members and staff have obtained Top Secret/SCI clearances. Staff and OA have also constructed appropriate office space[38] to house the Board's operations within the White House complex. This suite includes secure facilities for the review and storage of classified information, as well as secure telephone and fax lines. Office space build out included laying secure communications lines to connect the suite with existing secure lines located at the Winder Building that houses the Office of the United States Trade Representative.

Comment [WH3]: WH Staff objects to this level of detail.

Formatted: Font: Times New Roman

The Chairman, Vice Chairman, and Board staff were issued passes that allow them general access to the White House complex.

With the assistance of White House administrative staff and the EOP Office of Administration, the Board has developed a working budget for fiscal years 2006 and 2007. In its FY 2006 appropriations bill, Congress specified that "of the funds appropriated [to the White House Office,] $1,500,000 shall be for the Privacy and Civil Liberties Oversight Board."[39] The Board was in existence for only half of FY 2006.

Deleted: But as a unit within the WHO, the Board does not have its own dedicated budget.

An estimate of specific line item costs incurred by the Board to date includes the following items:

- $340,000 for full-time staff salaries and benefits
- $60,000 for Member and staff security clearances and background investigations

[38] The Board's office and suite are located at 1724 F St. NW in Washington, DC.

[39] House Rep. No. 109-307 at 78 (Nov. 18, 2005), accompanying passage of Pub. L. 109-115 (Nov. 30, 2005).

DRAFT

- $13,000 for Member travel costs
- $103,000 for Member per-diem payments

As noted above, the Board was not responsible for providing the funds for the significant costs associated with the build out of its office space, including secure facilities for the review and storage of classified documents; the laying of secure communications line under F Street, between the Board's suite and the White House complex; office rent or utilities costs; office information technology costs and support; and costs associated with detailed employees from the Executive Branch, which will account for a significant portion of its staffing needs in the year to come.

Comment [WH4]: WH Staff opposes discussion of budget specifics.

The Board is able to meet its statutory responsibilities under the present budget arrangement and funds available.

Formatted: Font: Times New Roman, 12 pt

Deleted: satisfied that it is

Deleted: to it

B. Substantive Actions to Fulfill Statutory Mandate

In carrying out its substantive statutory mandates, the Board has formally met twenty-three times in its first year. All but five of these meetings occurred in person and all but two had unanimous attendance. All meetings took place in or around Washington, DC – within the White House complex, at various departments and agencies, and one meeting at Georgetown University. To place the activity of the Board's part-time membership in perspective, the Board has formally met an average of about once every two weeks. Members always remain in near-constant communication with each other and the staff through e-mail and telephone. In the first few months of operation, the Board adopted a number of formative procedures and policies, including issue prioritization, everyday operations, public communications, and analytical methodologies.

As an initial matter, the Board adopted its first annual agenda. The agenda functioned as a business plan by allocating responsibility for tasks among staff and setting expectations regarding how the Board would function. It also served as a substantive agenda by laying out an initial list of issues on which the Board agreed to focus its energies. The Board adopted a communications plan that laid out a strategy for engaging the public through direct means (such as a website and publications in the *Federal Register*) and through media outlets (both traditional and emerging). As part of its direct communication strategy, the Board approved the creation of a web site – www.privacyboard.gov – to discuss the Board's history, mission, and activities and provide the public access to Board Member biographies, Board statements, and other related documents. The web site also serves as a means by which the public may contact

Deleted: -

Deleted: es

DRAFT

the Board.

Deleted: Additionally, the Board has promulgated interim regulations to implement the Freedom of Information Act (FOIA).[40]

The Board also developed a series of preliminary processes, procedures, and methods by which it could fulfill its advice and oversight responsibilities to the President and Executive Branch agency heads. Of greatest importance, it agreed upon a methodology for analyzing and evaluating proposed programs. It established both a regular means for Board staff to report their activities to the Members and a means of discussing issues and offering possible actions for the Board to take. It also adopted a set of White House Security Guidelines. These processes and templates are discussed in greater detail in Section V.A.

DRAFT

IV. OUTREACH AND EDUCATION

The Board moved immediately to establish lines of communication within and outside of the Federal government, to educate itself on relevant issues of interest and concern relating to efforts to protect the Nation against terrorism, and to educate others on its mission and oversight and advisory roles.

A. The White House and Executive Office of the President

In order to obtain the most complete, real-time access to information regarding proposed and operational anti-terror programs, the Board must establish trust and credibility between itself and the relevant members of the Executive Branch. To that end, the Board has developed a sound, regular, and productive working relationship with the President's most senior advisors tasked with anti-terrorism responsibilities. This relationship has put the Board in a position to integrate itself into the policymaking process and obtain the necessary support from the Administration to offer meaningful advice.

Deleted: where it hopes to be able

The Board has met personally with the following principal senior White House officials:

- Chief of Staff Joshua B. Bolten and then-Chief of Staff Andrew Card
- National Security Advisor Stephen J. Hadley
- Homeland Security and Counterterrorism Advisor Frances F. Townsend
- Counsel to the President Fred Fielding and then-Counsel Harriet Miers
- Staff Secretary Raul F. Yanes (and also while he served as General Counsel of the Office of Management and Budget).
- A.B. Culvahouse, Chairman of the Intelligence Oversight Board and member of the President's Foreign Intelligence Advisory Board.

Comment [WH5]: WH Staff opposes use of personal names.

These meetings have allowed the Board to forge strong working relationships with agencies within the Executive Office of the President, including the National Security Council, Homeland Security Council, Office of Management and Budget, Office of the Counsel to the President, and the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board, among others. Additionally, the Board's professional staff meets weekly with an EOP working group which consists of commissioned officer

Formatted: Font: Times New Roman

representatives from the Office of the White House Chief of Staff, the National Security Council, the Homeland Security Council, the Office of the Counsel to the President, the Office of Legislative Affairs, the Office of Communications, and the Office of Management and Budget.

B. Executive Branch

The Board has also met with senior administration officials throughout the Executive Branch who have responsibilities for developing and implementing war-on-terrorism policies and strategies. These officials include:

- Attorney General Alberto Gonzales
  - Deputy Attorney General Paul McNulty
  - Assistant Attorney General for Legal Policy Rachel Brand
  - Assistant Attorney General for National Security Kenneth L. Wainstein.
  - Acting-Assistant Attorney General for Legal Counsel Stephen G. Bradbury
- The Secretary for Homeland Security Michael Chertoff
- Department of the Treasury Under Secretary for Terrorism and Financial Intelligence Stuart Levey
  - Assistant Secretary for Intelligence and Analysis Janice B. Gardner
- Then-Director of National Intelligence John Negroponte
  - Then-Principal Deputy DNI (now CIA Director) General Michael Hayden
  - Information Sharing Environment (ISE) Program Manager Ambassador Thomas McNamara
  - ODNI General Counsel Benjamin A. Powell
- FBI Director Robert Mueller

DRAFT

- Director of the National Security Agency Lt. General Keith Alexander
  - Then-National Security Agency Inspector General Joel Brenner
  - Director of Signals Intelligence Directorate James Cusick
  - General Counsel Vito Potenza

Formatted: Bullets and Numbering

- Director of the National Counterterrorism Center Vice Admiral John Scott Redd, USN (Ret.)
  - Deputy Director for Strategic Operational Planning, Vice Admiral Bert Calland
- Then-Director of the Terrorist Screening Center Donna Bucella.

The Board and its staff have made repeated visits to a number of government facilities to observe how those agencies operate, develop anti-terror policies, and train their employees to protect privacy and civil liberties. On-site visits also tend to promote a high-quality dialogue between Board Members and advisors. Consequently, the Board has personally visited the Department of Justice, the Department of Homeland Security, the National Security Agency, the National Counterterrorism Center, the Terrorist Screening Center, the Federal Bureau of Investigation, and the Department of Defense Counterintelligence Field Activity Office.

Deleted: Activities office

Perhaps most importantly, the Board has established strong working relationships with the developing privacy and civil liberties offices within the government's anti-terror agencies. These offices and officers advance privacy and civil liberties at the ground level and generally have the greatest practical impact on the development and implementation of policies within their respective agencies. The privacy and civil liberties offices with which the Board works most closely include those at the Department of Justice, the Department of Homeland Security, and the Office of the Director of National Intelligence. These officials have likewise developed lines of communication and authority within their organizations' structure.

These relationships allow the Board to encourage the sharing of information and best practices among those offices. The relationships have also allowed the Board to coordinate and offer assistance when the privacy or civil liberties officers encounter problems. The Board has helped and will continue to help coordinate and foster the development of a privacy and civil liberties infrastructure throughout the Executive Branch. This portion of the Report includes a brief summary of the PCL offices' major

DRAFT

activities over the last year and is in addition to the Board's own independent activities described in Part V, *infra*.

- Department of Justice: Like the Board, over the past year the DOJ Privacy and Civil Liberties Office has also begun its early work in earnest. The Violence Against Women and Department of Justice Reauthorization Act of 2005[41] required the Attorney General to appoint a senior official to assume primary responsibility for privacy policy. The Attorney General appointed Jane C. Horvath as the Department's first Chief Privacy and Civil Liberties Officer on February 21, 2006. Placed within the Office of the Deputy Attorney General, the DOJ Privacy Office considers issues relating to the Privacy Act, privacy and civil liberties, and e-government compliance. Among other activities, this office joined DHS in the delegation that represented the United States in negotiations with the European Union regarding the transfer of Passenger Name Record (PNR) information from Europe to the Bureau of Customs and Border Protection. In participating in these negotiations, this delegation helped ensure that all parties adequately considered privacy and civil liberties interests. In conjunction with the ODNI Civil Liberties and Privacy Office, the DOJ Privacy Office also helped draft privacy guidelines governing the ISE. The office has also worked with the Board and other privacy and civil liberties offices to assist in drafting a Memorandum of Understanding that will establish standardized procedures to address complaints regarding air travel watch lists.

- The Office of the Director of National Intelligence: Like the Board, the ODNI Civil Liberties and Privacy Office (CLPO) came into existence with the passage of IRTPA. The statute requires CLPO to ensure that civil liberties and privacy protections are appropriately incorporated into the policies of the ODNI and the intelligence community, oversee compliance by the ODNI with legal requirements relating to civil liberties and privacy, review complaints about potential abuses of privacy and civil liberties in ODNI programs and activities, and ensure that technologies sustain and do not erode privacy. The Director of National Intelligence appointed Alexander W. Joel to lead the CLPO, and Mr. Joel hired a deputy to address privacy issues and another deputy to consider civil liberties concerns. In addition to completing a number of necessary stand-up requirements, the ODNI has, through the work of the CLPO, established internal ODNI policy for Protection of Privacy and Civil Liberties. In addition, the CLPO has identified a senior official at each intelligence agency to serve as the focal point of privacy and civil liberties issues at that agency. Perhaps most importantly, the CLPO co-drafted the privacy protection guidelines that govern the Information Sharing Environment, and is co-chairing the process for ensuring that agencies have sufficient guidance and support to implement the guidelines

[41] Pub. L. 109-162 (Jan. 5, 2006).

Comment [MAR6]: Transition sentence added at suggestion of Counsel to address OIRA comments 7 and 8, below.

Formatted: Font: Italic

Deleted: accomplishments

Deleted: Ms. Horvath

Deleted: was part of the delegation

Deleted: Ms. Horvath

Deleted: The

Deleted: co-d

Deleted: (in conjunction with the ODNI)

Comment [OIRA7]: General comment: the report should first and foremost describe the activities and results of the Board and then second how the Board's support encouraged other activities led at other agencies. Suggest deleting as this does not report results of PCLOB as much as it does DOJ's CPO. Alternatively, the connection between how the PCLOB supported DOJ's CPO can be stronger.

Comment [MAR8]: Text modified to acknowledge efforts of others in these areas per WH staff concerns.

Formatted: Font: Times New Roman, 12 pt

Deleted: No.

DRAFT

effectively and consistently. Moreover, the CLPO has conducted numerous reviews of intelligence community programs and activities, helped shape significant policies and guidelines, and established procedures for community personnel to provide the CLPO with information about possible privacy and civil liberties abuses.

- The Department of Homeland Security: The DHS Privacy Office is headed by Hugo Teufel and is the first statutorily created privacy office[27] within the federal government designated to the oversight of privacy protections. As such, Hugo Teufel, as Chief Privacy Officer and Chief FOIA Officer, serves as the primary advisor on privacy matters and, by designation, departmental disclosure matters to the Secretary of DHS. In addition to privacy policy advice, the DHS Privacy Office (we) (1) to assure that the use of technologies sustain, and do not erode, privacy protections; (2) to assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices; (3) to evaluate legislative and regulatory proposals involving personal information within federal government; (4) to conduct privacy impact assessments of proposed rules of DHS; (5) to coordinate with the Officer for Civil Rights and Civil Liberties; and (6) to prepare an annual report to Congress on activities of the Department that affect privacy. The Privacy Office is structured into two functional components: privacy and freedom of information. The freedom of information component addresses issues to include FOIA and Privacy Act requests and appeals and FOIA policy and regulations. The privacy component addresses the above statutory and policy-based responsibilities, in a collaborative environment to include Compliance; International Privacy Policy; Legislative and Regulatory Affairs; and Technology. Much of the Privacy Office work focuses on developing a compliance framework for the Privacy Act and E-Government Act. This effort standardized and harmonized privacy compliance concerning Privacy Impact Assessment (PIA) and System of Records Notice (SORN) reporting requirements. Both documents require agencies to complete an analytical template that describes the intended benefits of a particular program or change, the possible privacy concerns or risks generated by such a program or change, and how the agency mitigates privacy risks. Operationally, the Privacy Office provided privacy advice regarding the Secure Flight program, reviewed the implementation of the arrangement to transfer PNR information from air carriers in the European Union to the Bureau of Customs and Border Protection, participated with DOJ and DHS Privacy and Civil Liberties officers in drafting the ISE Privacy Guidelines, and advised DHS on privacy issues concerning data governance and data security.

[27] Pub. L. 107-296, § 222 (Nov. 25, 2002) (codified at 6 U.S.C. § 142)

Comment [OIRA9]: Not clear how the PCLOB function supported this section, this appears to be better placed in an appropriate report from the DNI.

Deleted: In addition to completing a number of necessary stand-up requirements, CLPO has issued ODNI's Instruction for Protection of Privacy and Civil Liberties and has identified the basic contacts throughout the intelligence community necessary to ensure the protection of privacy and civil liberties. Perhaps most importantly, the CLPO co-drafted the privacy protection guidelines that govern the Information Sharing Environment. It has conducted reviews of potentially

Deleted: -

Deleted: problematic programs and has established procedures for ODNI personnel to file complaints.

Formatted: Font: Times New Roman, 12 pt

Deleted: focuses primarily

Deleted: ensuring

Deleted: with

Deleted: The Privacy Office has focused on standardizing

Deleted: mandating

Deleted: with

Deleted: »

Deleted: s

Deleted: civil liberties

Deleted: or program

Deleted: minimizes those concerns

Deleted: The office has also

Formatted: Font: Times New Roman, 12 pt

Formatted: Font: Times New Roman, 12 pt

Formatted: Space After: 6 pt

Deleted: 6 U.S.C. § 142 (2007), Pub. L., 107-296, 116 Stat. 2135, 2155,

Deleted: Sec.

Formatted: Font: Times New Roman, 12 pt

Formatted: Font: Times New Roman, 12 pt

The DHS Office for Civil Rights and Civil Liberties (CRCL) has a relatively broad responsibility to ensure that DHS programs and activities comply with constitutional, statutory, regulatory, policy, and other requirements related to civil rights and civil liberties. It also must investigate complaints that allege possible abuses of civil rights or civil liberties. The CRCL is led by Daniel W. Sutherland, the Officer for Civil Rights and Civil Liberties. Of specific relevance to the Board, the CRCL has focused a great deal of its efforts on resolving complaints arising from the use of aviation watch lists. Along these same lines, the CRCL has worked with the Board and other privacy officers to develop a standardized procedure – to be embodied in a Memorandum of Understanding – to resolve watch list complaints.

The Departments of State, Treasury, and Defense have also designated officials to act as privacy points of contact for the Board. The Board anticipates and looks forward to building similar working relationships with other privacy and civil liberties offices throughout the Executive Branch.

C. Congress

Board Members and the White House Office of Legislative Affairs have reached out to Senators and Representatives to brief them on the Board's mission, priorities, and activities, as appropriate. The Chairman and Vice Chairman have responded to all Congressional requests for testimony. The Board has also authorized its Executive Director to ensure that appropriate lines of communication and information exist between it and Congress. These Congressional interactions include the following:

- On November 8, 2005, Carol Dinkins and Alan Raul testified at their confirmation hearing before the Senate Judiciary Committee. Prior to their confirmation hearing, they conducted courtesy visits with Senators Richard J. Durbin, Edward M. Kennedy, Arlen Specter, Jeff Sessions, and John Cornyn.

Deleted: , and Arlen Specter

- On May 4, 2006, the Executive Director met with a bipartisan group of staff from the House Permanent Select Committee on Intelligence.
- On June 6, 2006, Chairman Dinkins and Vice Chairman Raul testified before the House Government Reform Subcommittee on National Security, Emerging Threats, and International Relations.
- On August 10, 2006, the Executive Director met with majority staff from the Senate Committee on Homeland Security and Governmental Affairs.

DRAFT

- On November 3, 2006, the Executive Director met with minority staff from the Senate Judiciary and Senate Homeland Security and Governmental Affairs Committees.

- The Executive Director worked with Senate Judiciary Committee staff regarding certain administrative matters relating to confirmation materials.

- On November 27, 2006, Carol Dinkins, Alan Raul and Lanny Davis briefed bipartisan staff from the Senate Judiciary, Intelligence and Homeland Security Committees.

- On December 13, 2006, the Executive Director met with staff of Representatives Shays, Maloney, and Thompson.

- On December 19, 2006, Member Lanny Davis and the Executive Director met with staff to Senators Lieberman and Durbin.

- On February 8, 2007 the Executive Director met with minority staff of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security.

- The Board has either corresponded with individual Members of Congress or been the subject of correspondence between Members and the Executive Office of the President on a number of occasions since enactment of the Intelligence Reform and Terrorism Prevention Act of 2004.[43]

Deleted: ¶
The Board and its activities have been referenced in two Congressional reports: (1) House Permanent Select Committee on Intelligence Oversight Subcommittee's report: *Initial Assessment on the Implementation of the Intelligence Reform and Terrorism Prevention Act of 2004* (July, 2006); and (2) Government Accountability Office report: *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public* (September 2006).

D. Media

The Board works in coordination with the White House Communications and Press offices. On September 10, 2006, Members Lanny Davis and Ted Olson appeared on a Discovery Channel special hosted by Ted Koppel entitled *The Price of Security*. Members of the media were invited to attend the Board's December 5, 2006 public meeting, and Board Members gave numerous interviews following that event. Additionally, media representatives are encouraged to monitor the Board's web page (www.privacyboard.gov) for activities and statements. The Board has been the subject of

[43] The Board and its activities have been referenced in two Congressional reports: (1) House Permanent Select Committee on Intelligence Oversight Subcommittee's report: *Initial Assessment on the Implementation of the Intelligence Reform and Terrorism Prevention Act of 2004* (July, 2006); and (2) Government Accountability Office report: *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public* (September 2006).

Formatted: Font: Times New Roman, 12 pt

DRAFT

numerous articles nation-wide in the press and on-line. Members believe they have responded to all requests for interviews or comments.

E. Private Sector, Non-profit, Academic, and Advocacy Groups and Experts

The Board has set as a high priority engaging in a productive and ongoing dialogue with privacy, non-profit, and academic organizations within the privacy and civil liberties community. These conversations have helped identify issues important to the community, exchange ideas regarding how to craft anti-terrorism policies and procedures, and establish trust between the Board and the community. For example, the Board has strived to communicate regularly with the co-chairs of the 9/11 Commission, Governor Thomas Kean and Congressman Lee Hamilton.[44] Chairman Dinkins and Vice Chairman Raul met collectively with Governor Kean and Congressman Hamilton and apprised them of the Board's major activities. They have also held individual telephone conferences with Governor Kean and Congressman Hamilton. Following the December telephone conference, Congressman Hamilton requested the Board's executive director to contact him every 60 days with additional updates on the Board's efforts. In addition, the Board's executive director has met with then-State Department Counselor and former Commission executive director Philip D. Zelikow and Commission General Counsel Daniel Marcus. The Board is dedicated to meeting the letter and spirit of the 9/11 Commission's recommendations, consistent with its statutory authority, and looks forward to continued contact with the Commission's co-chairs.

Deleted:

Additionally, the Chairman and Vice Chairman met with representatives from the American Civil Liberties Union and the Center for Democracy and Technology within the first two months of the Board's operation. The Board also has held meetings with: the American Conservative Union; the Center for Strategic and International Studies; the Electronic Privacy Information Center and the Privacy Coalition; the Markle Foundation; Cato Institute; the Heritage Foundation; the Liberty Coalition; and the National Institute of Standards and Technology. Board representatives have appeared at the Progress and Freedom Foundation's Annual Aspen Summit, the U.S. Army Judge Advocate General's School Advanced Intelligence Law Conference, and the Intelink and the Information Sharing Conference and Technology Exposition.

Deleted: the Intelink and the Information Sharing Conference and Technology Exposition;

Deleted: and

Deleted: .

The Board has also appeared before or participated in advisory committees and workshops conducted by DHS (the Data Privacy and Integrity Advisory Committee); ODNI (Privacy Protection Technologies Workshops hosted by ODNI and the Disruptive Technologies Office); DOJ (Intergovernmental Privacy Issues Forum and Global Justice Information Sharing Initiative, Global Advisory Committee); American University (Masters of Public Administration Seminar on Separation of Powers); and National

[44] As noted previously, the Commission's recommendations led to the Board's creation.

DRAFT

Academies of Science (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and other National Goals).

On December 5, 2006, Georgetown University's Institute for International Law and Politics hosted the Board's seventeenth meeting, a public forum discussion between the Board, privacy and civil liberties advocacy groups, academicians, and the public. The Board was joined by Alexander W. Joel, Civil Liberties Protection Officer at the Office of the Director of National Intelligence; Jane C. Horvath, Chief Privacy and Civil Liberties Officer at the Department of Justice; and Daniel Sutherland, Officer for Civil Rights and Civil Liberties at the Department of Homeland Security. Panelists included Caroline Fredrickson, Director of the Washington Legislative Office of the American Civil Liberties Union; David Keene, Chairman of the American Conservative Union and Co-chair of the Constitution Project's Liberty and Security Initiative; Marc Rotenberg, Executive Director of the Electronic Privacy Information Center; Michael Ostrolenk, Co-founder and National Director of the Liberty Coalition; Brian Walsh, Senior Legal Research Fellow at the Heritage Foundation; James Dempsey, a member of the Markle Foundation Task Force on National Security in the Information Age; Fred Cate, Distinguished Professor and Director for the Center for Applied Cybersecurity Research at Indiana University; Peter Swire, the C. William O'Neill Professor of Law at Ohio State University and former Chief Counselor for Privacy in the U.S. Office of Management and Budget under President Clinton; Neal K. Katyal, Professor of Law at Georgetown University; and Anthony Clark Arend, Professor of Government and Foreign Service and Director of the Institute for International Law and Politics at Georgetown University.

F. International Forums

As appropriate, the Board intends to participate in international discussions on issues of relevance and interest. For example, Vice Chairman Alan Raul represented the Board as a member of the U.S. delegation to the 28th International Data Protection and Privacy Commissioners' Conference in London on November 2 and 3, 2006. This is an annual gathering of the various European Union and other International Data Protection officers. The U.S. has observer status to this conference. The delegation is led by the Department of Homeland Security and also includes representatives from the Department of Justice and Federal Trade Commission.

DRAFT

V. ISSUE IDENTIFICATION, PRIORITIZATION, AND DISCUSSION

As previously explained, IRTPA vests the Board with the broad mandate to provide advice and oversight concerning "regulations, executive branch policies, and procedures (including the implementation of such regulations, policies, and procedures), related laws pertaining to efforts to protect the Nation from terrorism, and other actions by the executive branch related to efforts to protect the Nation from terrorism."[45] Consistent with these statutory responsibilities, the Board considered how it could set its scope, agenda, and methodology in order to advise the President in as effective a manner as possible and in a manner that will bring the greatest value to the American people. To these ends, the Board began to identify and evaluate proposed and existing programs and policies that fall within its statutory mandate. Obviously, the list of policies and programs warranting the Board's attention will evolve over time. Additionally, as new policies are considered, developed, and implemented, the Board's identification of priorities will necessarily change as well.

As a general matter, the Board encounters and engages issues using one of three approaches:

- **Vertical Review**: At the direction of the President, through the request of an Executive Branch department or agency head, or as a result of self-initiation, the Board engages in an in-depth review and analysis of a particular policy or program.

Deleted:

- **Horizontal Review**: The Board examines an issue as part of existing policy development and implementation processes within the Executive Office of the President and the Executive Branch. The Office of Management and Budget (OMB) has integrated the Board into the Legislative Referral Memorandum (LRM) process. Through this process, the Board reviews Administration-wide policies, regulations, and programs that involve its statutory mission.

Deleted: that presently exist

Deleted: its

Deleted: as part of the regular clearance process

- **Initial Spot Review**: The Board informally gathers basic information on a policy, program, or issue that Board Members believe could implicate privacy and civil liberties concerns. This approach allows the Board to determine whether a more formal review is necessary.

[45] IRTPA § 1061(c)(2)(A).

DRAFT

A. Scope and Process

In construing the mandate contained in IRTPA, the Board has initially determined that it will focus its efforts on issues concerning U.S. Persons[46] or occurring on American soil. As a result, it will not evaluate specific issues associated with the uniformed services' efforts against terrorism or activities directed against non-U.S. persons abroad. IRTPA instructs the Board to ensure the consideration and protection of "privacy and civil liberties" but neither defines this phrase nor guides the Board in determining whose privacy and civil liberties should warrant the Board's attention. In order to maximize the Board's effectiveness and to prevent the diffusion of its limited resources across too many programs, the Board has elected to concentrate on the United States and U.S. Persons.[47]

Deleted: conducted abroad

In making this decision, the Board considered the structure and purpose of IRTPA, its legislative history, common canons of statutory construction, and how to carry out its statutory mandate most effectively. As an initial matter, the Congressional findings in IRTPA concerning the Board suggest that "privacy and civil liberties" should have a domestic focus by "call[ing] for an enhanced system of checks and balances to protect the precious liberties that are vital to *our* way of life."[48] IRTPA – particularly the title that contains the Board[49] – has a domestic focus,[50] does not generally address military or diplomatic actions abroad, and does not reference interrogation, non-U.S. detention, or rendition practices. Moreover, the term "civil liberties" refers to the rights guaranteed by the Constitution and, according to some definitions, rights protected under Federal civil rights statutes. These rights have been held to apply, in general, to individuals located inside the United States and to U.S. Persons abroad.

Deleted: Privacy

[46] A "U.S. person" is defined, *inter alia*, as a United States citizen and a lawful permanent resident alien. *See, e.g.*, 50 U.S.C. § 1801(i); Executive Order 12333 § 3.4(i).

Formatted: Space After: 6 pt

Deleted: "

Deleted: "

Formatted: Font: Times New Roman, 12 pt

Formatted: Left

[47] The Board reserves the right to revisit this determination as circumstances or events may warrant.

[48] IRTPA § 1061(a)(2) (emphasis added). Indeed, the findings preceding the formal creation of the Board link the operation of the Board to the "potential shift of power and authority to the Federal Government . . . [i]n conducting the war on terrorism." *Id.* § 1061(a)(1).

[49] Title I – the portion of the Reform Act where Congress placed the Board – largely confines itself to organizational and structural matters.

[50] For example, the statute attempts to improve national security through a variety of actions, including restructuring the Federal intelligence-gathering apparatus, *id.* §§ 1011-1023, strengthening security measures for cargo, *id.* §§ 4051-54, transportation, *id.* §§ 4011-29, and border enforcement, *id.* §§ 5101-5204, and reforming certain immigration laws. *Id.* §§ 5401-5506.

DRAFT

Legislative history – in the form of the 9/11 Commission Report and in Senate debate accompanying passage of IRTPA – also contains a domestic focus. In its preface to recommending the creation of the Board, the Commission Report highlighted the impact of its recommendations on U.S. Persons' rights: "Many of our recommendations call for the government to increase its presence *in our lives* – for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies."[51] The Commission connected this potential harm to domestic liberties to the Board's charge: "At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend *our* civil liberties."[52] Similarly, during debate on the IRTPA conference report, numerous Senators emphasized Congress' desire to "protect the lives of *Americans*, and [to] protect *their* liberties. That is what the Board is setting out to do."[53]

Certain canons of statutory construction, including the presumption against extraterritoriality,[54] also suggest that IRTPA's provisions authorizing the Board should not reach beyond the Nation's borders. Additionally, the Board is reluctant to oversee traditional Commander-in-Chief authorities – including combat operations – without a specific and express legislative mandate.

Comment [DOJ10]: Although we agree with the application of this principle to the operations of the PCLOB, it is not clear that it is equally applicable to all other provisions of the IRTPA. Therefore, we recommend modifying the sentence as such, which avoids the more sweeping assertion that none of IRTPA's provisions should have any extraterritorial effect.

Deleted: text

Formatted: Font: Times New Roman, 12 pt

[51] 9/11 COMMISSION REPORT at 393-94 (emphasis added).

[52] *Id.* at 395 (emphasis added).

[53] *Debate on the Conference Report of the Intelligence Reform and Terrorism Prevention Act of 2004*, 150 Cong Rec 11939, 11949 (Dec. 8, 2004) (statement of Senator Durbin) (emphases added); *see also id.* at 11939 ("The creation of this Board is intended to ensure that at the same time we enhance our Nation's intelligence and homeland defense capabilities, we also remain vigilant in protecting *the civil liberties of Americans*.") (statement of Senator Dodd) (emphasis added); *id.* at 11978 ("The bill provides *protections for the rights of Americans* by creating a Privacy and Civil Liberties Oversight Board . . . .") (statement of Senator Mikulski) (emphasis added); *id.* ("While Americans are more willing to give up some of their privacy after 9/11, necessary intrusions must be carefully balanced against the *rights of U.S. citizens* and I believe the Board will help maintain the balance.") (statement of Senator Reed) (emphasis added).

Deleted: i

[54] *See, e.g.*, *Small v. United States*, 544 U.S. 385, 388-89 (2005) (noting that courts begin with "legal presumption that Congress ordinarily intends its statutes to have domestic, not extraterritorial, application"); *Arc Ecology v. United States Dep't of the Air Force*, 411 F.3d 1092, 1097 (9th Cir. 2005) ("Courts must assume that Congress legislates with knowledge of the presumption that a statute is primarily concerned with domestic conditions.") (internal quotation marks omitted).

DRAFT

Moreover, construing the scope of the Board's mandate substantially implicates questions regarding how best to allocate time and resources. The Board has decided to use these resources in a manner to serve the greatest number of United States citizens and U.S. Persons. Congress stands in a stronger position to oversee American anti-terrorism activities conducted abroad than the Board or its Members.

In addition to determining the general reach of its mandate, the Board established a standardized means to evaluate how well privacy and civil liberties have been considered in the development and implementation of anti-terrorism policies and programs. To that end, the Board has developed an "issues and process analysis methodology" that will bring full and consistent consideration of all issues that come before it.[55] This methodology allows the Board to consider separate substantive questions and the extent to which privacy and civil liberty officers within the relevant agency have meaningfully participated in the development and implementation of the policy or program. The methodology takes into account five large issues, as well as a number of subsidiary questions, including:

Deleted: considers

- The scope of the program
- The program's legal basis
- How the program supports efforts to protect the Nation against terrorism from the perspective of managing risk to privacy or to survival
- The extent to which officials within the relevant department or agency analyzed the privacy and civil liberties interests implicated by the policy, program or issue, including factors such as
    - **Privacy:** *How does the program affect individuals' ability to control how personal information about them is collected, used, maintained, or shared?*
    - **Fairness:** *Does the program treat individuals fairly at every step?*

[55] The Board wishes to acknowledge and thank Jim Harper, Director of Information Policy Studies at the Cato Institute, and the Department of Homeland Security Data Privacy and Integrity Advisory Committee, on which Mr. Harper sits, for their guidance and earlier work product, upon which much of this is based. *See, e.g., Framework for Privacy Analysis of Programs, Technologies, and Applications*, Department of Homeland Security Data Privacy and Integrity Advisory Committee, Report No. 2006-01 (March 7, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf (last accessed Jan. 29, 2007).

Deleted: 6

- **Civil Liberties:** *Does the program limit individual civil liberties in some dimension? What specific Constitutional or statutory interests are affected?*

- **Respect for the Individual:** *Does the program adequately preserve, to the extent possible, human dignity, autonomy, freedom of thought, expression and association?*

- **Data Security:** *How is personal information secured against threats to privacy and integrity?*

- Processes employed by the government to review privacy and civil liberties interests. This factor considers the existence and format of review procedures, how the government ensures that employees follow these procedures, the training required of employees, and how the government updates its policies.

With respect to internal deliberations, the Board has formalized procedures to allocate work and assignments among Board Members. These procedures have allocated assignments to, among others: Vice Chairman Raul to coordinate the Board's efforts concerning watch list redress procedures; Vice Chairman Raul and Member Davis to examine the NSA's surveillance activities; Member Frank Taylor to examine the Department of Defense Counterintelligence Field Activity (CIFA) TALON program; and Member Davis to examine elements of the reauthorized USA PATRIOT Act.

Deleted: Terrorist S

Deleted: P

Deleted: rogram

The Board has also developed a standardized format for reporting internal deliberations and investigations and offering recommendations to the full Board. This report format includes background information, the legal authority underlying a given program or policy, the existing privacy and civil liberties infrastructure, benefits of the program or policy, privacy concerns, sources consulted, an evaluation of the consideration of privacy and civil liberties interests in the development or implementation of the program or policy, and recommendations to the Board. These pre-decisional reports are considered by the full membership of the Board at its regular meetings.

Comment [OIRA11]: Is this report posted to the website (or can it be)?

Formatted: Font: Times New Roman

B. Specific Issues, Policies, Procedures, and Regulations

Employing this standardized methodology and operating within its statutory mandate, the Board has evaluated numerous proposed and currently existing terrorism-prevention policies, regulations, statutes, and other Executive actions. Some issues came to the Board's attention through its numerous meetings with privacy advocacy organizations, Executive officials, and Congressional leaders. The Board engaged other issues because media reports brought them to its attention, and other matters arose simply because the Board has begun to integrate itself into the regular Executive decision-making and policy

Deleted: the public's

DRAFT

implementation processes. In all of its efforts, the Board has had the opportunity to ask whatever questions it desired and has received answers to those questions. The following list of matters on which the Board has offered advice and oversight is intended not to be exhaustive but rather to offer a representative sample of issues that the Board has considered during its relatively brief existence. The Board is careful below not to reference facts, issues, or materials of a classified nature.

1. Oversight of Existing Federal Anti-terrorism Policies and Programs

The Board has begun its efforts to review some of the Federal government's most sensitive and far-reaching surveillance programs. As discussed below in greater detail, these programs include National Security Agency surveillance programs (such as the former Terrorist Surveillance Program (TSP) and the current program governed by the Foreign Intelligence Surveillance Court) and the Terrorist Finance Tracking Program (TFTP). The Board also conducted a review of the National Implementation Plan (NIP).

Deleted: the
Deleted: Terrorist Surveillance Program (TSP)
Deleted: ,
Deleted: SWIFT
Deleted: n

At its first meeting on March 14, 2006, the Board determined that it would have an on-going interest in monitoring the government's various surveillance programs. In order to bring any kind of value to their analysis, however, the Members decided that they first had to understand fully the scope of the government's efforts to protect the Nation against terrorism. Consequently, the Board undertook an extensive effort of educational due diligence. The Board believes that receiving premature briefings on any specific program without understanding the full context in which that program operates would not serve to help it fulfill its statutory mission.

The Board has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism. The Board has examined the agencies' and departments' mission and legal authorities, as well as their operational methodologies and privacy and civil liberties training, reporting, and auditing programs.[56]

Following the Board's educational efforts, and with the support of the Attorney General, the Director of National Intelligence, and the President's Chief of Staff, the Board formally requested a briefing on the TSP and TFTP in September 2006. The President's approval followed promptly, and the briefings were immediately scheduled.

Deleted: SWIFT
Deleted: ,

[56] For example, the Board's Vice Chairman and Executive Director attended a session of the standard National Security Agency employee privacy training given to all new employees and once every other year to all current employees. This training is based, among other authorities, on the requirements of USSID-18, which regulates the collection and use of information on U.S. Persons within the signals intelligence community.

Deleted: session

DRAFT

- *Terrorist Surveillance Program and January 10, 2007 Orders of the Foreign Intelligence Surveillance Court*

The Board devoted substantial time and focus in its first year of operation to reviewing anti-terrorist surveillance conducted by the National Security Agency (NSA) and the Terrorist Surveillance Program (TSP) described by the President on December 17, 2005.[57] The TSP involved surveillance of communications where one party to the communication is outside the United States and the government has probable cause to believe that at least one party to the communication is a member or agent of al Qaeda, or an affiliated terrorist organization.

Deleted:

Deleted: As stated by the President, t

The Board's review of the NSA's surveillance activities was conducted in the course of various briefings by senior NSA personnel, including the Director, and through briefings, questioning, and other interaction with analysts and program operators. Board members repeatedly visited NSA and observed the physical operations where the relevant surveillance is conducted. In particular, the Board reviewed material supporting the government's determination that there was probable cause to believe that at least one of the parties to a surveilled communication was a member or agent of al Qaeda, or an associated terrorist organization.

Deleted: under the TSP

The Board also received briefings and had opportunities to question NSA lawyers from the Office of General Counsel, Inspector General officials, and other knowledgeable personnel. The Board discussed TSP with the Attorney General Alberto Gonzales, the Acting Assistant Attorney General for the Office of Legal Counsel Steve Bradbury, and the current and former Counsel to the President, among other knowledgeable officials in the Executive Branch.

The Board was briefed on the multiple levels of review, approval and oversight for conducting this surveillance. At the NSA, operators must carefully justify tasking requests, and multiple levels of review and approval are required to initiate collection. Ongoing audits and legal reviews are conducted by the NSA's

[57] As noted below, the Board reviewed the operations of both the TSP (which has now ceased) and the surveillance program governed by the Foreign Intelligence Surveillance Court (FISC).

Formatted: Font: Times New Roman, 12 pt

Formatted: Space After: 6 pt

Deleted: b

Formatted: Font: Times New Roman, 12 pt

DRAFT

Office of Inspector General, General Counsel and Signals Intelligence Directorate Office of Oversight and Compliance. No surveillance may be conducted without leaving a reviewable audit trail that can be and routinely is subject to extensive continuing examination by Inspector General and Compliance staff.

Deleted: (IG)

Deleted: IG

In addition, the members of the Board reviewed U.S. Signals Intelligence Directive 18 (USSID 18), which reflects the classified guidelines established by the NSA and approved by the Attorney General pursuant to Executive Order 12333 to ensure that information about U.S. Persons is protected from improper or excessive collection, dissemination and distribution.[58] The NSA requires all of its personnel holding security clearances authorizing access to certain information to participate in extensive USSID 18 training upon the initiation of access and every two years during which they continue to have access. The Vice Chairman and Executive Director participated in the full USSID 18 training received by NSA personnel in order to examine the extent and quality of the training, and to assess awareness of the need to protect the privacy and civil liberties interests of U.S. Persons among NSA personnel with access to sensitive information.

Deleted: *See, e.g.*, EO 12333 § 2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.")

Deleted: those individuals to

On January 17, 2007, the Attorney General notified Senators Leahy and Specter that a Judge of the Foreign Intelligence Surveillance Court (FISC) had issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (FISC Orders). As a result of the FISC Orders, any electronic surveillance that was conducted under the TSP is now conducted subject to the approval of the FISC. After the FISC Orders were issued, the Board was extensively briefed by both the Department of Justice and NSA regarding this development. Members of the Board also have studied the classified FISC Orders themselves and closely reviewed the classified material submitted to the FISC in connection with the Orders, including the applications, legal memoranda, and supporting declarations.

Deleted: .

Deleted: also

Deleted: ,

Deleted: o

[58] *See, e.g.*, EO 12333 § 2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.").

Formatted: Font: Times New Roman, 12 pt

DRAFT

While the details of the FISC Orders remain classified, we can report in an unclassified format that as a result of the Orders the relevant surveillance is now subject both to extensive ongoing Department of Justice review and to the approval of the FISA Court. The Department of Justice's responsibilities for implementing the Orders are carried out by the new National Security Division in the Department of Justice headed by Assistant Attorney General Kenneth Wainstein, who has briefed the Board.

Deleted: a

Deleted: also

Based upon its review, the Board has concluded that the Executive Branch's conduct of these surveillance activities appropriately considers and reasonably protects the privacy and civil liberties of U.S. Persons. As a result of the new FISA Court Orders, the highly regimented Executive Branch process of justification, review, approval, and auditing has been further augmented by court supervision. This provides reasonable assurance that national security and privacy and civil liberties interests are appropriately balanced. The Board found no evidence or reasonable basis to believe that the privacy and civil liberties of U.S. Persons are improperly threatened or impinged under the surveillance conducted by the Executive Branch, either under the TSP or subsequently under the new FISC Orders. In the opinion of the Board, it appears that the officials and personnel who were involved in conducting the TSP, and who now are responsible for implementing surveillance under the FISC Orders, are significantly aware and respectful of U.S. Constitutional and legal rights and protections for U.S. Persons, and that they are actively committed to protecting privacy and civil liberties of U.S. Persons in conducting such surveillance.

Comment [DOD12]: DOD recommends deleting these words. Otherwise, as written, it implies that we DO threaten or impinge on the privacy and civil liberties of US persons who are linked to specified terrorist entities. This would not be an accurate statement.

Deleted: who are not linked to specified terrorist entities

Formatted: Font: Times New Roman, 12 pt

The Board notes that it was not involved in and has taken no position on the original design or legal authorization of the TSP. The Board believes that it is appropriate for it to provide continuing advice and oversight with respect to NSA's surveillance activities.

Deleted: the TSP

Deleted: and other surveillance programs

- *National Implementation Plan*

On November 28, 2006, at the National Counterterrorism Center (NCTC), the Board was briefed on the National Implementation Plan (NIP). This plan was approved by the President in June, 2006, and is intended to coordinate and integrate all instruments of national power in a unified effort to protect the Nation against

DRAFT

terrorism. Toward that end, it assigns hundreds of specific tasks to various Federal departments and agencies. Participating departments and agencies are now adopting and implementing their own supporting plans, and an annual strategic review of the entire NIP is in progress. The Board is working with NCTC to ensure that it has access to NIP tasks and activities that could raise privacy or civil liberties concerns.

Deleted: visibility

Deleted: into

Comment [DN113]: NIP Strategic Review began at the beginning of 2007, not in June 2007.

Deleted: will be conducted in June, 2007. The Board will be integrated into that strategic review

Formatted: Font: Times New

Deleted:

- *Terrorist Finance Tracking Program*

Also on November 28, at the Treasury Department, the Board was briefed on the Terrorist Finance Tracking Program (TFTP) by Stuart Levey, Under Secretary for Terrorism and Financial Intelligence, and Janice Bradley Gardner, Assistant Secretary for Intelligence and Analysis. Under this program, intelligence analysts review records acquired through administrative subpoenas from the Society for Worldwide Interbank Financial Telecommunication to locate financial connections to known or suspected terrorists. This program also predates the Board's existence.

Deleted: administratively-acquired

Deleted: (

Deleted: SWIFT

Deleted: TFTP)

In each briefing, Board members were free to engage in a probing inquiry and ask unfettered questions, all of which were answered. Following each briefing, the Board met to consider further areas of inquiry, additional issues associated with these specific programs to address, and underlying documents to review. Chairman Carol Dinkins has requested Vice Chairman Alan Raul and Member Lanny Davis to coordinate continuing activities with NSA and Member Frank Taylor to coordinate continuing activities with regard to the National Implementation Plan. These initial briefings were the beginning of the Board's review of these specific programs, not the totality of its involvement.

In addition to these three anti-terror programs – NIP, TFTP, and NSA surveillance activities – the Board examined a variety of other programs and policies:

Deleted: —

Deleted: SWIFT

Deleted: TSP

Deleted:

Deleted: —

Deleted:

- *Department of Defense CIFA TALON Program*

At the direction of the Board, Member Francis X. Taylor reviewed the Department of Defense Counterintelligence Field Activities (CIFA) Threat and Local Observation Notices (TALON) program. Within the last year, certain media reports alleged that the CIFA, through the TALON program, had monitored and collected information on U.S. Persons arising out of domestic activities that did not appear to present a threat to national security. During a May meeting of the Board, Chairman Carol E. Dinkins asked

Deleted: have

Member Taylor to gather background information on the alleged inappropriate activities, determine whether DOD had responded to such reports and the results of that response, and make recommendations as to whether additional review by the full Board was required. In carrying out the Chairman's charge, Member Taylor and Board staff met frequently with those who implemented and continued to oversee CIFA. Senior policy officials fully answered the Board's questions and provided any materials that were requested. At the conclusion of its investigation, the Board determined that a lack of clear guidance from the Deputy Secretary at the time the program was established and the absence of a designated TALON program manager resulted in an ambiguous program implementation and the improper and unauthorized collection and retention of information on U.S. Persons. The Board also reviewed and endorsed the steps that DOD took prior to the Board's investigation to correct these concerns. For example, the Deputy Secretary had ordered an immediate review of the program and issued additional guidance to clarify the TALON program's scope and to emphasize that the program would be conducted in full compliance with DOD policies and procedures regarding the collection of information on U.S. Persons. CIFA also has purged the TALON system of any inappropriately collected and retained information.

Deleted: oversee

- *Department of State E-Passport Program*

The Board reviewed efforts by the Department of State to distribute a passport containing an embedded data chip that holds personal information on the passport holder. The Board concluded that the *current* design of the passport does not pose substantial privacy concerns because (1) the information contained on the chip is identical to that contained in the actual passport; (2) such information is useless without an actual physical passport; (3) the passport utilizes substantial security protocols (anti-skimming technology, a unique PIN, and a varying identifier that prevents continuous tracking of the chip) to prevent someone from accessing that information remotely and from following an individual; and (4) the chip is engineered in a way that would require the State Department to recall and reissue passports before it could add more information on the chip (thereby preventing the government from easily amending the current contents of the passport). The Board stated that it would revisit this issue in the event the State Department desired to alter the program by including more information on the chip (such as new biometric

Deleted: civil liberties

measures like an iris or fingerprint scan that are in addition to the existing digital photograph that enables the biometric comparison using facial recognition technology), altering its border inspection procedures (e.g., to allow a chip to act as a proxy for a physical passport), or changing the schematics of the chip.

Deleted: eye

- *Passenger Name Recognition (PNR)*

The Board was briefed on U.S. negotiations with the E.U. over the collection and dissemination of passenger name records for flights between the two jurisdictions. The briefing provided the Board with substantive discussions of the negotiations, as well as how privacy and civil liberties officers within DOJ (Jane Horvath, Chief Privacy and Civil Liberties Officer) and DHS (John Kropf, Director of International Privacy Programs) were involved in those negotiations. The Board is satisfied with the significant role these privacy and civil liberties officers played in these negotiations.

Deleted: the

- *Department of Homeland Security US-VISIT Program*

The Board is currently examining the privacy and civil liberties protections contained in the US-VISIT program. US-VISIT facilitates a process that collects and retains biometric and biographic information regarding aliens who enter and leave the country and who apply for immigration benefits. Although the program largely concerns non-U.S. person aliens, a proposed rulemaking would extend its reach to include all aliens, including Legal Permanent Residents (who qualify as U.S. Persons). The greatest civil liberties questions center on how information collected as part of US-VISIT will be shared within the government and with outside entities.

- *USA PATRIOT Act Review*

The 2006 reauthorization of the USA PATRIOT Act included over 30 new civil liberties protections. Member Lanny Davis visited the Department of Justice on November 17, 2006 to be briefed on these new protections by staff with the new National Security Division. Member Davis has been tasked by the Board to continue working with the Department of Justice to monitor implementation and operation of these protections.

DRAFT

2. Examples Where the Board Has Offered Advice Regarding the Development of a Policy, Program, Regulation, or Statute

- *Watch List Redress*

At the request of the Board, Vice Chairman Alan Raul has undertaken the coordination of efforts among the various relevant Federal departments and agencies to establish a formalized, unified, and simplified redress procedure for individuals with adverse experiences with the government's watch list or during screening processes. Both government officials and non-governmental advocacy experts repeatedly raised this issue as an area where the Board could bring focus, organization and prioritization.

The Terrorist Screening Center (TSC) is charged with maintaining the U.S. government's consolidated terrorist watch list, which contains the identifying information of all known or appropriately suspected terrorists. Thirteen months after the Center began operations, it established a formal watch list redress process. The process allowed agencies that used the consolidated terrorist watch list data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appeared those complaints were watch list related. The goal of the redress process is to provide timely and fair review of individuals' complaints, and to identify and correct any data errors, including errors in the terrorist watch list itself.

TSC's redress process consists of a procedure to receive, track, and research watch list-related complaints and to correct the watch list or other data that caused an individual unwarranted hardship or difficulty during a screening process. Throughout 2005, TSC worked closely with screening agencies to establish a standardized process for referral of and response to public redress complaints. TSC also worked with federal law enforcement agencies and the intelligence community, each of which may nominate individuals to the watch list, to review the redress complaint of any individual on the terrorist watch list, evaluate whether that person was properly listed and that the associated information was correct, and make any corrections that were appropriate, including removal from the watch list when warranted.

Deleted: ,

Deleted: was causing

Deleted: watch

DRAFT

In the fall of 2005, TSC undertook to document formally the participating agencies' mutual understanding of their obligations and responsibilities arising out of the watch list redress process. Competing priorities within participating agencies, however, slowed progress. On June 20, 2006, Vice Chairman Raul convened a meeting of all relevant agencies and called for a renewed effort to prioritize this project. In attendance were representatives from TSC, the Departments of State, Defense, Treasury, Justice, and Homeland Security, the Office of the Director of National Intelligence, the FBI, the CIA and the National Counterterrorism Center.

Deleted: at the White House

The resulting draft Memorandum of Understanding (MOU) is a constructive and positive step intended to secure a commitment from these agencies that participate in the watch list process actively to engage in and support the redress process. The MOU resulted from a six-month period of negotiations between the agencies mentioned previously. Vice Chairman Raul convened a final working group meeting on November 30, 2006; in January 2007, a final draft of the MOU was approved and submitted for the signature of the heads of these agencies.

The MOU sets forth the existing multi-agency redress process in significant detail, from receipt of an individual's complaint to the response sent by the screening agency. Among other things, the MOU establishes obligations for all parties to secure personal information, update and correct their own record systems, and share information to ensure redress complaints are resolved appropriately. Each participating agency must also commit to providing appropriate staff and other resources to make sure the redress process functions in a timely and efficient manner. Finally, each agency must designate a senior official that is responsible for ensuring the agency's full participation in the redress process and overall compliance with the MOU.

Once the MOU has been executed and implemented, the Board intends to continue efforts to bring all possible transparency and public understanding to this process.

- *Department of Defense Report of the Technology and Privacy Advisory Committee*

In September, 2006, the Department of Defense forwarded to the Board the recommendations of the March 2004 Report of the Technology and Privacy Advisory Committee (TAPAC) to the Secretary of Defense.[59] Five of the twelve recommendations required action on a government-wide basis beyond the authority of the Department of Defense. The Board is currently evaluating that Report to determine the extent to which the government has already implemented those recommendations and what additional steps the government should take to complete those recommendations.

- *Administration Clearance Processes*

As mentioned above, the Board has been fully integrated into the various Administration and Executive Branch program and policy clearance processes, including the OMB Legislative Referral Memorandum (LRM) process. As such, it regularly receives and is invited to comment on policy initiatives, programs, regulations, proposed legislation, and public remarks by agency officials that may have privacy or civil liberties implications.

3. Information Sharing

IRTPA called for the creation of the Information Sharing Environment (ISE). The ISE is an approach that facilitates the sharing of information relating to terrorism by putting in place the processes, protocols, and technology that enable the sharing of this information among Federal, State, local, tribal and private sector entities, and foreign partners. The ISE brings together, aligns and builds upon existing information sharing policies, business processes and technologies (systems), and promotes a culture of information sharing through increased collaboration. IRTPA also established the Program Manager for the Information Sharing Environment with government-wide authority to plan, oversee, and manage the ISE. The Program Manager assists the President and government agencies in the development and operation of the ISE and monitors and assesses its progress.

Deleted: 3.
Formatted: Bullets and Numbering
Formatted: Indent: First line: 0.5", Space Before: Auto, After: 12 pt
Formatted: Font: Times New Roman, 12 pt
Deleted: as well
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Formatted: Font: Times New Roman, 12 pt
Deleted: by
Formatted: Font: Times New Roman, 12 pt
Deleted: (PM-ISE)
Deleted:
Deleted: ¶

[59] *Safeguarding Privacy in the Fight against Terrorism* (March 2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf (last accessed Dec. 29, 2006).

DRAFT

To guide efforts to establish the ISE and implement the requirements of IRTPA, on December 16, 2005, President Bush issued a Memorandum to the Heads of Executive Departments and Agencies. This Memorandum delineated two requirements and five guidelines which prioritize efforts that the President believes are most critical to the development of the ISE and assigns Cabinet officials responsibility for resolving some of the more complicated issues associated with information sharing. The five guidelines are: (1) Set Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE; (2) Create Common Framework for Sharing Information Between and Among Federal Agencies and State, Local and Tribal Governments, Law Enforcements Agencies and the Private Sector; (3) Standardize Procedures for Sensitive But Unclassified Information; (4) Facilitate Information Sharing with Foreign Partners; and (5) Protect the Information Privacy Rights and Other Legal Rights of Americans.

IRTPA required that these guidelines be drafted and implemented in consultation with the Board. And with regard to all five sets of guidelines, the Board's Executive Director is a member of the White House Information Sharing Policy Coordination Committee which sits above all the working groups and directly below the Deputies and Principals Committees.

The President assigned various agencies the lead in developing the five sets of guidelines. The Department of Justice and the Office of the Director of National Intelligence were jointly assigned the lead in developing Guideline 5, now referred to as the ISE Privacy Guidelines. Within those agencies, the lead was assigned to Jane Horvath, DOJ's Chief Privacy and Civil Liberties Officer, and Alex Joel, ODNI's Civil Liberties Protection Officer. This ISE Privacy Guidelines drafting group spent April through November, 2006, soliciting comments and working with the Program Manager and White House staff, including Homeland Security Council staff and Board staff.

On May 16, 2006, the Board held its fourth meeting and, among other things, was briefed on the ISE by Director of National Intelligence John Negroponte and Program Manager for the Information Sharing Environment Ambassador Thomas McNamara. On June 26, at the Board's eighth meeting, the working group leaders Alex Joel and Jane Horvath briefed the Board specifically on the ISE Privacy Guidelines.

Deleted: .

Comment [Treas14]: The Dec. 16 Memo specified the Dept. Heads responsible for each guideline – the PM was to provide support to these Departments for the implementation/drafting of these guidelines (see page 2 of the Memo)

Deleted: ¶
IRTPA also called for the establishment of an Information Sharing Environment (ISE) and authorized the appointment of a Program Manager to oversee the implementation of the ISE. On December 16, 2005, prior to the Board's existence, the President issued a message to Congress and a Memorandum to the Heads of Executive Departments and Agencies establishing the format of the ISE and instructing the Program Manager to

Deleted: support

Deleted: oversee the drafting of

Deleted: draft

Deleted: five sets of ISE guidelines: (1) Set Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE; (2) Create Common Framework for Sharing Information Between and Among Federal Agencies and State, Local and Tribal Governments, Law Enforcements Agencies and the Private Sector; (3) Standardize Procedures for Sensitive But Unclassified Information; (4) Facilitate Information Sharing with Foreign Partners; and (5) Protect the Information Privacy Rights and Other Legal Rights of Americans. ¶

Formatted: Font: Times New Roman, 12 pt

Comment [Treas15]: The Dec. 16 Memo specified the Dept. Heads responsible for each guideline [see Memo]

Deleted: Program Manager

Formatted: Font: Times New Roman, 12 pt

Deleted: o

Deleted: Guideline 5

Deleted: and May

Deleted: Guideline 5

DRAFT

On November 16, 2006, Director John Negroponte sent to Congress the ISE Implementation Plan, which discusses how to bring about an information sharing environment. Although the parameters of the plan were adopted in December 2005, prior to the Board's existence, the Board's Executive Director did offer substantive advice regarding its content. On November 22, 2006, the President approved the Guidelines 1, 2, 4, and 5 report, including the recommendation that the ISE privacy guideline be issued. These were subsequently released to the public by the Program Manager.

The ISE Privacy Guidelines (Protect the Information Privacy Rights and Other Legal Rights of Americans) work in conjunction with the other information sharing guidelines, requiring each set to address its specific area of interest in a manner that protects the privacy rights and civil liberties of Americans. The guidelines must also implement provisions of Executive Order 13388, which requires agencies to "protect the freedom, information privacy, and other legal rights of Americans" while sharing terrorism information.

The ISE Privacy Guidelines regulations establish an information sharing framework that balances the dual imperatives of sharing information and protecting privacy by establishing uniform procedures to implement required protections in unique legal and mission environments. In addition, the framework establishes an ISE privacy governance structure for compliance. The framework attempts to strike a balance between consistency and customization, substance and procedure, oversight and flexibility. It also builds upon existing resources within Executive agencies and departments for implementation.

The ISE Privacy Guidelines are based on a set of core principles that requires agencies to: identify any privacy-protected information to be shared; enable other agencies to determine the nature of the information and whether it contains information about U.S. Persons; assess and document applicable legal and policy rules and restrictions; put in place accountability and audit mechanisms; implement data quality and, where appropriate, redress procedures; and identify an ISE Privacy Official to ensure compliance with the guidelines.

The ISE Privacy Guidelines regulations also require Federal departments and agencies to designate an ISE Privacy Official to oversee the full implementation of the privacy regulations. The ISE Privacy Official is the department or agency's senior privacy official (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency.

The ISE Privacy Guidelines also provide for an ISE Privacy Guidelines Committee, consisting of the ISE Privacy Officials of the departments and agencies comprising the Information Sharing Council (ISC), and chaired by a senior official designated by the Program

Deleted: O
Deleted: O
Deleted: n November 16
Deleted: 16
Deleted: , 2006,
Deleted: D
Deleted: Director John Negroponte sent to Congress the ISE Implementation Plan, which discusses how to bring about an information sharing environment. Although the Board did not have sufficient time to comment in detail on the parameters of the plan itself (adopted in December
Deleted: ,
Deleted: 2005 and implemented in early 2006) its Executive Director did offer substantive advice regarding its content. On November 22, 2006, the President approved issuance of Guidelines 1, 2, 4, and 5, which were subsequently released to the public by the Program Manager
Deleted: to the public December 4, 2006
Deleted: ¶
Deleted: Guideline 5
Deleted: s
Deleted: the other four sets of
Deleted: (October 25, 2005)
Deleted: The Guideline 5
Deleted: Guideline 5
Deleted: is
Deleted: The Guideline 5
Deleted: Guideline 5
Deleted: s

DRAFT

Manager. Working closely with the Privacy and Civil Liberties Oversight Board as it exercises its oversight mission, the committee will seek to ensure consistency and standardization in implementation, as well as serve as a forum to share best practices and resolve inter-agency issues. The ISE Privacy Guidelines Committee will continually refine its guidance as the ISE develops and as specific sharing mechanisms are institutionalized. The Program Manager has designated Alex Joel and Jane Horvath to serve as co-chairs of this ISE Privacy Guidelines Committee, which will include the Board's Executive Director as a member.

The Board instructed its staff to meet with the Program Manager and provide options concerning its on-going oversight role and how that role can be most effectively and efficiently exercised.

DRAFT

VI. THE YEAR AHEAD

After working to establish the foundation discussed throughout this report, the Board looks forward to continuing to fulfill its statutory responsibilities in the upcoming year. The Board intends to utilize the knowledge and trust built over the last year to engage, as time and resources allow, issues that will have the greatest impact on the greatest number of U.S. Persons. While it is impossible to foresee all issues that may arise in the coming year warranting the Board's attention, issues which the Board presently intends to pursue include:

- *Information Sharing Environment (ISE).* As discussed above, the Board is specifically charged with responsibility for reviewing the terrorism information sharing practices of executive branch departments and agencies to determine adherence to guidelines designed to appropriately protect privacy and civil liberties. Accordingly, the Board was integrated into the process chaired by the Program Manager for the development and implementation of appropriate information sharing guidelines for Federal departments and agencies. The Board will work with the Program Manager to institutionalize its implementation oversight role.

- *Government surveillance operations.* The Board will continue to exercise its oversight role over terrorist surveillance.

- *Terrorist watch list issues.* The Board played a role in coordinating efforts among the various Federal departments and agencies to establish a unified, simplified redress procedure for individuals with adverse experiences during screening processes. The execution of an interagency memorandum of understanding on redress procedures is only a first step in establishing a simple, transparent process. The Board will continue its efforts to promote this process.

- *USA PATRIOT Act and National Security Letters (NSLs).* The 2006 reauthorization included over thirty new civil liberties protections. The Board will work with the Department of Justice to monitor implementation of these protections.

- *Federal data analysis and management issues.* Board Members intend to enhance significantly their understanding of issues associated with data mining activities, data sharing practices, and governmental use of commercial databases. This level of understanding will assist the Board in its review of many Federal anti-terrorism programs. Toward this end, the Board will follow up on recommendations of the March, 2004 report of the Technology and Privacy Advisory Committee (TAPAC) to the Secretary of Defense, *Safeguarding Privacy in the Fight Against Terrorism.*

Deleted: <#>*Presidential Directive.* The Board wishes to obtain from the President a charge to the Executive Branch stating clearly the authority of the Board and the level of cooperation and access he expects the Board to have when working with relevant departments and agencies, as well as establish a systematic basis to meet with and report to the President regarding appropriate consideration and adequate protection of privacy and civil liberties in the Nation's anti-terrorism activities.¶

Deleted: T

Deleted: The five sets of guidelines were largely completed in 2006.

Comment [MAR16]: HSC staff to recommend alternative language.

Formatted: Font: Times New Roman

Formatted: Font: Times New Roman

Formatted: Font: Times New Roman

Deleted: significantly

Deleted:

DRAFT

- *U.S. Persons Guidelines*. These guidelines limit the government's ability to collect, retain, and distribute intelligence information regarding U.S. Persons. These guidelines are applicable to agencies in the intelligence community pursuant to Executive Orders 12333 and 13284. As was noted in the 2005 report to the President on Weapons of Mass Destruction, these rules are complicated, subject to varying interpretations, and substantially different from one agency to another. The Attorney General and the Director of National Intelligence have established a staff level working group to review these guidelines and propose appropriate reforms. The Board intends to participate in this process.

- *State and local fusion centers*. State and local law enforcement entities are establishing joint centers where they share information and data of value to their common missions. Federal agencies are developing partnerships with these centers. The Board will review these sharing practices to ensure that privacy rights and civil liberties concerns are taken into appropriate consideration.

- *National Implementation Plan*. The Board will continue to monitor those tasks and activities that might raise privacy or civil liberties concerns.

- *Department of Homeland Security Automated Targeting System* (ATS). ATS is a decision support tool used by Customs and Border Protection to assist in making a threshold assessment in advance of arrival into the U.S. based on information that DHS would otherwise collect at the point of entry. The Board intends to review this system.

Administratively, the Board will focus on further developing its staff resources by supplementing the permanent staff with detailees from the intelligence, law enforcement, and technology communities. Depending on developing priorities, the Board intends to bring in six detailees for terms of six months to one year.

In addition, recognizing the value and benefit of the public dimension to its responsibilities, the Board will conduct a continuing series of open public forums, perhaps around the country, that will allow interested American citizens to express their concerns with regard to privacy and civil liberties implications in the war against terrorism.

Finally, the Board understands that it may adjust its agenda based on evolving issues and concerns - whether those issues are brought before the Board through its internal role within the Executive Office of the President or through public comment.

Deleted: ,

Deleted: and 13355

Deleted: Federal, s

Deleted: ,

Deleted: The Board will participate in the annual strategic review of the National Counterterrorism Center's National Implementation Plan, which commences in June, 2007.

Deleted: *<i>Material Witness Statute*. As a result of concerns raised at its December 5, 2006 public meeting, the Board will investigate public expressions of concern over how this statute is being used in Federal anti-terrorism efforts.¶

Deleted:

Comment [DHS17]: ATS does not assign "risks scores" to individuals seeking to enter the country. ATS is a decision support tool used by CBP to assist in making a threshold assessment in advance of arrival into the U.S. based on information that DHS would otherwise collect at the point of entry.

This bullet implies that a "risk score" is assigned.

Deleted: The Board plans to investigate how the Department of Homeland Security assesses and assigns "risk" ratings to those seeking to enter the country.

Formatted: Font: Times New

Deleted: The Board intends to seek substantive meetings with the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, and the new Director of National Intelligence and have additional, ongoing meetings with officials and agencies with whom the Board has already met.¶

Deleted: The Board intends to seek substantive meetings with the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the new Director of National Intelligence, and have additional, ongoing meetings with officials and agencies with whom the Board has already met.¶

DRAFT

VII. CONCLUSION

Standing up any new institution takes vision, energy, and commitment. The Board believes it has made substantial solid progress over the past year in setting priorities and integrating itself into existing Executive Branch policy formulation and implementation procedures. The Board is pleased with the enthusiasm and level of support it is receiving, both substantively and administratively, from White House staff, the Executive Office of the President and other Federal departments and agencies essential to the protection of privacy and civil liberties.

Most importantly, as mentioned several times in this report, the Board has established a sound and productive working relationship with the growing universe of privacy and civil liberties professionals within the Executive Branch. Working together, these professionals and the Board are developing a system of mutual trust and support. This relationship is fundamental to the Board's ability to fulfill its role of providing constructive, objective advice to the President and relevant agency heads.

The American people expect the Federal government to protect them from terrorism, and to do so consistent with the Constitution and important American values. The Privacy and Civil Liberties Oversight Board is one of many checks and balances existing within the Federal government to help promote this. It is not a substitute for the President's responsibility to preserve, protect, and defend the Constitution of the United States or the oversight roles exercised by Congress. Instead, it is a significant new body within the Federal government in a position of trust and proximity to the President that can offer an objective assessment of policy initiatives.

The Board Members take their statutory mission and responsibilities seriously and look forward to working with the Executive Branch and Congress[60] in fulfilling them in the upcoming year.

Comment [DOJ18]: We do not understand what is meant by the assertion that the PCLOB is a "body within" or part of the Legislative branch. Therefore, we recommend that the words "and legislative" be deleted from the sentence quoted.

Deleted: and legislative

Formatted: Font: Times New Roman, 12 pt

Formatted: Font: Times New Roman, 12 pt

[60] The 110th Congress is considering whether the Board's present construct, as established by IRTPA, warrants modification. Pending legislative initiatives would remove the Board from the Executive Office of the President, make it an independent agency within the Executive Branch, and provide it with subpoena power. Other proposed changes would keep the Board within the EOP but would require all Members to be nominated by the President and confirmed by the Senate to staggered six year terms, with the Chairman assuming a full-time appointment.

Deleted: DOJ COMMENT: We defer to OMB on whether the accuracy of this footnote, in context, is consistent with the Administration's strongly stated objections to the provisions described in the footnote.

ANSWERS TO POST-HEARING QUESTIONS POSED BY THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRWOMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW TO THE HONORABLE ALAN CHARLES RAUL, ESQ., PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, THE WHITE HOUSE, WASHINGTON, DC

U.S. House of Representatives
Judiciary Subcommittee on Commercial and Administrative Law
July 24, 2007 Hearing

QUESTIONS FOR ALAN CHARLES RAUL
Vice Chairman of the Privacy and Civil Liberties Oversight Board

1. In the Board's June 15, 2007 letter to Governor Kean and Congressman Hamilton, Chair Carol Dinkins states that "there has been no occasion where we have not eventually received all information or cooperation requested" from the Executive branch.

   Please explain any occasions where there was a delay in receiving the information or cooperation requested.

As explained in detail in the Board's 2007 annual report to Congress, the Board spent most of its first several months of existence educating itself and exercising due diligence to become familiar with the activities of the departments and agencies responsible for protecting the Nation against terrorism by meeting with senior officials, examining their missions and legal authorities, learning of their specific programs, and reviewing their operational methodologies and privacy and civil liberties training, reporting, and auditing programs. When the Board requested access to specific programs for review, they were granted without exception.

2. In the Board's June 15, 2007 letter to Governor Kean and Congressman Hamilton concerning questions about the watch list redress project, which you lead, Chair Dinkins stated that the Board intends "to review the process and push for as much transparency as possible."

   What will you and the Board do to ensure that there will be as much transparency as possible?

The Board has been very actively involved in this issue since its original adoption of priorities in the spring of 2006. I believe the Board has played a highly constructive role.

The Terrorist Screening Center (TSC) is charged with maintaining the U.S. government's consolidated terrorist watch list, which contains the identifying information of all known or appropriately suspected terrorists. Thirteen months after the Center began operations, it established a formal watch list redress process. The process allowed agencies that used the consolidated terrorist watch list data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appeared those complaints were watch list-related. The goal of the redress process is to provide timely and fair review of individuals' complaints and to identify and correct any data errors, including errors in the terrorist watch list itself.

TSC's redress process consists of a procedure to receive, track, and research watch list-related complaints and to correct the watch list or other data that caused an individual unwarranted

hardship or difficulty during a screening process. Throughout 2005, TSC worked closely with screening agencies to establish a standardized process for referral of and response to public redress complaints. TSC also worked with federal law enforcement agencies and the Intelligence Community, each of which may nominate individuals to the watch list, to review the redress complaint of any individual on the terrorist watch list, evaluate whether that person was properly listed and that the associated information was correct, and make any corrections which were appropriate, including removal from the watch list when warranted.

In the fall of 2005, TSC undertook to document formally the participating agencies' mutual understanding of their obligations and responsibilities arising out of the watch list redress process. Competing priorities within participating agencies, however, slowed progress. On June 20, 2006, I convened a meeting of all relevant agencies and called for a renewed effort to prioritize this project. In attendance were representatives from the Departments of State, Defense, Treasury, Justice, and Homeland Security, the Office of the Director of National Intelligence, the CIA, the FBI, the National Counterterrorism Center, and TSC.

The resulting draft Memorandum of Understanding (MOU) is a constructive and positive step intended to secure a commitment from these agencies that participate in the watch list process to engage actively in and support the redress process. The MOU resulted from a six-month period of negotiations between the agencies mentioned previously. I convened a final working group meeting on November 30, 2006; in January 2007, a final draft of the MOU was approved and submitted for the signature of the heads of these agencies.

The MOU sets forth the existing multi-agency redress process in significant detail, from receipt of an individual's complaint to the response sent by the screening agency. Among other things, the MOU establishes obligations for all parties to secure personal information, update and correct their own record systems, and share information to ensure redress complaints are resolved appropriately. Each participating agency must also commit to providing appropriate staff and other resources to make sure the redress process functions in a timely and efficient manner. Finally, each agency must designate a senior official who is responsible for ensuring the agency's full participation in the redress process and overall compliance with the MOU.

Unfortunately, under PL 110-53, the current members of the Board will no longer be able serve as of January 30, 2008, namely 180 days from the date PL 110-53 was enacted on August 3, 2007. We hope the new members of the Board will be able to carry on these efforts.

3. Page 22 of the Board's First Annual Report to Congress, states, "In order to maximize the Board's effectiveness and to prevent the diffusion of its limited resources across too many programs, the Board has elected to concentrate on the United States and U.S. Persons." Footnote 46 on page 22 of the Report, however, notes that the Board may revisit this determination.

What was the reason why the Board chose to limit its scope of review?

As there is no express mention in the statute or legislative history suggesting the Board should address issues outside or beyond the United States or U.S. Persons, to maximize the Board's

effectiveness and to prevent the diffusion of its limited resources, the Board determined to focus on the responsibilities directly assigned to it by Congress.

> If Congress appropriated more funds to the Board, would the Board then have the resources to review, for example, the civil liberties questions raised by the detention of detainees at Guantanamo, and meet its mission and mandate in Intelligence Reform and Terrorism Prevention Act of 2004?

As I noted in response to the prior question, the Board did not find any indication by Congress that it should focus on matters outside the United States or beyond U.S. Persons. The service of the current members of the Board has been truncated by P.L. 110-53, so presumably new members of the Board will determine for themselves whether the scope of the Board's activities should be modified. I would note that while P.L. 110-53 significantly amended the Board's charter, it did not expand or clarify responsibilities of the Board with respect to matters outside the United States or beyond U.S. Persons.

> Should Congress express a legislative mandate for the Board to review these areas?

Congress has expressed a revised legislative mandate for the Board in P.L. 110-53 and it apparently chose not to address these areas.

4. What advice and oversight will the Board give with respect to surveillance activities conducted by the National Security Agency, as mentioned on page 29 of the Board's First Annual Report to Congress?

The Board is in the process of determining what activities the current members should engage in during the remainder of their service. Speaking personally, I would anticipate reviewing the impact of the legislation amending FISA on the existing surveillance programs.

5. Please explain the process the Board undertook in concluding that the Executive Branch considered and, most importantly, protected the privacy and civil liberties of U.S. Persons in conducting surveillance under the Terrorist Surveillance Program and the January 10, 2007 Orders of the Foreign Intelligence Surveillance Court.

That process is discussed in detail in the Board's 2007 annual report to Congress (pp. 26-29).

6. Has the Board completed its assessment of the matters raised in the Justice Department Inspector General's report on the use of National Security Letters by the Federal Bureau of Investigation (FBI)?

Yes. I anticipate that the Board's report will be issued presently.

7. What advice and oversight has the Board given the FBI in how that agency should design and implement a program to ensure compliance with statutes, regulations, and policies, especially those regarding the FBI's use of National Security Letters?

The Board's recommendations and findings will be contained in a report for the Attorney General and released to the public.

8. How confident are you that the Department of Defense's Counterintelligence Field Activities did indeed purge the TALON system of all inappropriately collected and retained information, as contended in the Board's First Annual Report to Congress on page 31?

The Board is very confident. And in any event, it should be noted that the Department of Defense announced August 22, 2007 that it is disbanding the entire TALON data base. The Board believes that its efforts, and in particular, those of Member Francis Taylor, were helpful in encouraging the Department of Defense to revisit this program.

9. Please explain why the brief statement on the National Security Letters abuses by the FBI was relegated to the cover letter of the Board's First Annual Report to Congress, and not included as an extensive discussion in the Report.

The prominent placement of the Board's highly critical assessment of the NSL situation in the cover letter transmitting the Board's report to Congress was explained at the July 24, 2007 oversight hearing. The Board's report covered the time period from its first meeting on March 14, 2006 up to March 1, 2007. Given that the Board's review of the FBI matter did not begin until after that date, the Board wanted to ensure that its critique of the NSL situation received significant public attention. Discussion of the NSL problems in the cover letter addressed to the President of the Senate and the Speaker of the House of Representatives assured prominent congressional and public attention to this highly troubling matter.

10. How independent can the Board be when it initially cedes to nearly all the suggestion by the White House Counsel's Office, such as the reference to the Material Witness statute, as Mr. Lanny Davis discusses in his May 14, 2007 letter to the Board?

The White House and inter-agency staffing process produced various editing suggestions for the Board's report. The suggested edit of the Material Witness reference was one of them. This proposed deletion (like the others) was by no means intended – or received – as any kind of binding direction. My recollection is that following a discussion I had with a White House staff member, the White House receded from the proposed deletion. (I discussed it with staff because I was an original proponent of including this Material Witness language in the Board's report.) Indeed, I considered the Material Witness issue to have been very easily resolved to the Board's satisfaction, and any suggestion to the contrary does not comport with my recollection or understanding.

11. What has the Board done to address the concerns Mr. Davis' discussed in his May 14, 2007 letters to the President and to the rest of the Board?

My understanding is that the remaining members of the Board did not agree with Mr. Davis' concerns as articulated in his letters.

12. Mr. Davis has likened the positioning of the Privacy and Civil Liberties Oversight Board within the Executive Office of the President to trying to "fit a square peg in a round hole."

Do you agree with that statement?

No.

13. As a member of the Board, were you required to submit your statement for the July 24, 2007 Subcommittee on Commercial and Administrative Law hearing to the White House for clearance?

I did submit my draft statement for review and comment; and, it is my understanding that, under standard Administration protocols, draft Executive Branch testimony is supposed to be staffed and reviewed through the legislative clearance process administered by OMB. Since the then applicable statutory language governing the Board's activities expressly stipulated that the Board "shall perform its functions within the executive branch and under the general supervision of the President" (P.L. 108-458, Sec 1061(k), consulting the White House was, of course, particularly appropriate.

14. What have been the Board's greatest accomplishments and challenges, to date?

The Board's accomplishments are discussed in great detail in its 2007 annual report to Congress.

Without doubt our greatest accomplishment was standing up a brand new organization. In order to stand up its operation during the first year, the Board allocated its resources among three core areas, discussed below, to build a foundation on which to offer substantive advice and oversight. Activities in these areas have helped the Board establish its viability, subject matter expertise, and credibility. The Board unanimously identified substantive accomplishments in these three areas at the outset as necessary prerequisites for long term success and included them in its first annual agenda, adopted in June 2006.

Organization, Administration and Process. The Board understood that, due to its part-time Membership, it had to establish the means and infrastructure necessary to help it accomplish its statutory mission. Toward that end, it has hired a professional staff, reached agreement with the Director of National Intelligence on the scope and logistics of detailing additional staff from within the Intelligence Community, acquired the necessary security clearances, built out appropriate office space with secured facilities for classified information, and developed a web site for communication with the public. Due to its position within the White House Office, the Board receives additional administrative support from White House staff.

Education and Outreach. The Board has engaged policy officials and experts within the Executive Branch, Congress, the public, and private, non-profit, and academic institutions. It has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism by meeting with senior officials, examining their missions and legal authorities, learning of their specific programs, and reviewing

their operational methodologies and privacy and civil liberties training, reporting, and auditing programs. For example, the Board has met personally, among others, with the Attorney General, the Secretary of the Department of Homeland Security, the Director of National Intelligence, the Directors of the National Counterterrorism Center and National Security Agency, the Information Sharing Environment Program Manager, the Undersecretary of the Treasury for Terrorism and Financial Intelligence, and the President's senior staff. Among other non-governmental experts and advocacy groups, it has met with representatives from the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Markle Foundation, and the American Conservative Union. It also held its first public forum at Georgetown University on December 5, 2006.

As a part of this education and outreach effort, the Board has made it a priority to work with a new and growing network of Executive Branch homeland security professionals specifically dedicated to consideration of privacy and civil liberties issues. The Board considers one of its fundamental responsibilities to foster a sense of community among these new professional privacy and civil liberties officers and members of the relevant professions that have existed within the Federal government for decades – including attorneys, inspectors general, and relevant program policy officials. The Board intends to continue providing these offices with the necessary support to enable them better to accomplish their own responsibilities.

Issue Prioritization. The Board's existing statutory authority is broad. The Board has focused on those issues that could provide the most value for the American people, the President, and the Executive Branch. Policies and programs warranting the Board's attention will evolve over time. Identification of these priorities will necessarily change as new initiatives are considered, developed, and implemented. This report outlines the process and consideration undertaken by the Board in developing and reviewing those issues.

The biggest challenge proved to be convincing a skeptical Congress and privacy community to keep an open mind about the Board's ability to make an important contribution. In addition, I believe that organizing additional public sessions and hiring additional staff took longer than I would have hoped.

15. Can the Board be effective if its members serve on a part-time basis?

Part-time service has the tremendous advantage of allowing senior individuals with considerable experience to provide their independent perspective to the President and Cabinet officials without fear of the repercussions of delivering unwelcome advice or oversight. Of course, there are challenges resulting from the competing demands on the time of part-time, special government employees. On balance, I believe part-time service is beneficial to the Board's ability to serve effectively. Additional staff, however, is desirable in order to ensure that the Board is in a position to probe deeply and persistently into the matters within its jurisdiction.

16. What steps have been taken to replace Mr. Davis on the Board? When can we expect to see his position filled?

Decisions on replacing Mr. Davis are the province of the President. The Board has no role in selecting its own members.

17. What are the Board's major priorities for the coming year?

Our priorities were outlined in the 2007 annual report to Congress. Of course, the current members of the Board may not serve beyond January 30, 2008, pursuant to P.L. 110-53. But to the extent possible, the Board had agreed to pursue the following priorities:

- *Information Sharing Environment (ISE).* As discussed above, the Board is specifically charged with responsibility for reviewing the terrorism information sharing practices of Executive Branch departments and agencies to determine adherence to guidelines designed to appropriately protect privacy and civil liberties. Accordingly, the Board was integrated into the process chaired by the Program Manager for the development and implementation of appropriate information sharing guidelines for Federal departments and agencies. The Board will work with the Program Manager to institutionalize its implementation oversight role.

- *Government surveillance operations.* The Board will continue to exercise its oversight role over terrorist surveillance.

- *Terrorist watch list issues.* The Board played a role in coordinating efforts among the various Federal departments and agencies to establish a unified, simplified redress procedure for individuals with adverse experiences during screening processes. The execution of an interagency memorandum of understanding on redress procedures is only a first step in establishing a simple, transparent process. The Board will continue its efforts to promote this process.

- *USA PATRIOT Act and National Security Letters (NSLs).* The 2006 reauthorization included over 30 new civil liberties protections. The Board will work with the Department of Justice to monitor implementation of these protections.

- *Federal data analysis and management issues.* Board Members intend to enhance significantly their understanding of issues associated with data mining activities, data sharing practices, and governmental use of commercial databases. This level of understanding will assist the Board in its review of many Federal anti-terrorism programs. Toward this end, the Board will follow up on recommendations of the March 2004 report of the Technology and Privacy Advisory Committee (TAPAC) to the Secretary of Defense, *Safeguarding Privacy in the Fight Against Terrorism.*

- *U.S. Persons Guidelines.* These guidelines limit the government's ability to collect, retain, and distribute intelligence information regarding U.S. Persons. These guidelines are applicable to agencies in the intelligence community pursuant to Executive Orders 12333 and 13284. As was noted in the 2005 report to the President on Weapons of Mass Destruction, these rules are complicated, subject to varying interpretations, and substantially different from one agency to another. The Attorney General and the Director of National Intelligence have established a staff level working group to review

these guidelines and propose appropriate reforms. The Board intends to participate in this process.

- *State and local fusion centers.* State and local law enforcement entities are establishing joint centers where they share information and data of value to their common missions. Federal agencies are developing partnerships with these centers. The Board will review these sharing practices to ensure that privacy rights and civil liberties concerns are taken into appropriate consideration.

- *National Implementation Plan (NIP).* The National Counterterrorism Center is presently conducting the first strategic review of the NIP. The Board is interested in the results of this review and actions taken as a result of its findings and recommendations. The Board will also continue to monitor those on-going NIP tasks and activities that might raise privacy or civil liberties concerns.

- *Department of Homeland Security Automated Targeting System (ATS).* ATS is a decision support tool used by Customs and Border Protection to assist in making a threshold assessment in advance of arrival into the U.S. based on information that DHS would otherwise collect at the point of entry. The Board intends to review this system.

- *Material Witness Statute.* As a result of concerns raised at its December 5, 2006 Georgetown University forum, the Board will investigate public expressions of concern over how this statute is being used in Federal anti-terrorism efforts.

18. Does the Board have a member with experience in immigration rights? If not, do you believe the Board would benefit if a member had specific immigration rights experience?

I do not believe that any current member of the Board has distinct immigration rights experience. This could be one of various different areas of experience that could be valuable to the Board.

19. Please provide your views of H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005" which was considered in the 109th Congress.

Neither I nor the Board has reviewed or opined on this legislation.

ANSWERS TO POST-HEARING QUESTIONS POSED BY THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRWOMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW TO THE HONORABLE HUGO TEUFEL III, ESQ., U.S. DEPARTMENT OF HOMELAND SECURITY

Question#:	1
Topic:	Privacy Act
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Your office acknowledges on page 24 of the April 2007 Government Accountability Office (GAO) Report on DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public, that "the biggest challenge it faces in ensuring DHS compliance with the Privacy Act" is updating legacy system-of-records notices.

What efforts has your office made in identifying, coordinating, and updating these notices?

When do you anticipate fully completing the process?

Answer: When the Department was created, the Privacy Office was faced with the unprecedented task of updating nearly 300 legacy systems of records, in addition to all our other statutory responsibilities. Given our significant workload, we were forced to prioritize our efforts. We focus on writing System of Record Notices (SORNs) for new systems first. Next we tackle those legacy SORNs whose systems are undergoing changes which necessitate a new SORN. Following these, we reissue legacy SORNs describing systems with a significant impact on personal privacy. Finally, we examine legacy SORNs describing routine systems with relatively little impact on personal privacy. These lower priority legacy SORNs often require little updating other than changing, for instance, "U.S. Customs Service" to "Customs and Border Protection" and "U.S. Department of Homeland Security."

While the review is underway, the privacy of US Citizens and Lawful Permanent Residents is protected, as the components continue to function under these legacy SORNs. Such use is permitted under section 1512 of the Homeland Security Act of 2002 – the Savings Provision – whereby the Department may rely on SORNs that were properly in place before the creation of the Department. *See* 6 U.S.C. § 552(d)

The Privacy Office recently added additional staff to work on this project full time. I plan to complete the review and reissuance of all legacy SORNs by January 2009.

Question#:	2
Topic:	annual report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Your office's most recent annual report issued in November 2006 covered activities from July 2004 to July 2006.

When can we expect your office's next report?

Answer: We are completing work on the annual report and it will be public soon.

Question#:	3
Topic:	OMB Circular A-130
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Office of Management Bureau (OMB) Circular A-130 directs federal agencies to review their notices biennially to ensure that they accurately describe all systems of records. Apparently DHS has not been in compliance.

Why?

How will your office ensure that DHS will be in compliance with OMB Circular A-130?

Answer: Given the vast number of systems of records inherited from legacy agencies which became DHS, we have had to prioritize our review of all our systems of records as described above. We recently expanded the compliance staff to facilitate this review and anticipate being in full compliance with this requirement once our initial survey of all legacy systems of records is complete in January 2009. DHS will provide an update within the FISMA and Privacy Reporting provided quarterly and at the end of each fiscal year.

Question#:	4
Topic:	GAO recommendation
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The GAO recommended in its April 2007 report that DHS designate full-time privacy officers in key departmental components to help speed the processing of privacy impact assessments. The GAO indicated that DHS took this recommendation "under advisement."

What is the current status of DHS's consideration of this GAO recommendation?

Answer: The Privacy Office recognizes a strong correlation between the designation of privacy officers at the component and program level, and the success of the Privacy Office's mission within those components and programs. Privacy officers at the Transportation Security Administration and the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program office, for instance, are an important factor ensuring privacy is operationalized. While GAO observed that the components with designated privacy officers have produced a majority of the PIAs issued to date, this is just one example of the important contribution these component privacy officers make in embedding privacy into departmental programs. These component privacy officers provide day-to-day privacy expertise within their components to programs at all stages of development, ensuring that privacy is considered from the design through the implementation phase of every program within their component.

This recommendation is consistent with DHS Privacy Act Compliance Management Directive (MD) No. 0470.2. Specifically, section V.B.1. of the MD directs Under Secretaries and all DHS Designated Officials to: "Appoint an individual with day-to-day responsibility for implementing the privacy provisions of the Privacy Act, and any other applicable statutory privacy requirement."

Since GAO made this recommendation, FEMA has designated a privacy officer, the Science and Technology (S&T) directorate has identified a full time privacy point of contact, and U.S. Citizenship and Immigration Services and Immigration and Customs Enforcement have posted vacancy announcements for privacy officers on usajobs.gov.

The Privacy Office will continue to press the importance of placing privacy officers within the components and work with the Department to develop position descriptions and provide necessary training to support this development. We are working with senior

Question#:	4
Topic:	GAO recommendation
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

leadership of the Department to designate component privacy officers in components that make significant use of PII.

Question#:	5
Topic:	timely reports
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: What specifically has DHS done to ensure timely production of reports so that the public does not perceive DHS as neglecting privacy concerns and can also obtain some value from timely reports?

Answer: The Privacy Office acknowledges the need for the timely issuance of its reports, including its annual report, and applies full effort to meet any report deadlines. The Privacy Office works with components and programs impacted by its reports to provide for both full collaboration and coordination within DHS and timely issuance of its reports. We are confident that our reports will be timelier in the future. Our next annual report will cover the period from July 2006 to July 2007, and will soon be completed and sent to Congress.

In its initial formative years, the Privacy Office focused on building the initial mechanism to operationalize privacy protection across the still-evolving Department. The Privacy Officer is further extending the reach of the Office and creating a stable, scalable model for federal government privacy protection – an important part of which is timely, reliable administration and reporting.

Question#:	6
Topic:	privacy concerns
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The Privacy Office sponsors programs for new employees as well as ongoing programs for current employees on privacy concerns.

What efforts has the Privacy Office made to determine whether these employee programs are effective and actually result in improved privacy protections?

Answer: The Privacy Office believes effective privacy training is critical to ensuring compliance with the Privacy Act and all other laws and procedures relating to privacy. The Privacy Office regularly seeks to improve training materials and to discover new needs for privacy training across the Department, particularly in new program areas. For example, in June 2007, the Chief Privacy Officer and the Undersecretary for Management issued a joint memorandum to all DHS components outlining requirements for protecting personnel-related data. The memorandum requires all DHS personnel handling personnel related data to be trained on privacy by the beginning of October 2007. Additionally, in response to OMB M-07-16, the Privacy Office in coordination with the Chief Human Capital Officer and the Office of the General Counsel, plan to roll out training on preventing and responding to data breaches including PII.

The Privacy Office has not yet undertaken a systematic review of the effectiveness of its training, as its training modules are still relatively new. As DHS compiles its overall personnel education program, and as the Privacy Office integrates its existing and developing privacy training into that departmental education enterprise, it will become easier for the Privacy Office to measure and track the effectiveness of the various training programs it provides.

Question#:	7
Topic:	personal information
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: In its April 2007 report, the GAO recommended that DHS develop policies concerning the department's use of personal information obtained from commercial data providers.

Has DHS drafted such a policy, and if not, why the delay?

Answer: The Privacy Office has incorporated a number of questions regarding commercial data providers and the use of commercial data into its latest Privacy Impact Assessment Official Guidance material. This follows upon the specific recommendation of the DHS Data Privacy and Integrity Advisory Committee December 6, 2006, report to the Secretary and Chief Privacy Officer advising that the Office revise the PIA template to include examination of agency use of commercial data.

Given the different uses of commercial data at DHS, the Privacy Office has determined it will not issue department-wide policy on the use of commercial data; rather, the office will provide narrowly tailored guidance through the PIA process. The PIA process is the best way to ensure that the Office is made aware of the uses of commercial data and that programs have considered the privacy impact of using such data in their programs. Programs are asked, for example, to describe why information from a commercial aggregator is being used; why such data is relevant and necessary to the program's purpose; whether the commercial aggregator of information is used to check data for accuracy and if so to describe this process and the levels of accuracy required by the contract; how the reliability of the commercial data is assessed; and how data accuracy and integrity are preserved.

The Privacy Office may issue more general guidance on commercial data in the future.

Question#:	8
Topic:	Privacy Act of 1974
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: How does the Privacy Office assure agency compliance with the Privacy Act of 1974?

What authority does the Privacy Office have to compel compliance with privacy requirements?

Should the Privacy Office be given subpoena power and broader power to initiate investigations?

Answer: Section 222 of the Homeland Security Act makes the Chief Privacy Officer responsible for "assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." The Privacy Act carries civil and criminal liability for non-compliance. All Privacy Act complaints received by the Privacy Office will be referred to the DHS Office of Inspector General (OIG) for their consideration and action. If investigations initiated by the Privacy Office uncover non-compliance with the Privacy Act, we will similarly refer the matter to the OIG.

The Privacy Officer already has broad authority to initiate investigations and reviews of privacy matters at the Department. The Implementing Recommendations of the 9/11 Commission Act of 2007, moreover, granted the Chief Privacy Officer with the power to issue subpoenas in some instances.

Question#:	9
Topic:	Data Privacy
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: What role do you envision for the Data Privacy and Integrity Advisory Committee in assisting you in carrying out your duties?

Have you sought advice from that Committee on specific issues? If so, please explain.

What steps, if any, have you taken to ensure that the Committee's recommendations – such as its recommendation regarding radio frequency identification technology (RFID) – are incorporated into departmental policy?

Answer: The purpose of the Data Privacy and Integrity Advisory Committee (DPIAC) is to provide the Secretary and Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, data integrity, and other privacy related issues.

In the past two years, the Committee has issued six reports with 36 recommendations to the Department, based on our specific requests:

1. Comments Regarding the Notice of Proposed Rulemaking for Implementation of the REAL ID Act
2. Use of Radio Frequency Identification (RFID) for Human Identity Verification
3. Use of Commercial Data Report
4. Framework for Privacy Analysis of Programs, Technologies, and Applications
5. Recommendations on the Secure Flight Program
6. Use of Commercial Data to Reduce False Positives in Screening Programs

Committees established under the Federal Advisory Committee Act (FACA) may only provide advice. Federal officials are ultimately responsible for determining whether or not to implement a given recommendation. In the Privacy Office, we are committed to ensuring the DPIAC's recommendations are given due consideration by Department officials. This is best achieved by involving program officials in the committee activities. For instance, Department officials regularly provide testimony at DPIAC's public meetings and answer the committee's questions. These officials are encouraged to attend panel testimony given by privacy community advocacy groups, to hear additional perspectives on their programs. Finally, reports and recommendations are shared with program officials for their consideration.

Question#:	9
Topic:	Data Privacy
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

DPIAC's guidance on RFID, for example, informs the Privacy Office's work on RFID-related projects across the Department. The Privacy Office works closely with the DHS Radio Frequency Identification Working Group (RFID WG) and those programs across the Department using RFID to both develop and integrate privacy protection guidance into the use of this technology.

Question#:	10
Topic:	privacy issues
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: What do you consider to be the most pressing privacy issues currently facing your office and how are you addressing these issues?

Answer: Among the most pressing privacy issues facing our Office is our ability to provide timely and meaningful guidance to the many programs seeking our assistance and to integrate that guidance into the actual development and operation of the many DHS programs that involve personally identifiable information and may raise privacy concerns. This is especially true of the numerous credentialing (e.g., REAL ID, WHTI, Enhanced Driver's License, E-Verify), screening (e.g., Secure Flight, ATS, TWIC, Trusted Traveler), and intelligence (e.g., NAO) programs, and complex technologies (e.g., Service Oriented Architecture and advanced analytics) within the Department. To address this pressing issue, the Privacy Office is adding staff. Moreover, we are improving our training material and efforts to operationalize privacy so component employees are better at spotting issues needing the Privacy Office's attention.

Question#:	11
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The 2007 Data Mining Report - DHS Privacy Office Response to House Report 109-699 (July 6, 2007) (2007 Data Mining Report) notes that a variety of definitions of data mining exist, including those used by the Government Accountability Office, Congressional Research Service, and the DHS Inspector General, in addition to the definition established by Congress in legislation requiring House Report 109-699 (House Report). While the Data Mining Report details the various differences in definitions, it makes no conclusions about what a useful definition of data mining should be.

Based on the experience of the Privacy Office in reviewing DHS programs, what definition of data mining would be most useful in identifying departmental programs that could pose privacy questions?

Please provide a rationale for your definition.

Answer: The Privacy Office's 2007 Data Mining Report utilized a definition of data mining provided by Congress. Under this definition, "data mining" is:

> *"[A] query or search or other analysis of 1 or more electronic databases, whereas –*
> *(A) at least 1 of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement;*[13]
> *(B) a department or agency of the Federal Government or a non-Federal entity acting on behalf of the Federal Government is conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity; and*
> *(C) the search does not use a specific individual's personal identifiers to acquire information concerning that individual."*

Question#:	11
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

This definition satisfactorily captures the meaning of data mining as we understand it. More importantly, the Privacy Office has a working understanding of the definition and how it relates to DHS programs, having used it in the 2007 report.

We note that Congress has provided a new definition of data mining in the 9/11 Commission Act. The Privacy Office has not had time to fully analyze the impact of this new definition on our working understanding of DHS data mining activities.

Question#:	12
Topic:	ADVISE Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The ADVISE Report - DHS Privacy Office Review of the Analysis, Dissemination, Visualization, Insight and Semantic Enhancement Program (July 11, 2007) (ADVISE Report) notes that several applications have been developed or tested. One in particular, the Threat Vulnerability Integration System (TVIS) would appear to be a candidate for inclusion in the 2007 Data Mining Report based on the description provided in the ADVISE Report. Further, the ADVISE Report notes that TVIS had not complied with the requirement to conduct a Privacy Impact Assessment (PIA) prior to using personally identifiable information (PII), thus potentially raising privacy concerns. While the 2007 Data Mining Report includes a brief description of ADVISE, it makes no reference to any specific applications of the ADVISE tool.

Why does the description of the ADVISE Program in the 2007 Data Mining Report not include any references to specific applications?

In particular, why is TVIS not included, either as part of the Data Mining Report's discussion of ADVISE or as a separate system?

Answer: The Privacy Office's 2007 Data Mining report relies upon the definition of data mining provided in House Report No. 109-699. This definition includes specific reference to "*conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity.*" None of ADVISE's specific applications, including TVIS, searched for predictive patterns. These early efforts were limited to establishing whether the ADVISE architecture was even feasible. They focused on loading data into the system only, and did use of the data to make any predictions of criminal or terrorist activity. Accordingly, TVIS and other specific applications of ADVISE, were not included in the report.

Question#:	13
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Page 9 of the 2007 Data Mining Report states, "The Privacy Office remains committed to urging the adoption of these recommendations within DHS; however, additional time will be needed in order to inform programs fully and develop appropriate implementations for the recommendations."

Please explain how much time you estimate will be necessary to inform programs fully and to develop appropriate implementations for such recommendations.

Is your estimate affected by your staffing resources or amount of appropriations?

Answer: The Privacy Office's resources are fully engaged with its ongoing responsibilities. The new investigation, training, and reporting responsibilities within the 9/11 Commission Act will place additional burdens on the office.

The Privacy Office began implementation of the Data Mining Report recommendations by identifying a group of Component representatives from across the Department who will work together to address the concerns expressed in the report. Many of the recommendations will require new research and departmental policies and procedures (e.g., data quality standards, data mining models, anonymization techniques) that will necessarily take time to develop and implement properly. We anticipate measurable progress over the course of this year, reportable in the next annual Data Mining report. In order for the Privacy Office and the Components to focus on implementation, it is vital that additional reporting requirements be coordinated for a true annual time frame.

Question#:	14
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Page 16 of the Data Mining Report notes that the Privacy Office is "currently conducting a review of the ADVISE Technology Framework and any associated pilots to ensure the completion of all appropriate privacy-related documentation."

Will this review include the preparation of a Privacy Impact Assessment (PIA)?

When will this review be completed?

Answer: DHS recently announced that it will no longer utilize ADVISE, therefore the Privacy Office has suspended work on a PIA.

Before this announcement, however, the Privacy Office completed its review of ADVISE and issued a report dated July 11, 2007. The report states that a PIA, as defined by the E-Government Act of 2002, is not the best mechanism to use in assessing the impact of a toolset like ADVISE, because these traditional PIAs focus on the particular use of PII in a specific context, and a toolset may be used for different purposes by different programs.

The Privacy Office has since created two new mechanisms to guide the articulation of privacy protections for DHS use of technology and DHS programs that do not fit within the limited scope of a traditional PIA. The first is the DHS Privacy Office Privacy Technology Implementation Guide (PTIG). The PTIG is a step-by-step guide IT managers and developers can use to address privacy compliance requirements throughout the development and operating life cycle of IT systems.

The second is a new PIA template based on the Fair Information Practice Principles. This FIPPs PIA template addresses the fundamental privacy concerns that underlie all privacy analysis: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Security, Data Quality and Integrity, and Accountability and Audit. A follow-up, traditional PIA would be required for each particular deployment of the program based on the toolset where PII is used.

The Privacy Office created these tools for those programs which do not meet the specific thresholds of the Section 222 of E-Government Act of 2002 but, according to the requirements of Section 208 of the Homeland Security Act of 2002, should still be

Question#:	14
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

reviewed for compliance with privacy protection requirements – such as the ADVISE technology framework.

Question#:	15
Topic:	DARTTS
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Though Data Analysis and Research for Trade Transparency System (DARTTS) is one of only six data mining systems determined by DHS to be reportable under Congressional criteria, DHS notes that neither a PIA nor a system-of-records notice (SORN) has been completed for this system, which is a legacy system brought to DHS from the Department of the Treasury. Given the prominence of privacy issues associated with data mining programs, complete privacy documentation for such a program is critical.

Why has the department not completed the required privacy documentation for the DARTTS data mining program? When will this documentation be completed?

Answer: As mentioned on page 22 of the Privacy Office's 2007 Data Mining Report, ICE is currently working on the privacy compliance documentation for the DARTTS program. Once ICE completes the first draft of the documentation, the Privacy Office will work closely with the DARTTS program office to finalize and publish both the PIA and the SORN.

Question#:	16
Topic:	DARTTS
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The discussion of data security for DARTTS makes much of the fact that the system has no Internet connectivity and can only be accessed through specially designed clients. Yet the section on goals and plans for the program notes that an effort is underway to migrate DARTTS to a web-based interface. Please discuss how security is to be maintained when the system is made available through a web interface.

Answer: At present, Data Analysis and Research for Trade Transparency System (DARTTS) is a stand-alone system hosted at the Chester Arthur Building (CAB) in Washington, DC. DARTTS is operating with a complete certification and accreditation (C&A) package as required by the Federal Information Security Management Act and has full Authority to Operate (ATO) valid until September 28, 2009. This means that appropriate security controls are in place given the nature of the information on the system. Recently, the plan to make DARTTS an enterprise-wide system was discussed and funding has been approved for FY08 initiation. This new "web-based" DARTTS will conform to the DHS Systems Development Lifecycle (SDLC) and ICE Systems Lifecycle Methodology (SLM), including a complete re-certification and accreditation to ensure the proper management, operational and technical safeguards are in place to secure the upgraded system. In accordance with DHS Sensitive Systems Policy and Handbook 4300A, Information Technology Security Program, DARTTS will obtain a new Authority to Operate (ATO) as an enterprise-wide system at an acceptable level of risk to ICE and DHS. Approved privacy documentation would also be required prior to the ATO being issued.

Question#:	17
Topic:	Data Mining Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Based on the information provided in the report, very little progress appears to have been made in implementing the recommendations of the 2006 DHS Data Mining report. It appears that in two cases (centralized oversight of DHS data mining and anonymization), the Privacy Office in the 2007 Data Mining Report adopts a weaker position than recommended the previous year.

Why has DHS been so slow to take action on the Privacy Office's recommendations regarding data mining?

Does the Department support the Privacy Office's recommendations?

If not, why not?

Answer: The Department supports the Privacy Office's recommendations. This past year, implementing those recommendations has been particularly difficult and, as mentioned in earlier responses to the above questions, the Privacy Office must evaluate and prioritize the multitude of different high priority projects and issues.

The Privacy Office works closely with the Components to ensure programs comply with privacy protection requirements. New recommendations, particularly recommendations that trigger full departmental coordination and new scientific research are important, but must be implemented once higher priority tasks are completed.

This year, the Privacy Office started working immediately upon release of its Data mining report and will be organizing the first Departmental data mining working group in the next couple of months. The Privacy Office has also started working with S&T to define the kind of research required to identify, develop and implement anonymization technologies across the Department.

Question#:	18
Topic:	policy formulation
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Several of the recommendations relate to policy formulation, yet the 2007 Data Mining Report suggests that new policies to address the recommendations have not yet been drafted.

Why has the Privacy Office not yet drafted policies regarding automated decision making and individual review and redress?

When will such policies be in place?

Answer: As explained in the answer to question 17, the Privacy Office must triage and prioritize new obligations. The Privacy Office plans to work on new data mining policies and guidance during the year between this last annual data mining report and the next. It is important to note the new Data Mining report identified in the recent 9/11 Commission Act identifies an accelerated reporting period and provides another definition of "data mining." In order to meet the short publishing deadline of this new report, the Secretary, in conjunction with the Privacy Office, will again have to triage its obligations and focus on statutory requirements over implementing recommendations.

Question#:	19
Topic:	recommendations
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Several of the recommendations relate to development of standards, yet the 2007 Data Mining Report is not clear about whether any work has been done on these standards to date.

When will standards for data quality and validation of models or rules derived from data mining be developed?

What is the Privacy Office doing to ensure that standards are drafted as quickly as possible and become part of departmental policy as soon as they are available?

Answer: The Privacy Office is working closely with S&T to identify criteria for new standards for data mining programs in the Department. As mentioned in the answers to questions 17 and 18, above, the Privacy Office made the difficult choice to respond to reporting mandates with deadlines over the type of large-scale new recommendations identified in its previous report.

The Privacy Office retains its belief in the importance of technical and policy standards for complex technologies like data mining and has initiated discussion with both S&T and OCIO regarding how best to proceed in the long term effort to define, develop, and deploy new standards for data mining technology.

Question#:	20
Topic:	departmental policy
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Does the Privacy Office intend to draft a departmental policy regarding strong audit capabilities for data mining programs?

When will this policy be in place?

Answer: The Privacy Office intends to coordinate with the CISO to define "audit" in a way that is meaningful to IT developers, Information Security professionals, as well as privacy compliance and policy practitioners. The Privacy Office will coordinate the development of this unified definition and then extend the collaboration to develop and deploy a privacy-supportive system audit process that aligns with the Privacy Office's intended privacy audit program which the Privacy Office is only now able to begin conceptualizing given limited resources and competing priorities.

Question#:	21
Topic:	data mining projects
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The original recommendation suggested that data mining projects should be reviewed in advance by a separate organization within DHS, such as the DHS Data Integrity Board. Not only has this not been adopted, the Privacy Office now recommends only that a "coordinating group" of data mining programs be established to harmonize policies and practices.

Why does the Privacy Office no longer believe that some form of oversight of data mining programs is necessary?

How can the Privacy Office's current proposal—to establishing a coordinating group among data mining programs—provide a means for determining whether such programs have the proper authority to operate?

Answer: The Privacy Office believes that a strong cross-Component coordinating group is the most effective mechanism to assure collaboration and cooperation on the complex issue of data mining technology and programs.

The DHS Data Integrity Board is a statutorily mandated board (5 U.S.C. § 552a(u) narrowly focused on data matching agreements and thus is not the appropriate body to address the nature and use of data mining technology across the Department.

DHS currently has similar coordinating groups for other technologies such as biometrics, RFID, and Geospatial technologies. There is a robust precedent for technology coordinating groups across the Department. The Privacy Office will play the leading role in bringing together S&T to research data mining technology, OCIO to deploy, and the Operational Components to use and report on the effectiveness and compliance of data mining over this next year. Of course, the Privacy Office has oversight authority, generally, and with respect to data mining at the Department.

Question#:	22
Topic:	Privacy Office
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The original recommendation was that data mining projects should give explicit consideration to using anonymized data and document this consideration in their PIAs. The Data Mining Report, however, discusses anonymization as a research topic and states that the Privacy Office will use the results of its research to determine how best to integrate anonymization within DHS systems.

Why is the Privacy Office no longer calling on data mining programs to give explicit consideration to incorporating anonymization?

Please provide specific reasons why the Privacy Office has changed its position and discuss why those reasons did not apply when the 2006 Data Mining Report was issued.

Answer: Since the 2006 recommendations, the Privacy Office identified several unresolved issues related to the techniques and effectiveness of different anonymization techniques. The Privacy Office recently began discussion with S&T concerning research on approaches to anonymization including how best to anonymize so data is still usable in operational settings, and how to implement anonymizing practices uniformly throughout the Department.

The Privacy Office continues to address the issue of anonymization with any program offices of data mining systems and will coordinate deployment of the final DHS anonymization policy and procedures as soon as they are finalized.

Question#:	23
Topic:	GAO
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: In February 2007, the Government Accountability Office (GAO) issued a report on the DHS's development of an analytical tool known as Analysis Dissemination, Visualization, and Semantic Enhancement (ADVISE).[1] In its report, GAO found that DHS had not yet assessed privacy risks associated with use of the ADVISE tool, such as the potential for erroneous associations of individuals with crime or terrorism, the misidentification of individuals with similar names, and the use of data that were collected for other purposes. Accordingly GAO recommended that DHS immediately conduct a PIA of the ADVISE tool to identify potential risks and implement controls to mitigate those risks. The ADVISE Report notes that "some deployments of ADVISE used personally identifiable information without first conducting a privacy impact assessment as required."

> Why does the ADVISE Report not address the larger risks to privacy of the ADVISE tool itself that the GAO identified in its report?
>
> What is the status of the Privacy Technology Implementation Guide (PTIG) referenced in the ADVISE Report as part of the long term solution?
>
> Will the PTIG include the Privacy Office's recommendations regarding data mining, as stated in the 2006 Data Mining Report? If not, why not?

Answer: The Privacy Office's ADVISE report targeted that area of the issue that had not been covered by other reports on ADVISE: Whether there were specific violations of privacy protection requirements. At the time the Privacy Office's ADVISE was drafted, the plan was to issue specific privacy guidance for using the ADVISE tool. In working through that separate drafting process, the Privacy Office decided that it would be more effective to start with overall guidance for technology projects and issued the PTIG. The next step would have been to use the overall guidance as a foundation for ADVISE-specific privacy technology guidance. The Privacy Office also planned to use the newly developed FIPPs PIA Template to address the overall privacy concerns related to the ADVISE technology framework.

---

[1] **U.S. Government Accountability Office, *Data Mining: Early Attention to a Key DHS Program Could Reduce Risks*, GAO-07-293, (Washington: DC, February 28, 2007).**

Question#:	23
Topic:	GAO
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Since the publication of Privacy Office's ADVISE report, the Department announced it will no longer utilize ADVISE.

The Privacy Office released the PTIG on August 16, 2007. It is posted on the Privacy Office's public facing website: www.dhs.gov/privacy.

Question#:	24
Topic:	ADVISE Report
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The ADVISE Report describes the PTIG as "recommendations for incorporating privacy protections into the early stages of project development."

Will DHS data mining programs, including ADVISE, be required to address these recommendations?

For example, if the PTIG identifies a privacy risk related to ADVISE, will the Science and Technology Directorate (S&T) be required to implement mitigating controls?

Answer: As currently written, the PTIG is a general guide that articulates a combination of recommendations and requirements. All existing privacy compliance requirements are already managed through the Privacy Office's privacy compliance process and the combination of the CISO's security requirements and OGC's legal requirements.

The Privacy Office will use the recommendations in the PTIG to extend the existing privacy compliance review and documentation process; thus through the existing PTA, PIA, and SORN process, the Privacy Office will review the identified privacy protection risks relevant to a particular program and document how the program office has mitigated those risks. Since the PTIG drew from the considerations articulated in the various Privacy Office privacy compliance documents and policies, if a program office were to follow all of the recommendations in the PTIG, it would be easily able to demonstrate that it considered privacy protection at the front end of system design and development and could thoroughly articulate the privacy risk and mitigations that deployed along with the system itself.

Question#:	25
Topic:	ADVISE
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: The ADVISE tool has been under development by S&T since 2003 when the Privacy Office was established.

Why were the issues and recommendations identified in the ADVISE Report not identified earlier on?

Was this a case of a communication breakdown or a DHS component not following the advice of the Privacy Office?

What steps is the Privacy Office taking to avoid this situation in the future?

Answer: Both the Privacy Office and S&T started as new organizations when the Department was first created and over the three years since then there has been a great deal of fast-paced growth, reorganization and organizational integration. ADVISE as a technology framework, and as a set of deployments, existed as a DHS program and also as an outsourced effort led by outside organizations and individuals who are no longer associated with the effort or the various organizations. The ADVISE technology framework itself is complex, overshadowed only by the technical challenges it was designed to overcome.

Notwithstanding the cancellation of the ADVISE program, the recommendations in the Privacy Office's ADVISE report identified a series of long term responsive actions that the Privacy Office and S&T can implement to better coordinate and integrate privacy compliance into the S&T's overall research practices.

In addition, S&T has recently dedicated a full-time position as a privacy point of contact for the component. With this person in place, S&T is conducting a full inventory of all its uses of PII. This inventory, partnered with a review of S&T's strategic plan should thoroughly vet S&T for current and anticipated uses of PII so that privacy compliance processes can be implemented earlier, consistently, and comprehensively.

Question#:	26
Topic:	H.R. 2840
Hearing:	Privacy in the Hands of Government: The Privacy and Civil Liberties Oversight Board and the Privacy Officer for the U.S. Department of Homeland Security
Primary:	The Honorable Linda T. Sanchez
Committee:	JUDICIARY (HOUSE)

Question: Please provide your views of H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005," which was considered in the 109th Congress.

Answer: Under the authority of Section 222 of the Homeland Security Act of 2002, the Privacy Office already conducts PIAs for proposed rules of the Department and updates them upon issuance of the final rule.

ANSWERS TO POST-HEARING QUESTIONS POSED BY THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRWOMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW TO MS. LINDA KOONTZ, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

United States Government Accountability Office
Washington, DC 20548

September 7, 2007

The Honorable Linda Sánchez
Chair, Subcommittee on Commercial and Administrative Law
Committee on the Judiciary
House of Representatives

Subject: *Privacy: Subcommittee Questions Concerning the Department of Homeland Security's Privacy Office*

Dear Madam Chair:

This letter responds to your August 14, 2007 request that we provide answers to questions relating to your July 24, 2007 hearing. At that hearing, we testified on progress made and challenges faced by the Department of Homeland Security's (DHS) Privacy Office.[1] Your questions, along with our responses, follow.

1. What do you consider to be the major accomplishments of the DHS Privacy Office?

The DHS Privacy Office has been effective at establishing a process for ensuring departmental compliance with the E-Gov Act's requirement that privacy impact assessments (PIA) be conducted whenever the department develops or procures information technology that collects, maintains, or disseminates information in an identifiable form. Instituting this process has led to increased attention to privacy requirements on the part of departmental components, contributing to an increase in the quality and number of PIAs issued. The Privacy Office has also taken actions to integrate privacy considerations into the DHS decision-making process, through such steps as establishing a federal advisory committee, conducting public workshops on key issues, and participating in policy development for several departmental initiatives.

2. What do you consider to be the major challenges that the DHS Privacy Office currently faces?

[1] Government Accountability Office, *Homeland Security: DHS Privacy Office has Made Progress but Faces Continuing Challenges*, GAO-07-1024T, (Washington, D.C.: July 24, 2007).

A major challenge that the privacy office faces is in keeping public notices required by the Privacy Act up to date. Little progress has been made in updating notices for "legacy" systems of records—older systems of records that were originally developed by other agencies prior to the creation of DHS. Because many of these notices are not up-to-date, the department cannot be assured that the privacy implications of its many systems that process and maintain personal information have been fully and accurately disclosed to the public.

Another challenge is issuing public reports in a timely manner. The Privacy Office has generally not been timely in issuing public reports, potentially limiting their value and impact. For example, the office issued only two annual reports in the three-year period beginning in April 2003, when it was established. Further, a report on the Multi-state Anti-Terrorism Information Exchange program—a pilot project for law enforcement sharing of public records data—was not issued until long after the program had been terminated. Such late issuance can limit the reports' value and erode the credibility of the office.

We have made recommendations to DHS to address these challenges, and DHS has reported that it is taking steps to implement them.

3. The GAO report notes on page 21 that DHS does not have policies in place concerning its uses of personal information obtained from commercial data providers.

This observation from our April 2007 report[2] is now out-of-date. The department's policy on the use of commercial data was established in the most recent version of its privacy impact assessment guidance, dated May 2007. Specifically, the PIA guidance incorporates new material concerning use of commercial or publicly available data. According to DHS Privacy Office officials, whom we met with following the July 24, 2007 hearing, once the Privacy Office identifies a program's use of commercial data through the PIA process, they will work with the program to ensure that commercial data is used properly, appropriate controls are in place, and that privacy notices reflect its use. Accordingly, we believe that DHS has addressed the recommendation we had previously made concerning use of commercial data.[3]

Are there other agencies that have policies in place? If yes, what agencies?

Our review of federal agency use of personal information from information resellers involved four agencies, Social Security Administration, Department of Justice, Department of State, and Department of Homeland Security. In that report, we made recommendations to all four agencies that they develop policies concerning the use of commercial data. To date, only DHS has established such policies. We will continue to monitor actions by the other three agencies.

---

[2] GAO, *DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public*, GAO-07-522 (Washington, D.C.; April 27, 2007).
[3] GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: April 4, 2006).

Could these agencies serve as a role model for DHS and other agencies in developing and implementing policies concerning personal information obtained from commercial data providers?

As previously noted, thus far only DHS has established a policy, through its PIA guidance, on the use of commercial data. Other agencies, including the Social Security Administration, Department of State, and Department of Justice, could take a similar approach or could establish policies on commercial data independent of their PIA guidance.

4. How can we guarantee DHS Privacy Office participation in the formulation of decisions about major DHS programs will be fully addressed?

The Privacy Office's participation in policy decisions helps to ensure that privacy concerns are explicitly raised during development of programs. The Privacy Office has been involved in a number of key programs with privacy concerns, including negotiations with the European Union regarding airline passenger information, the development of a special border crossing identification card for the Western Hemisphere Travel Initiative, and the development of implementing regulations for the REAL ID Act of 2005.[4]

Although the extent to which programs address privacy concerns may depend on factors outside of the Privacy Office's control—such as competing departmental priorities—the Privacy Office has nevertheless been effective in participating in the DHS decision making process and in using the PIA process to enhance consideration of privacy issues. Although no guarantees can be made, further assurance that Privacy Office concerns are fully addressed by major DHS programs could be achieved by enhancements to coordination between the Privacy Office and DHS components. This could improve attention to privacy concerns early in the design and development of DHS programs. Our recommendation that DHS appoint component level privacy officers could enhance such coordination.

5. Based on your analysis of the DHS Privacy Office, what recommendations do you have regarding how to provide the most effective format to protect civil liberties and privacy of personal information?

There is no consensus on the most effective format for privacy protection. The DHS Privacy Office has demonstrated that it can be effective in developing policies and procedures to implement privacy protections as an integral part of the department. Its position allows Privacy Office officials to serve as internal advisors to DHS components that may lack privacy expertise. The PIA process developed by the DHS Privacy Office is an example of an effective way to ensure programs are aware of requirements, have guidance to comply with them, and have expert support in preparing such assessments. The Privacy Office's effectiveness could be further enhanced by implementing our recommendation to appoint component level privacy officers in key DHS components who could also assist in ensuring that privacy concerns are addressed and could coordinate with the departmental office.

---

[4] Division B, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13 (May 11, 2005).

Are sui generis *privacy offices a more effective protector of these rights than an all encompassing privacy office, such as one similar to the ideals of the Privacy and Civil Liberties Oversight Board?*

Both *sui generis*[5] privacy offices and all encompassing privacy offices have roles to play in ensuring protection of privacy rights. *Sui generis* privacy offices—such as the Privacy Office at DHS—can serve as a mechanism for actively promoting attention to privacy concerns throughout the department. As an internal consultant and advisor, a Privacy Office official can assist programs in ensuring that privacy protections are built in from the early stages of development and re-assessed upon significant changes. While the DHS Privacy Office also has certain oversight responsibilities, its primary focus is on promoting a privacy-protective culture at DHS. Privacy officials across government often have concerns about adopting a stronger role as independent investigators of privacy complaints, a role often seen as more akin to that of an inspector general. Regarding DHS specifically, the recently-enacted Implementing Recommendations of the 9/11 Commission Act of 2007[6] requires the Privacy Officer to refer all complaints of privacy violations to the DHS Inspector General for potential further investigation, thus establishing a mechanism for oversight and enforcement through coordination of the two parties.

An all encompassing Privacy and Civil Liberties Board, if given the authority and resources, would be in a position to provide consistent guidance and direction to federal agencies on protecting privacy and civil liberties and conduct independent oversight across the federal government. Although the Office of Management and Budget is tasked with oversight of the implementation of the Privacy Act and E-Government Acts, we have previously reported shortcomings in OMB oversight of the Privacy Act. For example, OMB has not substantially updated its Privacy Act guidance since its issuance in 1975.

6. What do you consider to be the principal reasons for the various delays associated with the DHS Privacy Office's reports?

According to Privacy Office officials, there are a number of factors contributing to the delayed release of its reports, including time required to consult with affected DHS components as well as the departmental clearance process, which includes the Policy Office, the Office of General Counsel, and the Office of the Secretary. After that, drafts must be sent to OMB for further review. In addition, the Privacy Office did not establish schedules for completing these reports that took into account the time needed for coordination with components or departmental and OMB review.

How could this problem be addressed?

---

[5] The word *sui generis* means "of its own kind," or "unique." Accordingly, a *sui generis* Privacy Office is one that is built to address a specific agency, while an all encompassing Privacy Office refers to one that would address governmentwide privacy concerns.

[6] Section 802(c)(2), Implementing Recommendations of the 9/11 Commission Act of 2007, (Pub. L. 110-53).

We have recommended that a schedule for the timely issuance of Privacy Office reports be established that considers all aspects of report development, including departmental clearance. We believe such a schedule would be helpful in planning for reports to be released on a timely basis. It is important to note, however, that the Privacy Office cannot control the amount of time that other DHS components or external parties may take to review report drafts or the types of comments they may offer. It will be crucial that executive leadership within the department ensure that privacy office draft reports are reviewed expeditiously at all levels of the department.

It should also be noted that the recently-enacted Implementing Recommendations of the 9/11 Commission Act of 2007 requires the DHS Privacy Officer to report directly to Congress without prior comment or amendment by the DHS secretary or OMB.[7]

7. What is your view regarding the value of positioning the Chief Privacy Officer within DHS?

As currently positioned within the DHS organizational structure, the Chief Privacy Officer (CPO) has the ability to serve as a consultant on privacy issues to other departmental entities that may not have adequate expertise on privacy issues. For example, the CPO can work on an ongoing, day-to-day basis to advise and assist DHS program officials as they develop important privacy documentation, including privacy impact assessments () and system-of-records notices. Enhancing the value of these privacy documents from with the department is of substantial value in achieving the overall goal of protecting privacy. Further, a departmental CPO may have the opportunity to participate in departmental policy-making that could have privacy implications, such as decisions about how to conduct airline passenger screening or how to implement the REAL ID Act.

What is your view of positioning this office outside of DHS?

An independent CPO would have certain advantages, especially with regard to investigations, but would lack the advantages of the current *sui generis* CPO. An independent CPO would be in a better position to prepare and issue reports on its activities and findings without extensive departmental coordination. While an independent CPO could serve a greater role in providing public commentary on the privacy implications of DHS programs, it would have less direct influence on departmental decisions made about those programs. Finally, the activities of an independent CPO would presumably not be affected by changes in departmental leadership.

In preparing this correspondence, we relied on previously issued GAO products and interviews with DHS Privacy Office officials. Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-6240, or John de Ferrari, Assistant Director, at (202) 512-6335. We can also be reached by e-mail at koontzl@gao.gov and deferrarij@gao.gov, respectively.

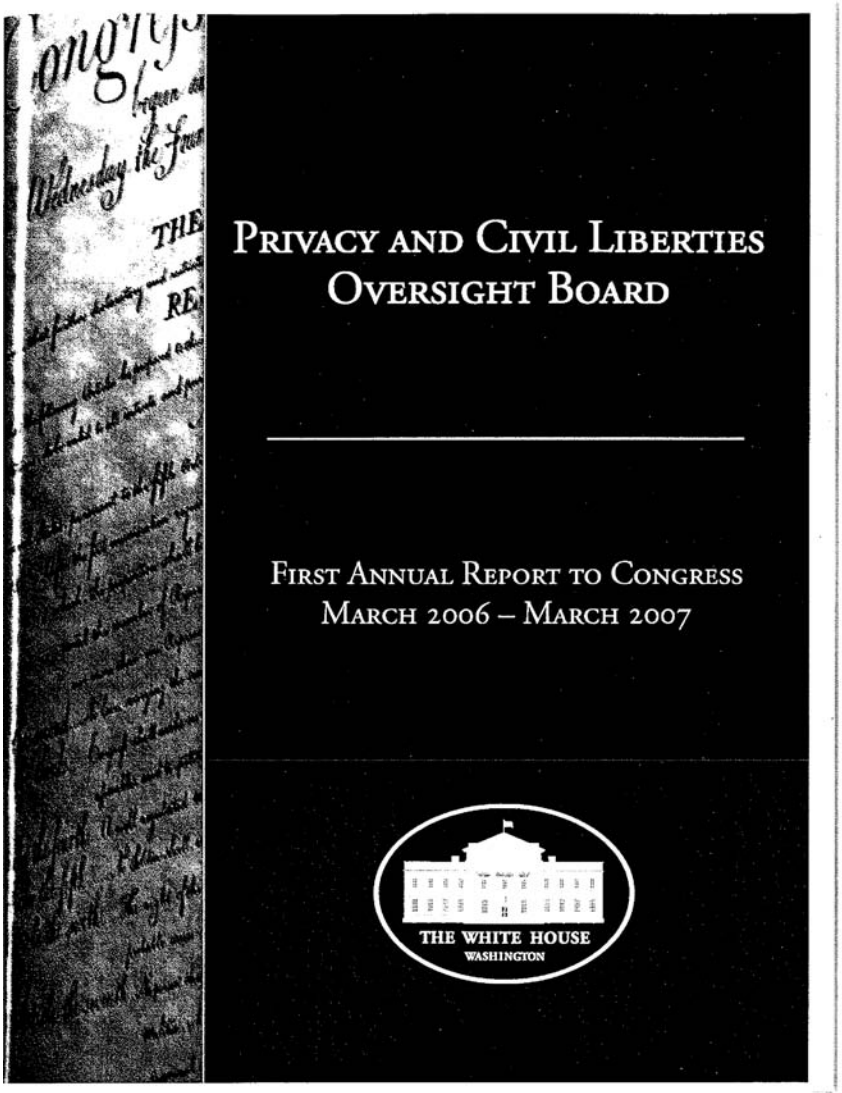
[7] Section 802(e), Implementing Recommendations of the 9/11 Commission Act of 2007, (Pub. L. 110-53).

Sincerely Yours,

Linda D. Koontz

Linda D. Koontz
Director, Information Management Issues

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 2007 REPORT TO CONGRESS, SUBMITTED BY THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRWOMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW



THE WHITE HOUSE

WASHINGTON

PRIVACY AND
CIVIL LIBERTIES
OVERSIGHT BOARD

April 20, 2007

Dear Mr. President and Madam Speaker:

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which created the Privacy and Civil Liberties Oversight Board (Board), requires the Board to report annually to Congress on its major activities during the preceding year. (P.L. 108-458, §1061(c)(4)). We are pleased to submit to Congress this first annual report of the Board's activities from its organizational meeting on March 14, 2006 through March 1, 2007. This report contains no classified information. Electronic copies of this report are available on the Board's webpage at www.privacyboard.gov.

IRTPA requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism." In carrying out this mandate, the Board has two primary tasks. *First*, it must "*advise* the President and the head of any department or agency of the executive branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation" of "laws, regulations, and executive branch policies related to efforts to protect the Nation from terrorism." *Second*, it must exercise *oversight* by "continually review[ing] regulations, executive branch policies, and procedures . . . and other actions by the executive branch related to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected." The statute specifically requires the Board to advise and oversee the creation and implementation of the Information Sharing Environment.

Unlike other boards and commissions charged with addressing an issue, making recommendations, issuing a report and then disbanding, this Board embodies a permanent commitment to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations and executive branch policies related to

efforts to protect the Nation against terrorism." The President has repeatedly stated that as the Federal government works to prevent terror against this Nation, its citizens and interests, it must do so in compliance with the Constitution and laws of the United States, and consistent with the values we share as Americans. The Board's statutory mandate and fundamental purpose is to further those objectives.

Since its creation in March 2006, the Board has focused on three areas in order to fulfill its statutory mandate. These areas have helped the Board establish its viability, subject matter expertise, and credibility within the government and with the public.

- ***Organization, Administration and Process***. The Board established the means and infrastructure necessary to support it in accomplishing its statutory mission. Toward that end, it has hired a professional staff; reached agreement with the Director of National Intelligence on the scope and logistics of detailing additional staff from within the intelligence community; acquired the necessary security clearances; built out appropriate office space with secured facilities for classified information; and developed a web site for communication with the public. Because it operates within the White House Office, the Board receives additional administrative support from White House staff. The Board adopted an annual agenda, a communications plan, an issue analysis methodology, and a reporting template. The Board has met as a group 23 times in the past twelve months.

- ***Education and Outreach.*** The Board has engaged policy officials and experts within the Executive Branch, Congress, the public, and private, non-profit, and academic institutions. It has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism by meeting with senior officials, examining their missions and legal authorities, learning of their specific programs, and reviewing their operational methodologies and privacy and civil liberties training, reporting, and auditing programs. For example, the Board has met personally, among others, the Attorney General, the Secretary of the Department of Homeland Security, Treasury Under Secretary for Terrorism and Financial Intelligence, the Director of National Intelligence, the Directors of the National Security Agency and the National Counterterrorism Center, the Information Sharing Environment Program Manager, and the President's senior staff. Among other non-governmental experts and advocacy groups, it has met with representatives from the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Markle Foundation, and the American Conservative Union. It also held its first public forum at Georgetown University on December 5, 2006.

As a part of this education and outreach effort, the Board has devoted particular effort to working with the new and growing presence of homeland security professionals within the Executive Branch specifically dedicated to consideration of privacy and civil liberties. The Board considers one of its fundamental responsibilities fostering a sense of community among, and helping empower, these new professional privacy and civil liberties officers, as well as attorneys, inspectors general, and other relevant agency program policy officials. The Board intends to provide the necessary support at the appropriate level so that all are better able to fulfill their own responsibilities.

- ***Issue Prioritization.*** Organizational and educational activities have occupied most of the Board's attention since its creation. Within the last few months, however, the Board has begun to engage in a substantive review of existing anti-terrorism programs and policies. For example, the Board has started to evaluate National Security Agency surveillance programs, the Treasury Department's Terrorist Finance Tracking Program, the Department of Defense's Counterintelligence Field Activities, the State Department's e-Passport initiative, and the National Counterterrorism Center's National Implementation Plan. It has helped coordinate the drafting of a Memorandum of Understanding to standardize and improve procedures for obtaining redress of watch list grievances. The Board has also been integrated into the drafting and implementation of the Information Sharing Environment guidelines.

In the year ahead, the Board will continue to fulfill its statutory responsibilities. In allocating its time and resources, the Board has determined that it will concentrate on those issues having the greatest potential impact on the largest number of U.S. persons.

Finally, since the drafting of the Board's Report, which it agreed would cover its work prior to March 1, the Attorney General notified the Board that the Inspector General of the Department of Justice (IG) would shortly issue his report concerning the FBI's use of National Security Letters (NSLs). The Attorney General and White House Counsel asked the Board to commence a substantive review of and invited recommendations concerning the matters raised in the IG's report.

The IG identified serious problems in the FBI's use of NSLs. The Board believes that such problems cannot be tolerated and must not be repeated. The Board is very concerned that effective means of oversight for the FBI's use of NSLs – commensurate with the expanded investigative powers authorized under the USA PATRIOT Act – were not, as found by the IG, in place. The Board was particularly troubled by the IG's finding that the FBI used so-called "exigent letters" without invoking proper statutory standards or following applicable procedures.

The Board has met with and questioned the FBI's Director and General Counsel and officials from the Department of Justice's National Security Division and Chief Privacy and Civil Liberties Office. In addition, the IG provided the Board with a thorough briefing. The Board has also solicited the views of and met with a number of representatives of the privacy and civil liberties community.

When it completes its assessment, the Board will provide the Attorney General and FBI Director with its views and recommendations for rectifying what all agree is an unacceptable situation. Based on the Board's inquiries to date, it is apparent that there must be greater accountability, oversight, and internal controls, as well as more effective guidance and training on this issue throughout the FBI. The Board will continue to monitor this issue and focus on the FBI's development of new guidance, training, reporting and tracking procedures. The Board is especially pleased that the FBI Director has assured it that he is committed to developing a strong compliance program. The Board intends to offer its assistance toward the design and implementation of an effective program to promote compliance with the legal requirements that apply to the FBI's use of NSLs.

The Board is, of course, aware that Congress, the Department of Justice, and the FBI itself are evaluating the NSL situation and considering reforms to improve FBI compliance. The Board also will continue to evaluate the use of NSLs in order to offer advice and oversight to help prevent a recurrence of this serious and unfortunate failure to comply with the terms and conditions of the USA PATRIOT Act and laws authorizing FBI investigations.

The cause of protecting the nation from terrorism is not advanced by undermining the public's confidence in the government's ability to exercise investigative powers in compliance with applicable legal standards and required procedures. The formidable investigative powers extended in the USA PATRIOT Act can help protect our nation against terrorists, but only if utilized by all Federal officials in strict compliance with the requirements of the law and Executive Branch policy and guidance. Safeguards for privacy and civil liberties are not mere procedural formalities. They are essential to preservation of our constitutional rights and American values.

The Board will continue to address this very important matter as a top priority.

The Board appreciates the cooperation it has received from the President's senior staff and the relevant Federal departments and agencies in the past year. The Board also welcomes the independent oversight of Congress itself in weighing the country's national security needs to fight terrorism effectively while also assuring meaningful protection of privacy and civil liberties.

Sincerely,

Carol E. Dinkins
Chairman

Alan Charles Raul
Vice Chairman

Lanny J. Davis
Member

Theodore B. Olson
Member

Francis X. Taylor
Member

The Honorable Richard B. Cheney
President of the Senate
Washington, DC 20510

The Honorable Nancy Pelosi
Speaker of the House of Representatives
Washington, DC 20515

MAR:s

Enclosure: 2007 Annual Report to Congress

PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

2007 REPORT TO CONGRESS

I. INTRODUCTION 1
II. HISTORY AND MISSION 4
III. ORGANIZATION, ADMINISTRATION AND PROCESS 9
  A. Necessary Administrative Actions and Budget 9
  B. Substantive Actions to Fulfill Statutory Mandate 10
IV. OUTREACH AND EDUCATION 12
  A. The White House and Executive Office of the President 12
  B. Executive Branch 13
  C. Congress 17
  D. Media 18
  E. Private Sector, Non-profit, Academic, and Advocacy Groups and Experts 18
  F. International Forums 20
V. ISSUE IDENTIFICATION, PRIORITIZATION, AND DISCUSSION 21
  A. Scope and Process 22
  B. Specific Issues, Policies, Procedures, and Regulations 25
    1. Oversight of Existing Federal Anti-terrorism Policies and Programs 26
    2. Examples Where the Board Has Offered Advice Regarding the Development of a Policy, Program, Regulation, or Statute 32
    3. Information Sharing 35
VI. THE YEAR AHEAD 39
VII. CONCLUSION 42

I. INTRODUCTION

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which created the Privacy and Civil Liberties Oversight Board (Board), requires that "[n]ot less frequently than annually, the Board shall prepare a report to Congress, unclassified to the greatest extent possible . . . on the Board's major activities during the preceding period."[1] This report discusses the Board's activities from its first meeting on March 14, 2006, at which the Members were sworn in and an Executive Director was appointed, through March 1, 2007. This report contains no classified information.

Unlike other boards and commissions charged with addressing an issue, making recommendations, issuing a report and then disbanding, this Board embodies a permanent commitment to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations and executive branch policies related to efforts to protect the Nation against terrorism."[2] The President has repeatedly stated that as the Federal government works to prevent acts of terror against the Nation, its citizens, and its interests, it must do so in compliance with the law, protective of the rights and liberties guaranteed by the Constitution, and consistent with the values we share as Americans. The Board's statutory mandate and fundamental purpose is to further those objectives.

During its first year, the Board met approximately twice a month. The Board dedicated itself to organization, staffing, and substantive background briefings on significant Executive Branch anti-terrorism programs affecting privacy rights and civil liberties and meeting with interested members of the privacy and civil liberties community. These included meetings with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of the National Security Agency, the National Counterterrorism Center, the Federal Bureau of Investigation, and the Terrorist Screening Center as well as the National Security Advisor, the Homeland Security Advisor, the White House Chief of Staff, the White House Counsel, and the Information Sharing Environment Program Manager. The Board has been briefed at the highest level of classification on the NSA's surveillance programs, the Treasury Department's Terrorist Finance Tracking Program, and the National Counterterrorism Center's National Implementation Plan on the War on Terror. While the Board was unable in its first year to spend as much time on evaluating and providing oversight of programs most affecting privacy rights and civil liberties as it would have liked, as this Report describes in Section VI (The Year Ahead), the Board now has the appropriate foundation to provide the advice and oversight required by IRTPA.

---

[1] Pub. L. 108-458, §1061(c)(4) (Dec. 17, 2004).

[2] *Id.* § 1061(c)(1)(C).

In order to stand up its operation during the first year, the Board allocated its resources among three core areas, discussed below, to build a foundation on which to offer substantive advice and oversight. Activities in these areas have helped the Board establish its viability, subject matter expertise, and credibility. The Board unanimously identified substantive accomplishments in these three areas at the outset as necessary prerequisites for long term success and included them in its first annual agenda, adopted in June 2006. This first report to Congress outlines the Board's activities in these areas:

Organization, Administration and Process. The Board understood that, due to its part-time Membership, it had to establish the means and infrastructure necessary to help it accomplish its statutory mission. Toward that end, it has hired a professional staff, reached agreement with the Director of National Intelligence on the scope and logistics of detailing additional staff from within the intelligence community, acquired the necessary security clearances, built out appropriate office space with secured facilities for classified information, and developed a web site for communication with the public. Due to its position within the White House Office, the Board receives additional administrative support from White House staff.

Education and Outreach. The Board has engaged policy officials and experts within the Executive Branch, Congress, the public, and private, non-profit, and academic institutions. It has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism by meeting with senior officials, examining their missions and legal authorities, learning of their specific programs, and reviewing their operational methodologies and privacy and civil liberties training, reporting, and auditing programs. For example, the Board has met personally, among others, with the Attorney General, the Secretary of the Department of Homeland Security, the Director of National Intelligence, the Directors of the National Counterterrorism Center and National Security Agency, the Information Sharing Environment Program Manager, the Undersecretary of the Treasury for Terrorism and Financial Intelligence, and the President's senior staff. Among other non-governmental experts and advocacy groups, it has met with representatives from the American Civil Liberties Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Markle Foundation, and the American Conservative Union. It also held its first public forum at Georgetown University on December 5, 2006.

As a part of this education and outreach effort, the Board has made it a priority to work with a new and growing network of Executive Branch homeland security professionals specifically dedicated to consideration of privacy and civil liberties issues. The Board considers one of its fundamental responsibilities to foster a sense of community among these new professional privacy and civil liberties officers and members of the relevant professions that have existed within the Federal government for decades – including attorneys, inspectors general, and relevant program policy officials. The Board intends to continue providing these offices with the necessary support to enable them better to accomplish their own responsibilities.

Issue Prioritization. The Board's statutory authority is broad. The Board has focused on those issues that could provide the most value for the American people, the President, and the Executive Branch. Policies and programs warranting the Board's attention will evolve over time. Identification of these priorities will necessarily change as new initiatives are considered, developed, and implemented. This report outlines the process and consideration undertaken by the Board in developing and reviewing those issues.

With these foundational accomplishments behind it, the Board stands at the beginning of its second year well equipped to address further the substantive issues of its statutory mandate.

II. HISTORY AND MISSION

Following the attacks of September 11, 2001, Congress and the President established the National Commission on Terrorist Attacks on the United States (9/11 Commission or Commission), a bipartisan panel charged with investigating the events of 9/11 and offering "recommendations designed to guard against future attacks."[3] As the Commission acknowledged, many of its recommendations "call[ed] for the government to increase its presence in our lives – for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies."[4] However, the Commission also noted that "[t]he choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home."[5] Consequently, the Commission also recommended the creation of "a board within the Executive Branch to oversee . . . the commitment the government makes to defend our civil liberties."[6] In order to implement the Commission's numerous recommendations, Congress passed and President Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004.[7] Among other actions – including reshaping the intelligence community under one Director of National Intelligence[8] – IRTPA authorized the creation of the Privacy and Civil Liberties Oversight Board.

IRTPA requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism."[9] In carrying out this mandate, the Board has two primary tasks. *First*, it must "*advise* the President and the head of any department or agency of the Executive Branch to ensure that privacy and civil liberties are appropriately considered in the development and implementation"[10] of "laws, regulations, and executive branch policies related to efforts to protect the Nation from terrorism."[11] *Second*, it must exercise *oversight* by

[3] *National Commission on Terrorist Attacks on the United States, available at* http://www.9-11commission.gov/about/index.htm (last accessed Nov. 1, 2006).

[4] THE 9/11 COMMISSION REPORT, 393-94 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf (last accessed Nov. 1, 2006).

[5] *Id.* at 395.

[6] *Id.*

[7] Pub. L. 108-458 (Dec. 17, 2004).

[8] *Id.* § 1001 *et seq.*

[9] *Id.* § 1061(c)(3).

[10] *Id.* § 1061(c)(1)(C) (emphasis added).

[11] *Id.* § 1061(c)(1)(B).

"continually review[ing] regulations, executive branch policies, and procedures . . . and other actions by the executive branch related to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected."[12] The statute expressly requires the Board to advise[13] and oversee[14] the creation and implementation of the Information Sharing Environment (ISE).

In order to offer informed advice and oversight, the Board may access "from any department or agency of the executive branch, or any Federal officer or employee of any such department or agency[,] all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law."[15] And to allow Board Members timely access to classified materials to carry out their mandate, the statute requires "appropriate departments and agencies of the executive branch [to] cooperate with the Board to expeditiously provide Board members and staff with appropriate security clearances."[16] The Board may also demand that persons other than departments, agencies, and elements of the Executive Branch provide "relevant information, documents, reports, answers, records, accounts, papers, and other documentary and testimonial evidence."[17] If a Federal agency, official, or other relevant persons choose not to produce information requested by the Board, the Board may pursue a remedy by notifying the Attorney General or the head of the relevant agency. The Attorney General may then "take such steps as appropriate to ensure compliance" with the Board's request, including issuing subpoenas.[18] Although the Board may have general access to "materials necessary to carry out its responsibilities,"[19] materials may be withheld if "the National Intelligence Director [sic], in consultation with the Attorney General, determines that it is necessary . . . to protect the national security interests of the United States"[20] or if the Attorney General determines that it is necessary to withhold information "to protect sensitive law enforcement or counterterrorism information or ongoing operations."[21]

---

[12] *Id.* § 1061(c)(2)(A).

[13] *Id.* § 1061(d)(2).

[14] *Id.* § 1061(c)(2)(B).

[15] *Id.* § 1061(d)(1)(A).

[16] *Id.* § 1061(h).

[17] *Id.* § 1061(d)(1)(D)(i).

[18] *Id.* § 1061(d)(2)(B).

[19] *Id.* § 1061(d)(1).

[20] *Id.* § 1061(d)(4)(A).

[21] *Id.* § 1061(d)(4)(B).

As shown in the Board's location, assigned roles, and authority, IRTPA did not create an independent watchdog entity in the nature of an inspector general.[22] Rather, the statute created a Board that operates *within* the Executive Office of the President and ultimately reports to the President. The statute requires the Board to produce an annual report to Congress only "on [its] major activities"[23] – not on all of its internal deliberations and recommendations. The statute expressly places the Board within the Executive Office of the President (EOP), an office whose sole purpose is to support the Executive. Consistent with that placement and with the goal of offering candid advice,[24] the President has located the Board even more closely to him by placing it within the White House Office (WHO). As the statute explicitly acknowledges, all five Board Members (like other EOP and WHO employees) serve at the pleasure of the President.[25] By empowering the Board with broad access to records, IRTPA has created a Board that can offer a distinctly independent perspective to the President, along with oversight of executive agencies.

The Board acts in concert with a robust and developing privacy and civil liberties (PCL) infrastructure that is already operating throughout the Federal government, including offices within the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Office of the Director of National Intelligence (ODNI).[26] In most cases, these PCL offices are headed by officials with direct access to their agency heads. They are primarily staffed by diligent career civil servants who focus on and provide an additional degree of continuity regarding the appropriate consideration of privacy and civil liberties. As discussed below, the Board intends to provide a coordinating role for these PCL offices and will also assist in addressing unique problems that require government-wide coordination or specific White House involvement.[27]

IRTPA also sets the qualifications of the Board's Members. The President must appoint as Members "trustworthy and distinguished citizens outside the Federal Government who are qualified on the basis of achievement, experience, and

---

[22] *See, e.g.*, the Federal Inspector General Act of 1978, 5 U.S.C. Appx § 1 *et seq.*

[23] IRTPA § 1061(c)(4).

[24] Although the statute subjects the Board to the Freedom of Information Act (FOIA), *see id.* § 1061(i)(2), the regular exemptions to FOIA disclosure still apply. *See* 5 U.S.C. § 552(b).

[25] IRTPA § 1061(e)(1)(E) ("The chairman, vice chairman, and other members of the Board shall each serve at the pleasure of the President.").

[26] In IRTPA, Congress expressed its sense "that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." *Id.* § 1062.

[27] *Infra* Part V.B.2.

independence."[28] Both the Chairman and Vice Chairman of the Board also require Senate confirmation.[29] To these ends, President Bush appointed the following individuals as Members:

- ***Carol E. Dinkins, Chairman*** – Formerly served as Deputy Attorney General and Assistant Attorney General in charge of the Department of Justice's Environment and Natural Resources Division. She is a partner with Vinson & Elkins, L.L.P. in its Houston, TX office.

- ***Alan Charles Raul, Vice Chairman*** – Former General Counsel of both the U.S. Department of Agriculture and the Office of Management and Budget as well as Associate White House Counsel to President Reagan. He is a noted expert and author on privacy, data protection, and information security. He is a partner in Sidley Austin's Washington, DC office.

- ***Lanny J. Davis*** – Served as Special Counsel to President Bill Clinton and is a noted author and frequent television commentator. He is a partner in Orrick, Herrington and Sutcliffe's Washington, DC office.

- ***Theodore B. Olson*** – Served as U.S. Solicitor General from 2001 until 2004 and as Assistant Attorney General for the Office of Legal Counsel from 1981 until 1984. Mr. Olson is one of the Nation's premier appellate and Supreme Court advocates and is a partner in Gibson, Dunn and Crutcher's Washington, DC office.

- ***Francis X. Taylor*** – A retired Brigadier General with the U.S. Air Force and former Commander of the Air Force Office of Special Investigation. He also served as Assistant Secretary of State for Diplomatic Security and U.S. Ambassador at Large for Counterterrorism. He is presently the Chief Security Officer for the General Electric Company.

On February 17, 2006, the Senate confirmed Chairman Dinkins and Vice Chairman Raul. All five Members were sworn into office and held their first meeting on March 14, 2006. In taking office, the Board effectively took the place of the President's Board on Safeguarding Americans' Civil Liberties (President's Board), which the President created by Executive Order in 2004.[30] The President's Board was chaired by the Deputy Attorney General and consisted of 22 representatives from the Departments of State, Defense, Justice, Treasury, Health and Human Services, and Homeland Security,

[28] IRTPA § 1061(e)(1)(C).

[29] *Id.* § 1061(e)(1)(B).

[30] *See* EO 13353 (Aug. 27, 2004).

the Office of Management and Budget, and the Intelligence Community.[31] Following the enactment of IRPTA and the creation of the Board, the President's Board ceased to meet and transferred its papers to Board staff.

In addition to IRTPA, the Board works within the legal framework that guides all efforts to protect the Nation against terrorism.[32] Consequently, the Board has gathered and familiarized itself with relevant seminal documents and authorities that impact its mission.[33]

[31] The President's Board met as a full group six times and organized itself into six subcommittees. The six subcommittees were Investigative Legal Authorities, Redress Systems, Data Collection and Sharing Standards, Engagement with Arab-American Communities, Public Outreach, and Policies and Procedures.

[32] *See, e.g.*, IRTPA § 1061(d)(1) (allowing the Board to obtain documents subject to the statute's restrictions and "to the extent permitted by law").

[33] This list includes, but is not necessarily limited to: U.S. CONSTITUTION; Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 *et seq.*; *Strengthening the Sharing of Terrorism Information to Protect Americans*, EO 13388, 70 Fed. Reg. 62023 (Oct. 27, 2005); *Strengthening the Sharing of Terrorism Information to Protect Americans*, EO 13356 (Aug. 27, 2004), 69 Fed. Reg. 53599 (Sept. 1, 2004); *Strengthened Management of the Intelligence Community*, EO 13355 (Aug. 27, 2004), 69 Fed. Reg. 53593 (Sept. 1, 2004); *National Counterterrorism Center*, EO 13354 (Aug. 27, 2004), 69 Fed. Reg. 53589 (Sept. 1, 2004); *Establishing the President's Board on Safeguarding Americans' Civil Liberties*, EO 13353 (Aug. 27, 2004), 69 Fed. Reg. 53585 (Sept. 1, 2004); *Conduct of Intelligence Activities*, EO 12333, 46 Fed. Reg. 59941 (1981); *Memoranda from the President to Congress and Executive Departments and Agencies: Guidelines and Requirements in Support of the Information Sharing Environment* (Dec. 16, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html (last accessed Jan. 4, 2006); THE 9/11 COMMISSION REPORT; COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION: REPORT TO THE PRESIDENT OF THE UNITED STATES (March 31, 2005).

III. ORGANIZATION, ADMINISTRATION AND PROCESS

The Board has established and instituted the means and infrastructure to support it in accomplishing its statutory mission. As mentioned previously, the Board operates within the White House Office, a unit within the Executive Office of the President. Given this placement, the Board follows established White House Office policies in carrying out its administrative and budgetary responsibilities.

A. Necessary Administrative Actions and Budget

In order to manage its everyday affairs, the Board has hired a full-time staff. As an initial matter, it hired an Executive Director, Mark A. Robbins, who previously served as General Counsel of the U.S. Office of Personnel Management. Shortly thereafter, it hired a Deputy Executive Director and Counsel, Seth M. Wood, and a Staff Assistant, John V. Coghlan. The Board's staff communicates on a daily basis with all Members and regularly reports its activities to the Board. Staff – in conjunction with the Office of Government Ethics[34] and ethics counsel within the White House Counsel's office – have identified and clarified the relevant legal, ethical, and financial rules and guidelines applicable to special government employees,[35] as defined by law. The Members have entered into ethics agreements that ensure that their activities on behalf of clients and employers do not conflict with their service on the Board.

The Board has also begun the process of securing detailees from other agencies.[36] The former Director of National Intelligence determined that a detail assignment to the Board for a period of one year will fulfill the "joint duty" requirement for professional advancement within the intelligence community and requested that each of the 16 intelligence agencies reporting to ODNI propose candidates for such a detail

[34] Members and staff have held two formal meetings with the Office of Government Ethics and have sought informal advice as needed.

[35] Due to their part-time status, Board Members are classified as special government employees. 18 U.S.C. § 202(a) (defining a "special government employee" as one "who is retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days"). In order to determine a Member's employment status, staff has established a process for reporting and recording the time Members spend on Board activity.

[36] IRTPA § 1061(g)(2).

assignment.[37] The Board is not required to reimburse home agencies for detailees under the provisions of IRTPA.[38]

As a WHO unit, the Board did not have to hire separate staff dedicated to press and communications, legislative affairs, administration, or information technology but instead has utilized the services of the relevant components of the White House Office. The Board's administrative support staff has been integrated into the regular operations of the WHO and attends regularly-scheduled meetings with the White House Office of Management and Administration.

IRTPA requires the Board to adopt rules and procedures for physical, communications, computer, document, personnel, and other security in relation to the work of the Board.[39] As a WHO unit, the Board adopted the existing rules and procedures of the EOP.

Staff has carried out other necessary duties to allow Board Members full access to the potentially classified and otherwise sensitive documents necessary to complete their statutory obligations. For example, working with the relevant Executive authorities, Members and staff have obtained Top Secret/SCI clearances. Staff and the Office of Administration have also constructed appropriate office space to house the Board's operations within the White House complex. This suite includes secure facilities for the review and storage of classified information, as well as secure telephone and fax lines. The Chairman, Vice Chairman, and Board staff were issued passes that allow them general access to the White House complex.

B. Substantive Actions to Fulfill Statutory Mandate

In carrying out its substantive statutory mandates, the Board has formally met 23 times in its first year. All but five of these meetings occurred in person, and all but two had unanimous attendance. All meetings took place in or around Washington, DC – within the White House complex, at various departments and agencies, and one meeting at Georgetown University. To place the activity of the Board's part-time membership in perspective, the Board has formally met an average of about once every two weeks. Members always remain in near-constant communication with each other and the staff through e-mail and telephone. In the first few months of operation, the Board adopted a number of formative procedures and policies, including issue prioritization, everyday operations, public communications, and analytical methodologies.

[37] IRTPA also authorizes the Board to hire the services of consultants as necessary. *Id.* § 1061(g)(3).

[38] *Id.* § 1061(g)(2).

[39] *Id.* § 1061(h).

As an initial matter, the Board adopted its first annual agenda. The agenda functioned as a business plan by allocating responsibility for tasks among staff and setting expectations regarding how the Board would function. It also served as a substantive agenda by laying out an initial list of issues on which the Board agreed to focus its energies. The Board adopted a communications plan that laid out a strategy for engaging the public through direct means (such as a website and publications in the *Federal Register*) and through media outlets (both traditional and emerging). As part of its direct communication strategy, the Board approved the creation of a web site – www.privacyboard.gov – to discuss the Board's history, mission, and activities and provide the public access to Board Member biographies, Board statements, and other related documents. The web site also serves as a means by which the public may contact the Board.

The Board also developed a series of preliminary processes, procedures, and methods by which it could fulfill its advice and oversight responsibilities to the President and Executive Branch agency heads. Of greatest importance, it agreed upon a methodology for analyzing and evaluating proposed programs. It established both a regular means for Board staff to report their activities to the Members and a means of discussing issues and offering possible actions for the Board to take. It also adopted a set of White House Security Guidelines. These processes and templates are discussed in greater detail in Section V.A.

IV. OUTREACH AND EDUCATION

The Board moved immediately to establish lines of communication within and outside the Federal government, to educate itself on relevant issues of interest and concern relating to efforts to protect the Nation against terrorism, and to educate others on its mission and oversight and advisory roles.

A. The White House and Executive Office of the President

In order to obtain the most complete, real-time access to information regarding proposed and operational anti-terror programs, the Board has had to establish trust and credibility between itself and the relevant members of the Executive Branch. To that end, the Board has developed a sound, regular, and productive working relationship with the President's most senior advisors tasked with anti-terrorism responsibilities. This relationship has put the Board in a position to integrate itself into the policymaking process and obtain the necessary support from the Administration to offer meaningful advice.

The Board has met personally with the following principal senior White House officials:

- The current Chief of Staff and the former Chief of Staff
- The National Security Advisor
- The Homeland Security and Counterterrorism Advisor
- The current Counsel to the President and the former Counsel to the President
- The Staff Secretary
- The General Counsel of the Office of Management and Budget
- The Chairman of the Intelligence Oversight Board

These meetings have allowed the Board to forge strong working relationships with agencies and offices within the Executive Office of the President, including the National Security Council, Homeland Security Council, Office of Management and Budget, Office of the Counsel to the President, and the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board, among others. Additionally, the Board's professional staff meets weekly with an EOP working group that consists of

commissioned officer representatives from the Office of the White House Chief of Staff, the National Security Council, the Homeland Security Council, the Office of the Counsel to the President, the Office of Legislative Affairs, the Office of Communications, and the Office of Management and Budget.

B. Executive Branch

The Board has also met with senior administration officials throughout the Executive Branch who have responsibilities for developing and implementing war-on-terrorism policies and strategies. These officials include:

- The Attorney General
  - The Deputy Attorney General
  - The Assistant Attorney General for Legal Policy
  - The Assistant Attorney General for National Security
  - The Acting-Assistant Attorney General for Legal Counsel
- The Secretary for Homeland Security
- The Under Secretary of the Treasury for Terrorism and Financial Intelligence
  - The Assistant Secretary of the Treasury for Intelligence and Analysis
- The former Director of National Intelligence
  - The former Principal Deputy Director of National Intelligence
  - The Information Sharing Environment (ISE) Program Manager
  - The ODNI General Counsel
- The FBI Director
- The Director of the National Security Agency
  - The former National Security Agency Inspector General

- The Director of Signals Intelligence
- The National Security Agency General Counsel

- The Director of the National Counterterrorism Center
  - The Deputy Director for Strategic Operational Planning
- The former Director of the Terrorist Screening Center

The Board and its staff have made repeated visits to a number of government facilities to observe how those agencies operate, develop anti-terror policies, and train their employees to protect privacy and civil liberties. On-site visits also tend to promote a high-quality dialogue between Board Members and advisors. Consequently, the Board has personally visited the Department of Justice, the Department of Homeland Security, the National Security Agency, the National Counterterrorism Center, the Terrorist Screening Center, the Federal Bureau of Investigation, and the Department of Defense Counterintelligence Field Activity Office.

Perhaps most importantly, the Board has established strong working relationships with the developing privacy and civil liberties offices within the government. These offices and officers advance privacy and civil liberties at the ground level and generally have the greatest practical impact on the development and implementation of policies within their respective agencies. The privacy and civil liberties offices with which the Board works most closely include those at the Department of Justice, the Department of Homeland Security, and the Office of the Director of National Intelligence. These officials have likewise developed lines of communication and authority within their organizations' structure.

These relationships allow the Board to encourage the sharing of information and best practices among those offices. The relationships have also allowed the Board to coordinate and offer assistance when the privacy or civil liberties officers encounter problems. The Board has helped and will continue to help coordinate and foster the development of a privacy and civil liberties infrastructure throughout the Executive Branch. Before discussing the Board's activities, including its review of specific issues, policies, and procedures as described in Part V, *infra*, the Board wishes to summarize some of the major activities of the PCL offices with which it has most closely worked over the past year.

- Department of Justice: Like the Board, over the past year the DOJ Privacy and Civil Liberties Office has also begun its initial work in earnest. The Violence Against Women and Department of Justice Reauthorization Act of 2005[40] required the Attorney General to appoint a senior official to assume primary responsibility for privacy policy. The Attorney General appointed the Department's first Chief Privacy and Civil Liberties Officer on February 21, 2006. Placed within the Office of the Deputy Attorney General, the DOJ Privacy Office considers issues relating to the Privacy Act, privacy and civil liberties, and e-government compliance. Among other activities, this office joined DHS and other Federal entities in the delegation that represented the United States in negotiations with the European Union regarding the transfer of Passenger Name Record (PNR) information from Europe to the Bureau of Customs and Border Protection. In participating in these negotiations, this delegation helped ensure that all parties adequately considered privacy and civil liberties interests. In conjunction with the ODNI Civil Liberties and Privacy Office, the DOJ Privacy Office also helped draft privacy guidelines governing the ISE. The office has also worked with the Board and other privacy and civil liberties offices to assist in drafting a Memorandum of Understanding that will establish standardized procedures to address complaints regarding air travel watch lists.

- The Office of the Director of National Intelligence: Like the Board, the ODNI Civil Liberties and Privacy Office (CLPO) came into existence with the passage of IRTPA. The statute requires CLPO to ensure that civil liberties and privacy protections are appropriately incorporated into the policies of the ODNI and the intelligence community, oversee compliance by the ODNI with legal requirements relating to civil liberties and privacy, review complaints about potential abuses of privacy and civil liberties in ODNI programs and activities, and ensure that technologies sustain and do not erode privacy. The Director of National Intelligence appointed the Civil Liberties Protection Officer to lead the CLPO. In addition to completing a number of necessary stand-up requirements, the ODNI has, through the work of the CLPO, established internal ODNI policy for protection of privacy and civil liberties. In addition, the CLPO has identified a senior official at each intelligence agency to serve as the focal point of privacy and civil liberties issues at that agency. Perhaps most importantly, the CLPO co-drafted the privacy protection guidelines that govern the Information Sharing Environment and is co-chairing the process for ensuring that agencies have sufficient guidance and support to implement the guidelines effectively and consistently. Moreover, the CLPO has conducted numerous reviews of intelligence community programs and activities, helped shape significant policies and guidelines, and established procedures for community personnel to provide the CLPO with information about possible privacy and civil liberties abuses.

[40] Pub. L. 109-162 (Jan. 5, 2006).

- The Department of Homeland Security: The DHS Privacy Office is the first statutorily created privacy office[41] within the Federal government dedicated to the oversight of privacy protections. As such, the Chief Privacy Officer serves as the primary advisor on privacy matters and, by designation, departmental disclosure matters to the Secretary of Homeland Security. In addition to privacy policy advice, the DHS Privacy Office works (1) to assure that the use of technologies sustain and do not erode privacy protections; (2) to assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices; (3) to evaluate legislative and regulatory proposals involving personal information within federal government; (4) to conduct privacy impact assessments of proposed rules of DHS; (5) to coordinate with the Officer for Civil Rights and Civil Liberties; and (6) to prepare an annual report to Congress on activities of the Department that affect privacy. The Privacy Office is structured into two functional components: privacy and freedom of information. The freedom of information component addresses issues to include FOIA and Privacy Act requests and appeals and FOIA policy and regulations. The privacy component addresses the above statutory and policy-based responsibilities, in a collaborative environment, to include Compliance; International Privacy Policy; Legislative and Regulatory Affairs; and Technology. Much of the Privacy Office work focused on developing a compliance framework for the Privacy Act and E-Government Act. This effort standardized and harmonized privacy compliance concerning Privacy Impact Assessment (PIA) and System of Records Notice (SORN) reporting requirements. Both documents require agencies to complete an analytical template that describes the intended benefits of a particular program or change, the possible privacy concerns or risks generated by such a program or change, and how the agency mitigates privacy risks. Operationally, the Privacy Office provided privacy advice regarding the Secure Flight program, reviewed the implementation of the arrangement to transfer PNR information from air carriers in the European Union to the Bureau of Customs and Border Protection, participated with DOJ and DHS Privacy and Civil Liberties officers in drafting the ISE Privacy Guidelines, and advised DHS on privacy issues concerning data governance and data security.

  The DHS Office for Civil Rights and Civil Liberties (CRCL) has a relatively broad responsibility to ensure that DHS programs and activities comply with constitutional, statutory, regulatory, policy, and other requirements related to civil rights and civil liberties. It also must investigate complaints that allege possible abuses of civil rights or civil liberties. The CRCL is led by the Officer for Civil Rights and Civil Liberties. Of specific relevance to the Board, the CRCL has focused a great deal of its efforts on resolving complaints arising from the use of aviation watch lists. Along these same lines, the CRCL has worked with the

[41] Pub. L. 107-296, § 222 (Nov. 25, 2002) (codified at 6 U.S.C. § 142).

Board and other privacy officers to develop a standardized procedure – to be embodied in a Memorandum of Understanding – to resolve watch list complaints.

The Departments of State, Treasury, and Defense have also designated officials to act as privacy points of contact for the Board. The Board anticipates and looks forward to building similar working relationships with other privacy and civil liberties offices throughout the Executive Branch.

C. Congress

Board Members and the White House Office of Legislative Affairs have reached out to Senators and Representatives to brief them on the Board's mission, priorities, and activities, as appropriate. The Chairman and Vice Chairman have responded to all Congressional requests for testimony. The Board has also authorized its Executive Director to ensure that appropriate lines of communication and information exist between it and Congress. These Congressional interactions include the following:

- On November 8, 2005, Carol Dinkins and Alan Raul testified at their confirmation hearing before the Senate Judiciary Committee. Prior to their confirmation hearing, they conducted courtesy visits with Senators John Cornyn, Richard J. Durbin, Edward M. Kennedy, Jeff Sessions, and Arlen Specter.

- On May 4, 2006, the Executive Director met with a bipartisan group of staff from the House Permanent Select Committee on Intelligence.

- On June 6, 2006, Chairman Dinkins and Vice Chairman Raul testified before the House Government Reform Subcommittee on National Security, Emerging Threats, and International Relations.

- On August 10, 2006, the Executive Director met with majority staff from the Senate Committee on Homeland Security and Governmental Affairs.

- On November 3, 2006, the Executive Director met with minority staff from the Senate Judiciary and Senate Homeland Security and Governmental Affairs Committees.

- The Executive Director worked with Senate Judiciary Committee staff regarding certain administrative matters relating to confirmation materials.

- On November 27, 2006, Carol Dinkins, Alan Raul and Lanny Davis briefed bipartisan staff from the Senate Judiciary, Intelligence and Homeland Security Committees.

- On December 13, 2006, the Executive Director met with staff of Representatives Shays, Maloney, and Thompson.

- On December 19, 2006, Member Lanny Davis and the Executive Director met with staff to Senators Lieberman and Durbin.

- On February 8, 2007, the Executive Director met with minority staff of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security.

- The Board has either corresponded with individual Members of Congress or been the subject of correspondence between Members and the Executive Office of the President on a number of occasions since enactment of the Intelligence Reform and Terrorism Prevention Act of 2004.[42]

D. Media

The Board works in coordination with the White House Communications and Press offices. On September 10, 2006, Members Lanny Davis and Ted Olson appeared on a Discovery Channel special hosted by Ted Koppel entitled *The Price of Security*. Members of the media were invited to attend the Board's December 5 2006 public meeting, and Board Members gave numerous interviews following that event. Additionally, media representatives are encouraged to monitor the Board's web page (www.privacyboard.gov) for activities and statements. The Board has been the subject of numerous articles nation wide in the press and on-line. Members believe they have responded to all requests for interviews or comments.

E. Private Sector, Non-profit, Academic, and Advocacy Groups and Experts

The Board has set as a high priority engaging in a productive and ongoing dialogue with privacy, non-profit, and academic organizations within the privacy and civil liberties community. These conversations have helped identify issues important to the community, exchange ideas regarding how to craft anti-terrorism policies and procedures, and establish trust between the Board and the community. For example, the Board has strived to communicate regularly with the co-chairs of the 9/11 Commission, Governor Thomas Kean and Congressman Lee Hamilton.[43] Chairman Dinkins and Vice

[42] The Board and its activities have been referenced in two Congressional reports: (1) House Permanent Select Committee on Intelligence Oversight Subcommittee's report: *Initial Assessment on the Implementation of the Intelligence Reform and Terrorism Prevention Act of 2004* (July 2006); and (2) Government Accountability Office report: *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public* (September 2006).

[43] As noted previously, the Commission's recommendations led to the Board's creation.

Chairman Raul met collectively with Governor Kean and Congressman Hamilton and apprised them of the Board's major activities. They have also held individual telephone conferences with Governor Kean and Congressman Hamilton. Following the December telephone conference, Congressman Hamilton requested the Board's executive director to contact him every 60 days with additional updates on the Board's efforts. In addition, the Board's executive director has met with former Commission executive director Philip D. Zelikow and Commission General Counsel Daniel Marcus. The Board is dedicated to meeting the letter and spirit of the 9/11 Commission's recommendations, consistent with its statutory authority, and looks forward to continued contact with the Commission's co-chairs.

Additionally, the Chairman and Vice Chairman met with representatives from the American Civil Liberties Union and the Center for Democracy and Technology within the first two months of the Board's operation. The Board also has held meetings with: the American Conservative Union, the Center for Strategic and International Studies, the Electronic Privacy Information Center and the Privacy Coalition, the Markle Foundation, the Cato Institute, the Heritage Foundation, the Liberty Coalition, and the National Institute of Standards and Technology. Board representatives have appeared at the Progress and Freedom Foundation's Annual Aspen Summit, the U.S. Army Judge Advocate General's School Advanced Intelligence Law Conference, and the Intelink and the Information Sharing Conference and Technology Exposition.

The Board has also appeared before or participated in advisory committees and workshops conducted by DHS (the Data Privacy and Integrity Advisory Committee), ODNI (Privacy Protection Technologies Workshops hosted by ODNI and the Disruptive Technologies Office), DOJ (Intergovernmental Privacy Issues Forum and Global Justice Information Sharing Initiative, Global Advisory Committee), American University (Masters of Public Administration Seminar on Separation of Powers), and National Academies of Science (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and other National Goals).

On December 5, 2006, Georgetown University's Institute for International Law and Politics hosted the Board's seventeenth meeting, a public forum discussion between the Board, privacy and civil liberties advocacy groups, academicians, and the public. The Board was joined by the Civil Liberties Protection Officer at the Office of the Director of National Intelligence, the Chief Privacy and Civil Liberties Officer at the Department of Justice, and the Officer for Civil Rights and Civil Liberties at the Department of Homeland Security. Panelists included Caroline Fredrickson, Director of the Washington Legislative Office of the American Civil Liberties Union; David Keene, Chairman of the American Conservative Union and Co-chair of the Constitution Project's Liberty and Security Initiative; Marc Rotenberg, Executive Director of the Electronic Privacy Information Center; Michael Ostrolenk, Co-founder and National Director of the Liberty Coalition; Brian Walsh, Senior Legal Research Fellow at the Heritage Foundation; James Dempsey, a member of the Markle Foundation Task Force on National Security in the

Information Age; Fred Cate, Distinguished Professor and Director for the Center for Applied Cybersecurity Research at Indiana University; Peter Swire, the C. William O'Neill Professor of Law at Ohio State University and former Chief Counselor for Privacy in the U.S. Office of Management and Budget under President Clinton; Neal K. Katyal, Professor of Law at Georgetown University; and Anthony Clark Arend, Professor of Government and Foreign Service and Director of the Institute for International Law and Politics at Georgetown University.

F. International Forums

As appropriate, the Board intends to participate in international discussions on issues of relevance and interest. For example, Vice Chairman Alan Raul represented the Board as a member of the U.S. delegation to the 28th International Data Protection and Privacy Commissioners' Conference in London on November 2 and 3, 2006. This is an annual gathering of the various European Union and other International Data Protection officers. The U.S. has observer status to this conference. The delegation is led by the Department of Homeland Security and also includes representatives from the Department of Justice and Federal Trade Commission.

V. ISSUE IDENTIFICATION, PRIORITIZATION, AND DISCUSSION

As previously explained, IRTPA vests the Board with the broad mandate to provide advice and oversight concerning "regulations, executive branch policies, and procedures (including the implementation of such regulations, policies, and procedures), related laws pertaining to efforts to protect the Nation from terrorism, and other actions by the executive branch related to efforts to protect the Nation from terrorism."[44] Consistent with these statutory responsibilities, the Board considered how it could set its scope, agenda, and methodology in order to advise the President in as effective a manner as possible and in a manner that will bring the greatest value to the American people. To these ends, the Board began to identify and evaluate proposed and existing programs and policies that fall within its statutory mandate. Obviously, the list of policies and programs warranting the Board's attention will evolve over time. Additionally, as new policies are considered, developed, and implemented, the Board's identification of priorities will necessarily change as well.

As a general matter, the Board encounters and engages issues using one of three approaches:

- **Vertical Review**: At the direction of the President, through the request of an Executive Branch department or agency head, or as a result of self-initiation, the Board engages in an in-depth review and analysis of a particular policy or program.

- **Horizontal Review**: The Board examines an issue as part of existing policy development and implementation processes within the Executive Office of the President and the Executive Branch. The Office of Management and Budget (OMB) has integrated the Board into the Legislative Referral Memorandum (LRM) process. Through this process, the Board reviews Administration-wide policies, regulations, and programs that involve its statutory mission.

- **Initial Spot Review**: The Board informally gathers basic information on a policy, program, or issue that Board Members believe could implicate privacy and civil liberties concerns. This approach allows the Board to determine whether a more formal review is necessary.

[44] IRTPA § 1061(c)(2)(A).

A. Scope and Process

In construing the mandate contained in IRTPA, the Board has initially determined that it will focus its efforts on issues concerning U.S. Persons[45] or occurring on American soil. As a result, it will not evaluate specific issues associated with the uniformed services' efforts against terrorism or activities directed against non-U.S. persons abroad. IRTPA instructs the Board to ensure the consideration and protection of "privacy and civil liberties" but neither defines this phrase nor guides the Board in determining whose privacy and civil liberties should warrant the Board's attention. In order to maximize the Board's effectiveness and to prevent the diffusion of its limited resources across too many programs, the Board has elected to concentrate on the United States and U.S. Persons.[46]

In making this decision, the Board considered the structure and purpose of IRTPA, its legislative history, common canons of statutory construction, and how to carry out its statutory mandate most effectively. As an initial matter, the Congressional findings in IRTPA concerning the Board suggest that "privacy and civil liberties" should have a domestic focus by "call[ing] for an enhanced system of checks and balances to protect the precious liberties that are vital to *our* way of life."[47] IRTPA – particularly the title that contains the Board[48] – has a domestic focus,[49] does not generally address military or diplomatic actions abroad, and does not reference interrogation, non-U.S. detention, or rendition practices.

[45] A "U.S. Person" is defined, *inter alia*, as a United States citizen or a lawful permanent resident alien. *See, e.g.*, 50 U.S.C. § 1801(i); Executive Order 12333 § 3.4(i).

[46] The Board reserves the right to revisit this determination as circumstances or events may warrant.

[47] IRTPA § 1061(a)(2) (emphasis added). Indeed, the findings preceding the formal creation of the Board link the operation of the Board to the "potential shift of power and authority to the Federal Government . . . [i]n conducting the war on terrorism." *Id.* § 1061(a)(1).

[48] Title I – the portion of the Reform Act where Congress placed the Board – largely confines itself to organizational and structural matters.

[49] For example, the statute attempts to improve national security through a variety of actions, including restructuring the Federal intelligence-gathering apparatus, *id.* §§ 1011-1023, strengthening security measures for cargo, *id.* §§ 4051-54, transportation, *id.* §§ 4011-29, and border enforcement, *id.* §§ 5101-5204, and reforming certain immigration laws. *Id.* §§ 5401-5506.

Legislative history – in the form of the 9/11 Commission Report and in Senate debate accompanying passage of IRTPA – also contains a domestic focus. In its preface to recommending the creation of the Board, the Commission Report highlighted the impact of its recommendations on U.S. Persons' rights: "Many of our recommendations call for the government to increase its presence *in our lives* – for example, by creating standards for the issuance of forms of identification, by better securing our borders, by sharing information gathered by many different agencies."[50] The Commission connected this potential harm to domestic liberties to the Board's charge: "At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend *our* civil liberties."[51] Similarly, during debate on the IRTPA conference report, numerous Senators emphasized what one characterized as Congress' desire to "protect the lives of *Americans*, and [to] protect *their* liberties. That is what the Board is setting out to do."[52]

Certain canons of statutory construction, including the presumption against extraterritoriality,[53] also suggest that IRTPA's provisions authorizing the Board should not reach beyond the Nation's borders. Additionally, the Board is reluctant to oversee traditional Commander-in-Chief authorities – including combat operations – without a specific and express legislative mandate.

---

[50] 9/11 COMMISSION REPORT at 393-94 (emphasis added).

[51] *Id.* at 395 (emphasis added).

[52] *Debate on the Conference Report of the Intelligence Reform and Terrorism Prevention Act of 2004*, 150 Cong Rec 11939, 11949 (Dec. 8, 2004) (statement of Senator Durbin) (emphases added); *see also id.* at 11939 ("The creation of this Board is intended to ensure that at the same time we enhance our Nation's intelligence and homeland defense capabilities, we also remain vigilant in protecting *the civil liberties of Americans*.") (statement of Senator Dodd) (emphasis added); *id.* at 11978 ("The bill provides *protections for the rights of Americans* by creating a Privacy and Civil Liberties Oversight Board . . . .") (statement of Senator Mikulski) (emphasis added); *id.*("While Americans are more willing to give up some of their privacy after 9/11, necessary intrusions must be carefully balanced against the *rights of U.S. citizens* and I believe the Board will help maintain the balance.") (statement of Senator Reed) (emphasis added).

[53] *See, e.g., Small v. United States*, 544 U.S. 385, 388-89 (2005) (noting that courts begin with "legal presumption that Congress ordinarily intends its statutes to have domestic, not extraterritorial, application"); *Arc Ecology v. United States Dep't of the Air Force*, 411 F.3d 1092, 1097 (9th Cir. 2005) ("Courts must assume that Congress legislates with knowledge of the presumption that a statute is primarily concerned with domestic conditions.") (internal quotation marks omitted).

Moreover, construing the scope of the Board's mandate substantially implicates questions regarding how best to allocate time and resources. The Board has decided to use these resources in a manner to serve the greatest number of United States citizens and other U.S. Persons. Congress stands in a stronger position to oversee American anti-terrorism activities conducted abroad than the Board or its Members.

In addition to determining the general reach of its mandate, the Board established a standardized means to evaluate how well privacy and civil liberties have been considered in the development and implementation of anti-terrorism policies and programs. To that end, the Board has developed an "issues and process analysis methodology" that will bring full and consistent consideration of all issues that come before it.[54] This methodology allows the Board to consider separate substantive questions and the extent to which privacy and civil liberty officers within the relevant agency have meaningfully participated in the development and implementation of the policy or program. The methodology takes into account five large issues, as well as a number of subsidiary questions, including:

- The scope of the program
- The program's legal basis
- How the program supports efforts to protect the Nation against terrorism from the perspective of managing risk to privacy or to survival
- The extent to which officials within the relevant department or agency analyzed the privacy and civil liberties interests implicated by the policy, program or issue, including factors such as
    - **Privacy:** *How does the program affect individuals' ability to control how personal information about them is collected, used, maintained, or shared?*
    - **Fairness:** *Does the program treat individuals fairly at every step?*

[54] The Board wishes to acknowledge and thank Jim Harper, Director of Information Policy Studies at the Cato Institute, and the Department of Homeland Security Data Privacy and Integrity Advisory Committee, on which Mr. Harper sits, for their guidance and earlier work product, upon which much of this is based. *See, e.g., Framework for Privacy Analysis of Programs, Technologies, and Applications*, Department of Homeland Security Data Privacy and Integrity Advisory Committee, Report No. 2006-01 (March 7, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf (last accessed Jan. 29, 2007).

- **Civil Liberties:** *Does the program limit individual civil liberties in some dimension? What specific Constitutional or statutory interests are affected?*

- **Respect for the Individual:** *Does the program adequately preserve, to the extent possible, human dignity, autonomy, freedom of thought, expression and association?*

- **Data Security:** *How is personal information secured against threats to privacy and integrity?*

- Processes employed by the government to review privacy and civil liberties interests. This factor considers the existence and format of review procedures, how the government ensures that employees follow these procedures, the training required of employees, and how the government updates its policies.

With respect to internal deliberations, the Board has formalized procedures to allocate work and assignments among Board Members. For example, these procedures have allocated assignments to: Vice Chairman Raul to coordinate the Board's efforts concerning watch list redress procedures; Vice Chairman Raul and Member Davis to examine the NSA's surveillance activities; Member Frank Taylor to examine the Department of Defense Counterintelligence Field Activity (CIFA) TALON program; and Member Davis to examine elements of the reauthorized USA PATRIOT Act.

The Board has also developed a standardized format for reporting internal deliberations and investigations and offering recommendations to the full Board. This report format includes background information, the legal authority underlying a given program or policy, the existing privacy and civil liberties infrastructure, benefits of the program or policy, privacy concerns, sources consulted, an evaluation of the consideration of privacy and civil liberties interests in the development or implementation of the program or policy, and recommendations to the Board. These pre-decisional reports are considered by the full membership of the Board at its regular meetings.

B. Specific Issues, Policies, Procedures, and Regulations

Employing this standardized methodology and operating within its statutory mandate, the Board has evaluated numerous proposed and currently existing terrorism-prevention policies, regulations, statutes, and other Executive actions. Some issues came to the Board's attention through its numerous meetings with privacy advocacy organizations, Executive officials, and Congressional leaders. The Board engaged other issues because media reports brought them to its attention, and other matters arose simply because the Board has begun to integrate itself into the regular Executive decision-making and policy

implementation processes. In all of its efforts, the Board has had the opportunity to ask whatever questions it desired and has received answers to those questions. The following list of matters on which the Board has offered advice and oversight is intended not to be exhaustive but rather to offer a representative sample of issues that the Board has considered during its relatively brief existence. The Board is careful below not to reference facts, issues, or materials of a classified nature.

1. Oversight of Existing Federal Anti-terrorism Policies and Programs

The Board has begun its efforts to review some of the Federal government's most sensitive and far-reaching surveillance programs. As discussed below in greater detail, these programs include National Security Agency surveillance programs (such as the former Terrorist Surveillance Program (TSP) and the current program governed by the Foreign Intelligence Surveillance Court) and the Terrorist Finance Tracking Program (TFTP). The Board also has received initial briefings on the National Implementation Plan (NIP).

At its first meeting on March 14, 2006, the Board determined that it would have an on going interest in monitoring the government's various surveillance programs. In order to bring any kind of value to their analysis, however, the Members decided that they first had to understand fully the scope of the government's efforts to protect the Nation against terrorism. Consequently, the Board undertook an extensive effort of educational due diligence. The Board believes that receiving premature briefings on any specific program without understanding the full context in which that program operates would not serve to help it fulfill its statutory mission.

The Board has taken great care and exercised due diligence to become familiar with the departments and agencies responsible for protecting the Nation against terrorism. The Board has examined the agencies' and departments' mission and legal authorities, as well as their operational methodologies and privacy and civil liberties training, reporting, and auditing programs.[55]

Following the Board's educational efforts, and with the support of the Attorney General, the Director of National Intelligence, and the President's Chief of Staff, the Board formally requested a briefing on the TSP and TFTP in September 2006. The President's approval followed promptly, and the briefings were immediately scheduled.

[55] For example, the Board's Vice Chairman and Executive Director attended a session of the standard National Security Agency employee privacy training given to all new employees and once every other year to all current employees. This training is based, among other authorities, on the requirements of U.S. Signals Intelligence Directive 18, which regulates the collection and use of information on U.S. Persons within the signals intelligence community.

- *Terrorist Surveillance Program and January 10, 2007 Orders of the Foreign Intelligence Surveillance Court*

The Board devoted substantial time and focus in its first year of operation to reviewing anti-terrorist surveillance conducted by the National Security Agency (NSA) and the Terrorist Surveillance Program (TSP) described by the President on December 17, 2005.[56] The TSP involved surveillance of communications where one party to the communication is outside the United States and the government has probable cause to believe that at least one party to the communication is a member or agent of al Qaeda, or an affiliated terrorist organization.

The Board's review of the NSA's surveillance activities was conducted in the course of various briefings by senior NSA personnel, including the Director, and through briefings, questioning, and other interaction with analysts and program operators. Board members repeatedly visited NSA and observed the physical operations where the relevant surveillance is conducted. In particular, the Board reviewed material supporting the government's determination that there was probable cause to believe that at least one of the parties to a surveilled communication was a member or agent of al Qaeda or an affiliated terrorist organization.

The Board also received briefings and had opportunities to question NSA lawyers from the Office of General Counsel, Inspector General officials, and other knowledgeable personnel. The Board discussed TSP with the Attorney General, the Acting Assistant Attorney General for the Office of Legal Counsel, and the current and former Counsel to the President, among other knowledgeable officials in the Executive Branch.

The Board was briefed on the multiple levels of review, approval and oversight for conducting this surveillance. At the NSA, operators must carefully justify tasking requests, and multiple levels of review and approval are required to initiate collection. Ongoing audits and legal reviews are conducted by the NSA's Office of Inspector General, General Counsel, and Signals

[56] As noted below, the Board reviewed the operations of both the TSP (which has now ceased) and the surveillance program governed by the Foreign Intelligence Surveillance Court (FISC).

Intelligence Directorate Office of Oversight and Compliance. No surveillance may be conducted without leaving a reviewable audit trail that can be and routinely is subject to extensive continuing examination by Inspector General and Compliance staff.

In addition, the members of the Board reviewed U.S. Signals Intelligence Directive 18 (USSID 18), which reflects the classified guidelines established by the NSA and approved by the Attorney General pursuant to Executive Order 12333 to ensure that information about U.S. Persons is protected from improper or excessive collection, dissemination and distribution.[57] The NSA requires all of its personnel holding security clearances authorizing access to certain information to participate in extensive USSID 18 training upon the initiation of access and every two years during which they continue to have access. The Vice Chairman and Executive Director participated in the full USSID 18 training received by NSA personnel in order to examine the extent and quality of the training and to assess awareness of the need to protect the privacy and civil liberties interests of U.S. Persons among NSA personnel with access to sensitive information.

On January 17, 2007, the Attorney General notified Senators Leahy and Specter that a Judge of the Foreign Intelligence Surveillance Court (FISC) had issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (FISC Orders). As a result of the FISC Orders, any electronic surveillance that was conducted under the TSP is now conducted subject to the approval of the FISC. After the FISC Orders were issued, the Board was extensively briefed by both the Department of Justice and NSA regarding this development. Members of the Board also have studied the classified FISC Orders themselves and closely reviewed the classified material submitted to the FISC in connection with the Orders, including the applications, legal memoranda, and supporting declarations.

While the details of the FISC Orders remain classified, we can report in an unclassified format that as a result of the Orders the

[57] *See, e.g.*, EO 12333 § 2.4 ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad.").

relevant surveillance is subject both to extensive ongoing Department of Justice review and to the approval of the FISA Court. The Department of Justice's responsibilities for implementing the Orders are carried out by the new National Security Division in the Department of Justice.

Based upon its review, the Board has concluded that the Executive Branch's conduct of these surveillance activities appropriately considers and reasonably protects the privacy and civil liberties of U.S. Persons. As a result of the new FISA Court Orders, the highly regimented Executive Branch process of justification, review, approval, and auditing has been further augmented by court supervision. This provides reasonable assurance that national security and privacy and civil liberties interests are appropriately balanced. The Board found no evidence or reasonable basis to believe that the privacy and civil liberties of U.S. Persons are improperly threatened or impinged under the surveillance conducted by the Executive Branch, either under the TSP or subsequently under the new FISC Orders. In the opinion of the Board, it appears that the officials and personnel who were involved in conducting the TSP, and who now are responsible for implementing surveillance under the FISC Orders, are significantly aware and respectful of U.S. Constitutional and legal rights and protections for U.S. Persons, and they are actively committed to protecting privacy and civil liberties of U.S. Persons in conducting such surveillance.

The Board notes that it was not involved in and has taken no position on the original design or legal authorization of the TSP. The Board believes that it is appropriate for it to provide continuing advice and oversight with respect to NSA's surveillance activities.

- *National Implementation Plan*

On November 28, 2006, at the National Counterterrorism Center (NCTC), the Board was briefed on the National Implementation Plan (NIP). This plan was approved by the President in June 2006 and is intended to coordinate and integrate all instruments of national power in a unified effort to protect the Nation against terrorism. Toward that end, it assigns hundreds of specific tasks to various Federal departments and agencies. Participating departments and agencies are now adopting and implementing their own supporting plans, and an annual strategic review of the

entire NIP is in progress. The Board is working with NCTC to ensure that it has access to NIP tasks and activities that could raise privacy or civil liberties concerns.

- *Terrorist Finance Tracking Program*

  Also on November 28, at the Treasury Department, the Board was briefed on the Terrorist Finance Tracking Program (TFTP) by the Under Secretary for Terrorism and Financial Intelligence and the Assistant Secretary for Intelligence and Analysis. Under this program, intelligence analysts review records acquired through administrative subpoenas from the Society for Worldwide Interbank Financial Telecommunication to locate financial connections to known or suspected terrorists. This program also predates the Board's existence.

In each briefing, Board members were free to engage in a probing inquiry and ask unfettered questions, all of which were answered. Following each briefing, the Board met to consider further areas of inquiry, additional issues associated with these specific programs to address, and underlying documents to review. Chairman Carol Dinkins has requested Vice Chairman Alan Raul and Member Lanny Davis to coordinate continuing activities with NSA and Member Frank Taylor to coordinate continuing activities with regard to the National Implementation Plan. These initial briefings were the beginning of the Board's review of these specific programs, not the totality of its involvement.

In addition to these three anti-terror programs – NIP, TFTP, and NSA surveillance activities – the Board examined a variety of other programs and policies:

- *Department of Defense CIFA TALON Program*

  At the direction of the Board, Member Francis X. Taylor reviewed the Department of Defense Counterintelligence Field Activities (CIFA) Threat and Local Observation Notices (TALON) program. Within the last year, certain media reports alleged that the CIFA, through the TALON program, had monitored and collected information on U.S. Persons arising out of domestic activities that did not appear to present a threat to national security. During a May meeting of the Board, Chairman Carol E. Dinkins asked Member Taylor to gather background information on the alleged inappropriate activities, determine whether DOD had responded to such reports and the results of that response, and make recommendations as to whether additional review by the full Board was required. In carrying out the Chairman's charge, Member

Taylor and Board staff met frequently with those who implemented and continue to oversee CIFA. Senior policy officials fully answered the Board's questions and provided any materials that were requested. At the conclusion of its investigation, the Board determined that a lack of clear guidance from the Deputy Secretary at the time the program was established and the absence of a designated TALON program manager resulted in an ambiguous program implementation and the improper and unauthorized collection and retention of information on U.S. Persons. The Board also reviewed and endorsed the steps that DOD took prior to the Board's investigation to correct these concerns. For example, the Deputy Secretary had ordered an immediate review of the program and issued additional guidance to clarify the TALON program's scope and to emphasize that the program would be conducted in full compliance with DOD policies and procedures regarding the collection of information on U.S. Persons. CIFA also has purged the TALON system of any inappropriately collected and retained information.

- *Department of State E-Passport Program*

The Board reviewed efforts by the Department of State to distribute a passport containing an embedded data chip that holds personal information on the passport holder. The Board concluded that the *current* design of the passport does not pose substantial privacy concerns because (1) the information contained on the chip is identical to that contained in the actual passport; (2) such information is useless without an actual physical passport; (3) the passport utilizes substantial security protocols (anti-skimming technology, a unique PIN, and a varying identifier that prevents continuous tracking of the chip) to prevent someone from accessing that information remotely and from following an individual; and (4) the chip is engineered in a way that would require the State Department to recall and reissue passports before it could add more information on the chip (thereby preventing the government from easily amending the current contents of the passport). The Board stated that it would revisit this issue in the event the State Department desired to alter the program by including more information on the chip (such as new biometric measures like an iris or fingerprint scan that are in addition to the existing digital photograph that enables the biometric comparison using facial recognition technology), altering its border inspection procedures (e.g., to allow a chip to act as a proxy for a physical passport), or changing the schematics of the chip.

- *Passenger Name Recognition*

  The Board was briefed on U.S. negotiations with the E.U. over the collection and dissemination of passenger name records for flights between the two jurisdictions. The briefing provided the Board with substantive discussions of the negotiations, as well as how privacy and civil liberties officers within DOJ and DHS were involved in those negotiations. The Board is satisfied with the significant role these privacy and civil liberties officers played in these negotiations.

- *Department of Homeland Security US-VISIT Program*

  The Board is currently examining the privacy and civil liberties protections contained in the US-VISIT program. US-VISIT facilitates a process that collects and retains biometric and biographic information regarding aliens who enter and leave the country and who apply for immigration benefits. Although the program largely concerns non-U.S. person aliens, a proposed rulemaking would extend its reach to include all aliens, including Legal Permanent Residents (who qualify as U.S. Persons). The greatest civil liberties questions center on how information collected as part of US-VISIT will be shared within the government and with outside entities.

- *USA PATRIOT Act Review*

  The 2006 reauthorization of the USA PATRIOT Act included over 30 new civil liberties protections. Member Lanny Davis visited the Department of Justice on November 17, 2006 to be briefed on these new protections by staff with the new National Security Division. Member Davis has been tasked by the Board to continue working with the Department of Justice to monitor implementation and operation of these protections.

2. Examples Where the Board Has Offered Advice Regarding the Development of a Policy, Program, Regulation, or Statute

- *Watch List Redress*

  At the request of the Board, Vice Chairman Alan Raul has undertaken the coordination of efforts among the various relevant Federal departments and agencies to establish a formalized,

unified, and simplified redress procedure for individuals with adverse experiences with the government's watch list or during screening processes. Both government officials and non-governmental advocacy experts repeatedly raised this issue as an area where the Board could bring focus, organization and prioritization.

The Terrorist Screening Center (TSC) is charged with maintaining the U.S. government's consolidated terrorist watch list, which contains the identifying information of all known or appropriately suspected terrorists. Thirteen months after the Center began operations, it established a formal watch list redress process. The process allowed agencies that used the consolidated terrorist watch list data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appeared those complaints were watch list-related. The goal of the redress process is to provide timely and fair review of individuals' complaints and to identify and correct any data errors, including errors in the terrorist watch list itself.

TSC's redress process consists of a procedure to receive, track, and research watch list-related complaints and to correct the watch list or other data that caused an individual unwarranted hardship or difficulty during a screening process. Throughout 2005, TSC worked closely with screening agencies to establish a standardized process for referral of and response to public redress complaints. TSC also worked with federal law enforcement agencies and the Intelligence Community, each of which may nominate individuals to the watch list, to review the redress complaint of any individual on the terrorist watch list, evaluate whether that person was properly listed and that the associated information was correct, and make any corrections which were appropriate, including removal from the watch list when warranted.

In the fall of 2005, TSC undertook to document formally the participating agencies' mutual understanding of their obligations and responsibilities arising out of the watch list redress process. Competing priorities within participating agencies, however, slowed progress. On June 20, 2006, Vice Chairman Raul convened a meeting of all relevant agencies and called for a renewed effort to prioritize this project. In attendance were representatives from the Departments of State, Defense, Treasury, Justice, and Homeland Security, the Office of the Director of

National Intelligence, the CIA, the FBI, the National Counterterrorism Center, and TSC.

The resulting draft Memorandum of Understanding (MOU) is a constructive and positive step intended to secure a commitment from these agencies that participate in the watch list process to engage actively in and support the redress process. The MOU resulted from a six-month period of negotiations between the agencies mentioned previously. Vice Chairman Raul convened a final working group meeting on November 30, 2006; in January 2007, a final draft of the MOU was approved and submitted for the signature of the heads of these agencies.

The MOU sets forth the existing multi-agency redress process in significant detail, from receipt of an individual's complaint to the response sent by the screening agency. Among other things, the MOU establishes obligations for all parties to secure personal information, update and correct their own record systems, and share information to ensure redress complaints are resolved appropriately. Each participating agency must also commit to providing appropriate staff and other resources to make sure the redress process functions in a timely and efficient manner. Finally, each agency must designate a senior official who is responsible for ensuring the agency's full participation in the redress process and overall compliance with the MOU.

Once the MOU has been executed and implemented, the Board intends to continue efforts to bring all possible transparency and public understanding to this process.

- *Department of Defense Report of the Technology and Privacy Advisory Committee*

In September 2006, the Department of Defense forwarded to the Board the recommendations of the March 2004 Report of the Technology and Privacy Advisory Committee (TAPAC) to the

Secretary of Defense.[58] Five of the twelve recommendations required action on a government-wide basis beyond the authority of the Department of Defense. The Board is currently evaluating that Report to determine the extent to which the government has already implemented those recommendations and what additional steps the government should take to complete those recommendations.

- *Administration Clearance Processes*

  As mentioned above, the Board has been fully integrated into the various Administration and Executive Branch program and policy clearance processes, including the OMB Legislative Referral Memorandum (LRM) process. As such, it regularly receives and is invited to comment on policy initiatives, programs, regulations, proposed legislation, and public remarks by agency officials that may have privacy or civil liberties implications.

3. Information Sharing

IRTPA called for the creation of the Information Sharing Environment (ISE). The ISE is an approach that facilitates the sharing of information relating to terrorism by putting in place the processes, protocols, and technology that enable the sharing of this information among Federal, State, local, tribal and private sector entities and foreign partners. The ISE brings together, aligns and builds upon existing information sharing policies, business processes and technologies (systems), and promotes a culture of information sharing through increased collaboration. IRTPA also established the Program Manager for the Information Sharing Environment with government-wide authority to plan, oversee, and manage the ISE. The Program Manager assists the President and government agencies in the development and operation of the ISE and monitors and assesses its progress.

[58] *Safeguarding Privacy in the Fight against Terrorism* (March 2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf (last accessed Dec. 29, 2006).

To guide efforts to establish the ISE and implement the requirements of IRTPA, on December 16, 2005, the President issued a Memorandum to the Heads of Executive Departments and Agencies. This Memorandum delineated two requirements and five guidelines that prioritize efforts that the President believes are most critical to the development of the ISE and assigns Cabinet officials responsibility for resolving some of the more complicated issues associated with information sharing. The five guidelines are: (1) Set Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE; (2) Create Common Framework for Sharing Information Between and Among Federal Agencies and State, Local and Tribal Governments, Law Enforcements Agencies and the Private Sector; (3) Standardize Procedures for Sensitive But Unclassified Information; (4) Facilitate Information Sharing with Foreign Partners; and (5) Protect the Information Privacy Rights and Other Legal Rights of Americans.

IRTPA required that these guidelines be drafted and implemented in consultation with the Board. And with regard to all five sets of guidelines, the Board's Executive Director is a member of the White House Information Sharing Policy Coordination Committee which sits above all the working groups and directly below the Deputies and Principals Committees.

The President assigned various agencies the lead in developing the five sets of guidelines. The Department of Justice and the Office of the Director of National Intelligence were jointly assigned the lead in developing Guideline 5, now referred to as the ISE Privacy Guidelines. Within those agencies, the lead was assigned to the DOJ Chief Privacy and Civil Liberties Officer and ODNI's Civil Liberties Protection Officer. This ISE Privacy Guidelines drafting group spent April through November 2006 soliciting comments and working with the Program Manager and White House staff, including Homeland Security Council staff and Board staff.

On May 16, 2006, the Board held its fourth meeting and, among other things, was briefed on the ISE by the Program Manager for the Information Sharing Environment. On June 26, at the Board's eighth meeting, the working group leaders briefed the Board specifically on the ISE Privacy Guidelines.

On November 16, 2006, the Director of National Intelligence sent to Congress the ISE Implementation Plan, which discusses how to bring about an information sharing environment. Although the parameters of the plan were adopted in December 2005 prior to the Board's existence, the Board's Executive Director did offer substantive advice regarding its content. On November 22, 2006, the President approved the Guidelines 1, 2, 4, and 5 reports, including the recommendation that the ISE Privacy Guidelines be issued. These were subsequently released to the public by the Program Manager.

The ISE Privacy Guidelines (Protect the Information Privacy Rights and Other Legal Rights of Americans) work in conjunction with the other information sharing guidelines, requiring each set to address its specific area of interest in a manner that protects the privacy rights and civil liberties of Americans. The guidelines must also implement provisions of Executive Order 13388, which requires agencies to "protect the freedom, information privacy, and other legal rights of Americans" while sharing terrorism information.

The ISE Privacy Guidelines regulations establish an information sharing framework that balances the dual imperatives of sharing information and protecting privacy by establishing uniform procedures to implement required protections in unique legal and mission environments. In addition, the framework establishes an ISE privacy governance structure for compliance. The framework attempts to strike a balance between consistency and customization, substance and procedure, and oversight and flexibility. It also builds upon existing resources within Executive agencies and departments for implementation.

The ISE Privacy Guidelines are based on a set of core principles that requires agencies to: identify any privacy-protected information to be shared; enable other agencies to determine the nature of the information and whether it contains information about U.S. Persons; assess and document applicable legal and policy rules and restrictions; put in place accountability and audit mechanisms; implement data quality and, where appropriate, redress procedures; and identify an ISE Privacy Official to ensure compliance with the guidelines.

The ISE Privacy Guidelines regulations also require Federal departments and agencies to designate an ISE Privacy Official to oversee the full implementation of the privacy regulations. The ISE Privacy Official is the department or agency's senior privacy official (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency.

The ISE Privacy Guidelines also provide for an ISE Privacy Guidelines Committee, consisting of the ISE Privacy Officials of the departments and agencies comprising the Information Sharing Council (ISC), and chaired by a senior official designated by the Program Manager. Working closely with the Privacy and Civil Liberties Oversight Board as it exercises its oversight mission, the committee will seek to ensure consistency and standardization in implementation, as well as serve as a forum to share best practices and resolve inter-agency issues. The ISE Privacy Guidelines Committee will continually refine its guidance as the ISE develops and as specific sharing mechanisms are institutionalized. The Program Manager has designated the DOJ Chief Privacy and Civil Liberties Officer and ODNI's Civil Liberties Protection Officer to serve as co-chairs of this ISE Privacy Guidelines Committee, which will include the Board's Executive Director as a member.

The Board instructed its staff to meet with the Program Manager and provide options concerning its on going oversight role and how that role can be most effectively and efficiently exercised.

VI. THE YEAR AHEAD

After working to establish the foundation discussed throughout this report, the Board looks forward to continuing to fulfill its statutory responsibilities in the upcoming year. The Board intends to utilize the knowledge and trust built over the last year to engage, as time and resources allow, issues that will have the greatest impact on the greatest number of U.S. Persons. While it is impossible to foresee all issues that may arise in the coming year warranting the Board's attention, issues which the Board presently intends to pursue include:

- *Information Sharing Environment (ISE).* As discussed above, the Board is specifically charged with responsibility for reviewing the terrorism information sharing practices of Executive Branch departments and agencies to determine adherence to guidelines designed to appropriately protect privacy and civil liberties. Accordingly, the Board was integrated into the process chaired by the Program Manager for the development and implementation of appropriate information sharing guidelines for Federal departments and agencies. The Board will work with the Program Manager to institutionalize its implementation oversight role.

- *Government surveillance operations.* The Board will continue to exercise its oversight role over terrorist surveillance.

- *Terrorist watch list issues.* The Board played a role in coordinating efforts among the various Federal departments and agencies to establish a unified, simplified redress procedure for individuals with adverse experiences during screening processes. The execution of an interagency memorandum of understanding on redress procedures is only a first step in establishing a simple, transparent process. The Board will continue its efforts to promote this process.

- *USA PATRIOT Act and National Security Letters (NSLs).* The 2006 reauthorization included over thirty new civil liberties protections. The Board will work with the Department of Justice to monitor implementation of these protections.

- *Federal data analysis and management issues.* Board Members intend to enhance significantly their understanding of issues associated with data mining activities, data sharing practices, and governmental use of commercial databases. This level of understanding will assist the Board in its review of many Federal anti-terrorism programs. Toward this end, the Board will follow up on recommendations of the March 2004 report of the Technology and Privacy Advisory Committee (TAPAC) to the Secretary of Defense, *Safeguarding Privacy in the Fight Against Terrorism.*

- *U.S. Persons Guidelines.* These guidelines limit the government's ability to collect, retain, and distribute intelligence information regarding U.S. Persons.

These guidelines are applicable to agencies in the intelligence community pursuant to Executive Orders 12333 and 13284. As was noted in the 2005 report to the President on Weapons of Mass Destruction, these rules are complicated, subject to varying interpretations, and substantially different from one agency to another. The Attorney General and the Director of National Intelligence have established a staff level working group to review these guidelines and propose appropriate reforms. The Board intends to participate in this process.

- *State and local fusion centers.* State and local law enforcement entities are establishing joint centers where they share information and data of value to their common missions. Federal agencies are developing partnerships with these centers. The Board will review these sharing practices to ensure that privacy rights and civil liberties concerns are taken into appropriate consideration.

- *National Implementation Plan (NIP).* The National Counterterrorism Center is presently conducting the first strategic review of the NIP. The Board is interested in the results of this review and actions taken as a result of its findings and recommendations. The Board will also continue to monitor those on-going NIP tasks and activities that might raise privacy or civil liberties concerns.

- *Department of Homeland Security Automated Targeting System (ATS).* ATS is a decision support tool used by Customs and Border Protection to assist in making a threshold assessment in advance of arrival into the U.S. based on information that DHS would otherwise collect at the point of entry. The Board intends to review this system.

- *Material Witness Statute.* As a result of concerns raised at its December 5, 2006 Georgetown University forum, the Board will investigate public expressions of concern over how this statute is being used in Federal anti-terrorism efforts

The Board will continue its efforts to reach out to those Administration officials with significant responsibilities in protecting the Nation against terrorism. To that end, the Board looks forward to meeting with the Secretaries of State and Defense, the new Director of the Central Intelligence Agency, and the new director of the Terrorism Screening Center.

Administratively, the Board will focus on further developing its staff resources by supplementing the permanent staff with detailees from the intelligence, law enforcement, and technology communities. Depending on developing priorities, the Board intends to bring in six detailees for terms of six months to one year.

In addition, recognizing the value and benefit of the public dimension to its responsibilities, the Board will conduct a continuing series of open public forums, perhaps around the country, that will allow interested American citizens to express their

concerns with regard to privacy and civil liberties implications in the war against terrorism.

Finally, the Board understands that it may adjust its agenda based on evolving issues and concerns - whether those issues are brought before the Board through its internal role within the Executive Office of the President or through public comment.

VII. CONCLUSION

Standing up any new institution takes vision, energy, and commitment. The Board believes it has made substantial solid progress over the past year in setting priorities and integrating itself into existing Executive Branch policy formulation and implementation procedures. The Board is pleased with the enthusiasm and level of support it is receiving, both substantively and administratively, from White House staff, the Executive Office of the President and other Federal departments and agencies essential to the protection of privacy and civil liberties.

Most importantly, as mentioned several times in this report, the Board has established a sound and productive working relationship with the growing universe of privacy and civil liberties professionals within the Executive Branch. Working together, these professionals and the Board are developing a system of mutual trust and support. This relationship is fundamental to the Board's ability to fulfill its role of providing constructive, objective advice to the President and relevant agency heads.

The American people expect the Federal government to protect them from terrorism, and to do so consistent with the Constitution and important American values. The Privacy and Civil Liberties Oversight Board is one of many checks and balances existing within the Federal government to help promote this. It is not a substitute for the President's responsibility to preserve, protect, and defend the Constitution of the United States or the oversight roles exercised by Congress. Instead, it is a significant new body within the Federal government in a position of trust and proximity to the President that can offer an objective assessment of policy initiatives.

The Board Members take their statutory mission and responsibilities seriously and look forward to working with the Executive Branch and Congress[59] in fulfilling them in the upcoming year.

[59] The 110th Congress is considering whether the Board's present construct, as established by IRTPA, warrants modification. Pending legislative initiatives would remove the Board from the Executive Office of the President, make it an independent agency within the Executive Branch, and provide it with subpoena power. Other proposed changes would keep the Board within the EOP but would require all Members to be nominated by the President and confirmed by the Senate to staggered six-year terms, with the Chairman assuming a full-time appointment.